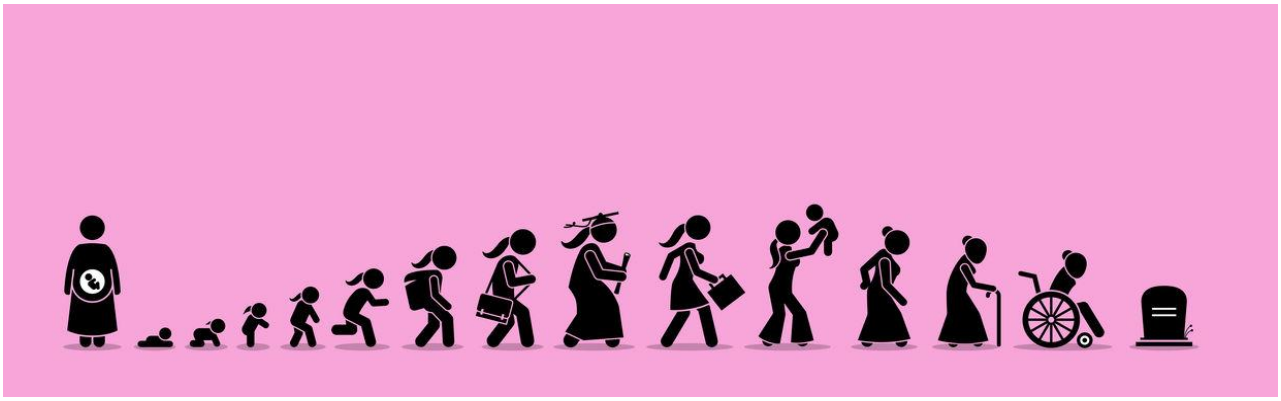
Cost Centres – Rethinking Legal Identity & Learning Vision



Author: Guy, Huntington, President, Huntington Ventures Ltd.
Original issue date: October 1, 2021
Updated: April 20, 2024
Note:

1. **This document version was updated with:**
    a. **Sections and costs on co-design**
    b. **Allocated one time subsidy funds for the federal government to issue to local states/provinces to encourage them to rapidly adopt a new CRVS framework.**
    c. **An edit of cost centres to reduce total guesstimated costs by combining resources and expertise to lower budget costs**

Executive Summary

The planet is dramatically changing with the arrival of AI systems, physical and digital bots. It directly affects national security. Why? An AI system in one jurisdiction on the planet can create malicious, smart digital bots at speeds of thousands or more per second. In the next second, they're operating in all other jurisdictions on the planet targeting citizens, companies, enterprises, and different levels of government. Today, on the planet, there is no legal identity architecture able to instantly determine entity friend from foe. Thus, we're screwed.

This document contains architecture addressing this. It gives each person, company, enterprise, and different levels of government on the planet an ability to instantly determine entity friend from foe. It also enables each of us, if we want to, the ability to live privately in a very non-private world. It does so with legal identity toolkits that works for all citizens, regardless of their abilities or disabilities.

Further, the architecture takes the above and leverages it to rethink learning for all learners on the planet, regardless of their abilities or disabilities. It gives each learner on the planet their own digital learning twin which constantly updates their own individualized education plan. The architecture leverages AI systems, physical and digital bots, rethought human learning specialists and AI/AR/VR learning environments. It leaves no learner behind on the planet.

As Albert Einstein said, "We can't solve problems by using the same kind of thinking we used when we created them." Thus, this cost centre document acknowledges the fact creating a new vision requires many parallel crawling steps to get us from where we are today to the promised land. Thus, for each of the 249 different subcomponent cost centres, the strategy used is to crawl, walk and then run. Each team within a cost centre has lessons learnt experts identifying what didn't work, what did work, learning from this, and then rapidly scale. Many activities can begin in parallel, without waiting for a linear completion of others.

The biggest political challenge is for the national government to rapidly get buy-in from their local state/provinces who administer CRVS systems. Thus, one-time federal government issued subsidies are used.

The biggest technical challenge is for the CRVS system to securely write legal identifiers to an entity's source code at transactional speeds. I suspect, but don't know, it requires a new programming language. Thus, significant funds are allocated to addressing this,

Total guesstimated costs for the architectures are between $21-35 billion. Leaders and their policy makers should skim. "**Why Should Your Government Fund The Architectures?**"

We're entering a major paradigm shift where our old ways won't work well anymore. Thus, it requires out of the box thinking for our out of the box times. That's what this document delivers.

TABLE OF CONTENTS

Introduction:

This document is a summary of my work, over the last eight years, wanting to rethink human and AI system/bots legal identities and then apply it to rethink learning. It creates an architecture:

- Which is politically acceptable to each jurisdiction
- Abel to instantly determine entity friend from foe
- Reduces legal identity friction in all business processes and workflows around the planet
- Could then be leveraged to rethink learning. It does so by understanding each learner, from a very young age, giving them digital learning twin, with the resources, human contact et al, to learn, regardless of their learning ability and where they live on the planet

My goal was to leave no one behind as the tech tsunami wave of change strikes out planetary shores. Next, I wanted to put myself in the seat of a jurisdiction leader, their finance minister, and funders, who would rightfully be asking me:

- How much this would cost?
- How we'd implement it given the complexity involved?

That's what this document is. It breaks down the vision into small architectural steps, identifying not only the cost centres, but as importantly, recommending a strategy to begin crawling towards the vision.

As you'll soon see, by skimming this doc, it's very involved i.e., long, and very detailed. There are numerous new pieces required to make all the magic work. Rather than try to convince the planet what a wonderful idea it is, my strategy instead is to find a funding country, using national security as the driving force, and then bear down on the work. Prove it out in small quick stages, learn what didn't work, what worked, and then rapidly scale.

My underlying premise is most jurisdictions around the planet don't have the resources, experts, budgets et al to continually address this continual new attack vectors created by this curve -. That's why the doc proposes the concept of two very well-funded, independent non-profits to do this:

- One to manage:
  - The legal identity framework, with a small license fee per:
    - CRVS event to a maximum yearly amount per jurisdiction and also
    - An extremely small fee for each credential issued to an entity
  - Do 24x7x365 threat assessment against the legal identity framework
  - Manage the SOLICT (Source of Legal Identity & Credential Truth) cloud databases
- The other to manage the new learning standards et al, with each jurisdiction licensing it by charging a very low per student annual charge to a maximum annual amount

Notes On This Document:

1. The way this document is structured is as follows:
    a. Vision section
        i. Read this if you want to see a 100,000-foot level vision
        ii. Skip it if you want to dive to the details
    b. Costs centres:
        i. As you'll soon see, there's 294 subcomponent cost centres
        ii. Each cost centre section begins with a pic showing the architectural components and cost centres beginning with a background, explaining more about the cost centre
        iii. It's then followed by a subcomponent cost section. This typically includes:
            1. Background explaining why the subcomponent exists
            2. Creating a starting budget to assemble a team to determine high level deliverables
            3. Create use cases
            4. Dive towards doing POC's (proof of concenpts0 to see what works and more importantly what doesn't work
            5. Work towards rapidly doing small, controlled pilots
            6. When successful, do lessons learnt and then rapidly scale
            7. That's why, for almost all cost centres, I recommend having lessons learnt experts as part of the team.
    c. **In many of the cost sections, I state I'm not the expert.** Thus, I'm expecting experts to amend what I'm recommending, offering a better way of doing it
    d. For many of the cost centres, it requires similar types of resources. Thus, rather than continually duplicate resources, each working independently of the other cost centre, I've proposed drawing resources out of common pools, extensively cross-sharing what's learnt as we rapidly design and test.
    e. FOR EACH COST CENTRE I HAVE NOT INCLUDED:
        i. Project and program manager resources. Why? I knew that depending on the funder, we would likely combine several cost centre subcomponents under one program manager and then decide how to best manage each subcomponent cost centre.
        ii. Overall support costs of finance, payroll, legal, HR, IT resources, etc. for each cost centre also isn't specifically included.
        iii. HOWEVER, there are operating costs associated with most cost centres. These will cover these expenses as well as providing the tech required for the cost centre, etc.

2. Leaders and their senior policy advisors should skim these documents:
    a. **"Why Should Your Government Fund The Architectures?"**
    b. "National Security – Reduce Risk By Instantly Determining Entity Friend From Foe"
    c. "Give Your Industry A Significant Competitive Edge"
    d. An Identity Day in the Life of Jane Doe" to see an example of a day in the life of your citizens leveraging the new architecture
    e. "Sir Ken Robinson - You Nailed It!" to understand how it will transform learning
    f. "National Security, Co-Design & People With Disabilities."
    g. "Why Should You Read The 500 Page Cost Centre Document?"
3. To understand the underlying problems, skim these articles:
    a. **"The Challenge with AI & Bots - Determining Friend From Foe"**
    b. **"A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings"**
    c. "Hives, AI, Bots & Humans - Another Whopper Sized Problem"
    d. "Legal Identity Problem Statements"
    e. "Legal Identity Relationships"
    f. "Verifiable Credentials For Humans and AI Systems/Bots"
    g. **"Legal Identity Vs. Legal Personhood"**
    h. "The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom"
4. To see a high level overview of the architectures skim:
    a. "Rethinking Human Legal Identity"
    b. "Creating AI Systems/Bots Legal Identity Framework"
    c. "Learning Vision Flyover"
5. To see how the architectures will leave no learner behind on the planet skim:
    a. **"Learning Journey of Two Young Kids In A Remote Village**
6. To see what new toolkits are required skim these articles:
    a. "TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age"
    b. "Entity Management System'"

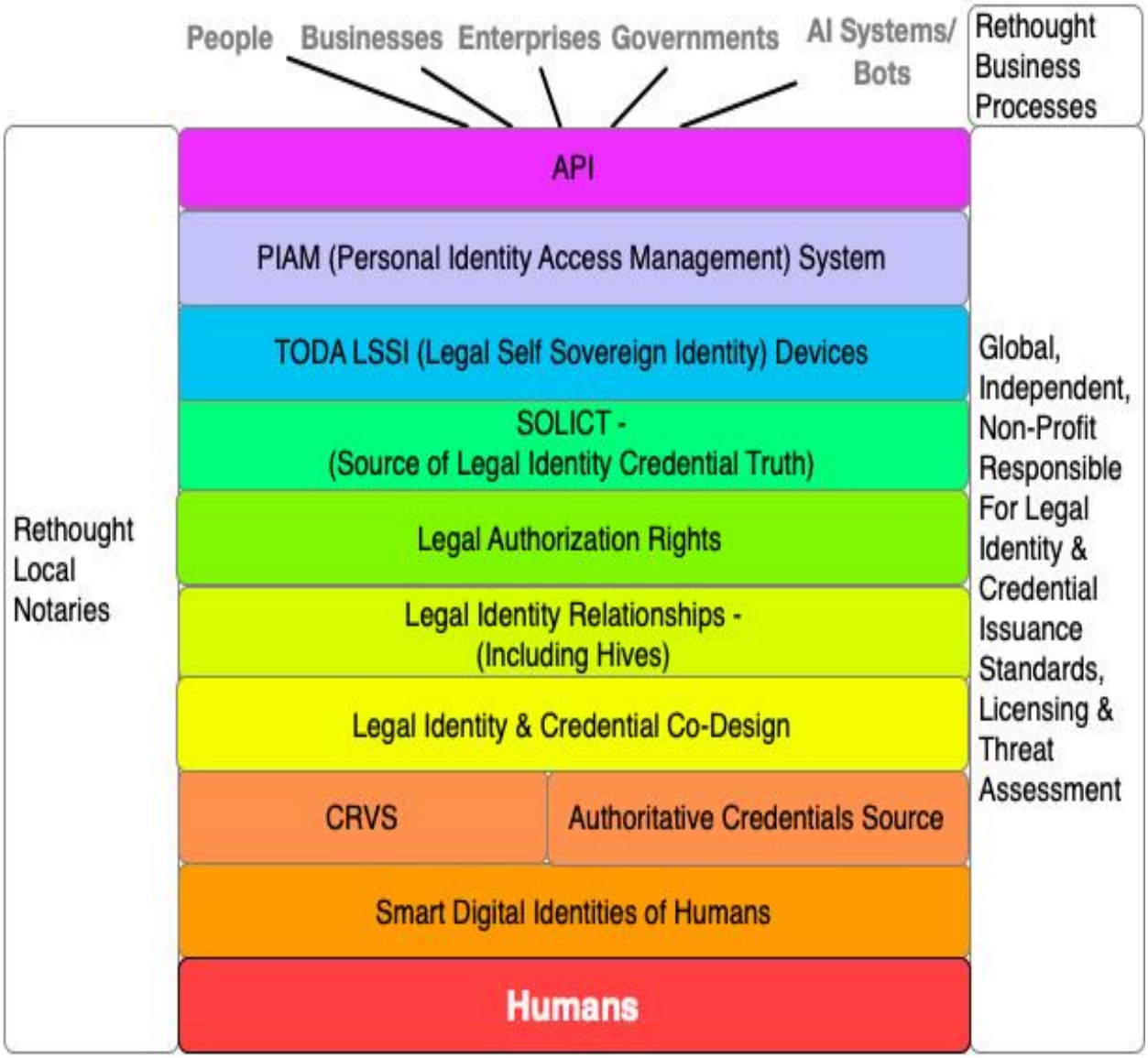
7. **Repeatedly throughout the document, I state my strategy of not trying to convince the planet what a wonderful idea all the above describes. Instead, I'm looking for an innovative out of the box country to work with funding, designing, implementing and maintaining the end-to-end architectural framework.**
    a. Over my lifetime of rescuing large projects, I've learnt to break them down into small crawl, walk and then run phases. Thus, I'm recommending doing this as described above i.e., rapid POCs, small, controlled pilots, implementation, and then rapid scaling.
    b. Start small, prove it out in a few jurisdictions. If it works well, it will rapidly be adopted by other jurisdictions to reduce identity friction, fraud, etc.
8. Regarding actual project management methods:
    a. Many of the cost centres can be done using an agile sprint project methodology
    b. Some will require a traditional waterfall management.
    c. My intent is to rapidly get to POC and small controlled pilot stages, i.e., its visionary "stuff" requiring the school of hard knocks learning what works and doesn't work.
9. Within scope of this document is an ability, where risk warrants it to register:
    a. Smart digital identities of humans, attaching it to the underlying physical legal identity.
    b. Legal identities of AI systems and bots (both physical and virtual)
10. **Out of scope for this document is development of a commercial version of the architecture**
    a. HOWEVER, note that I'm proposing to a funding country to create this using their banks. Skim "**Identryx**" - https://hvl.net/pdf/Identryx.pdf
11. **Actual budget guesstimates are contained with these two docs:**
    a. **Guesstimate Cost Notes Rethinking Legal Identity & Leveraging This to Rethink Learning (PDF)**
    b. **Guesstimate Costs Rethinking Legal Identity & Leveraging This to Rethink Learning (Excel Spreadsheet)**

Core Legal Identity Cost Components:

There are two fundamental underlying components of legal identities:

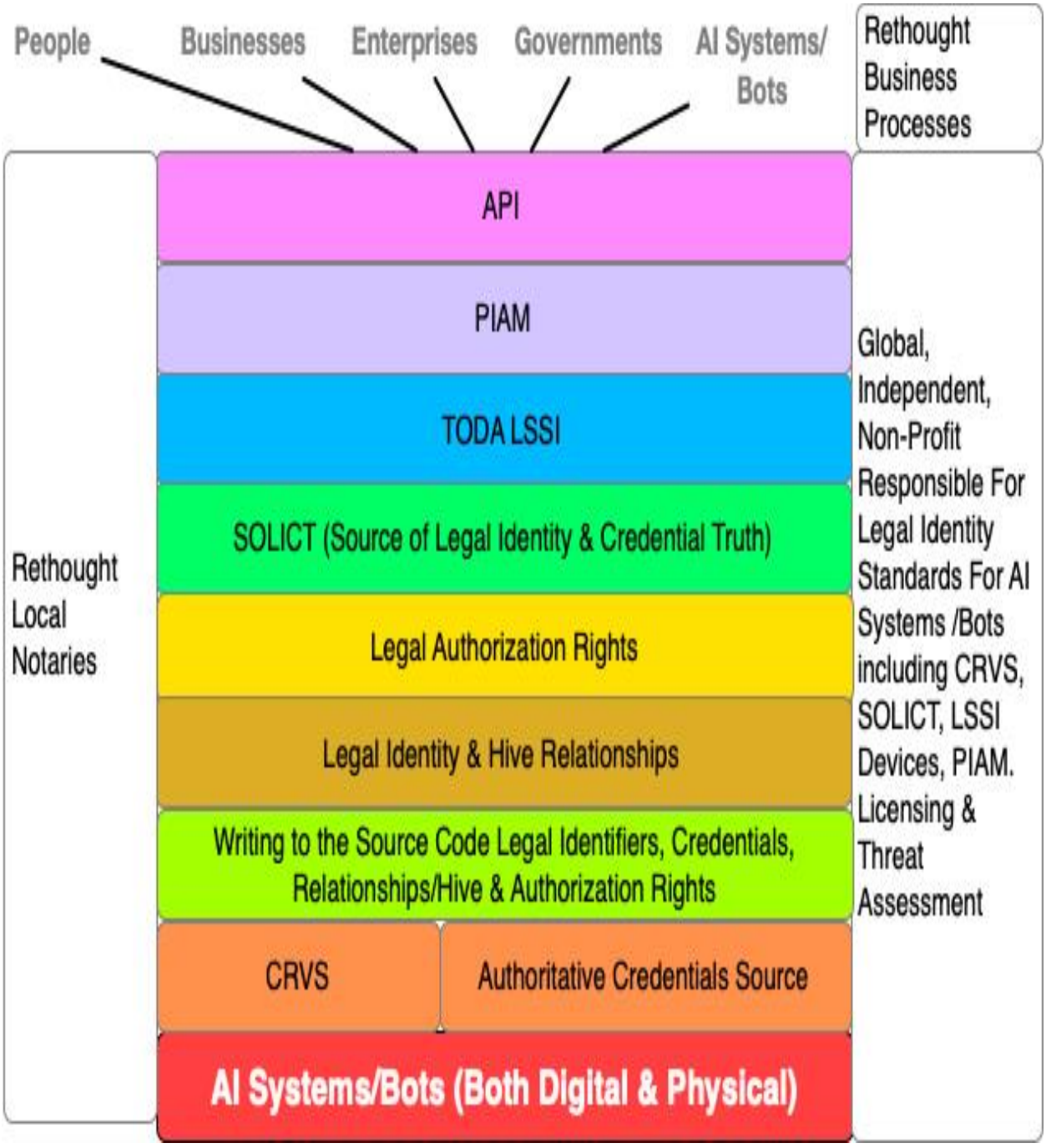
- Humans
- AI systems and bots

Humans Legal Identities:



Skim this doc to see a high-level overview of the components, "**Rethinking Human Legal Identity**"

AI Systems/Bots Legal Identities Cost Components:



Skim this doc to see a high-level overview of the components, "**Creating AI Systems/Bots Legal Identity Framework**".

Vision - Core Human Identity

Background:

Biometrics are not a secret. Skim this article, "**I Hate How We Use Biometrics Today**". They can be easily obtained at a distance without the user's consent e.g., this 2014 story of a German cabinet minister having her fingerprints easily obtained.

Thus, I ask the dumb question, "How does a person deal with the fact their biometrics have been stolen and are being maliciously used by others?"

Identity Vision:

To answerer this requires the ability to revoke and reissue biometrics. Within the CRVS Biometrics Cost Subcomponents Section, is an urgent research project, "**Research & Standards for Anonymous Biometric Identifiers Subcomponent Cost Centre**" to confirm the 2015 work of Rud Bolle on combining random numbers with biometrics making them revocable and re-issuable. Let's use Jane Doe as an example to illustrate the hypothetical potential power of this…

Identity Examples:

Step 1 – Issuance of Jane Doe's Legal Identity/Credentials

Jane Doe's fingerprints, iris scans and face image are obtained and stored in the CRVS systems. Hypothetically, assuming Rud's paper works out, a random number will be used as part of an algorithm, creating a digitized value. The CRVS will store the actual biometrics, along with the random number and the digitized value in the CRVS database, which will never leave the CRVS system.

Note:
Why store the actual forensic biometrics in the CRVS database? If Jane Doe dies, without legal identification, the local coroner can obtain her forensic biometrics, if available, and then do a search across all CRVS systems around the planet to confirm her identity. The ability to do this will be tightly controlled by laws and regulations i.e., the coroner can, in effect, search the entire CRVS database systems planet wide.

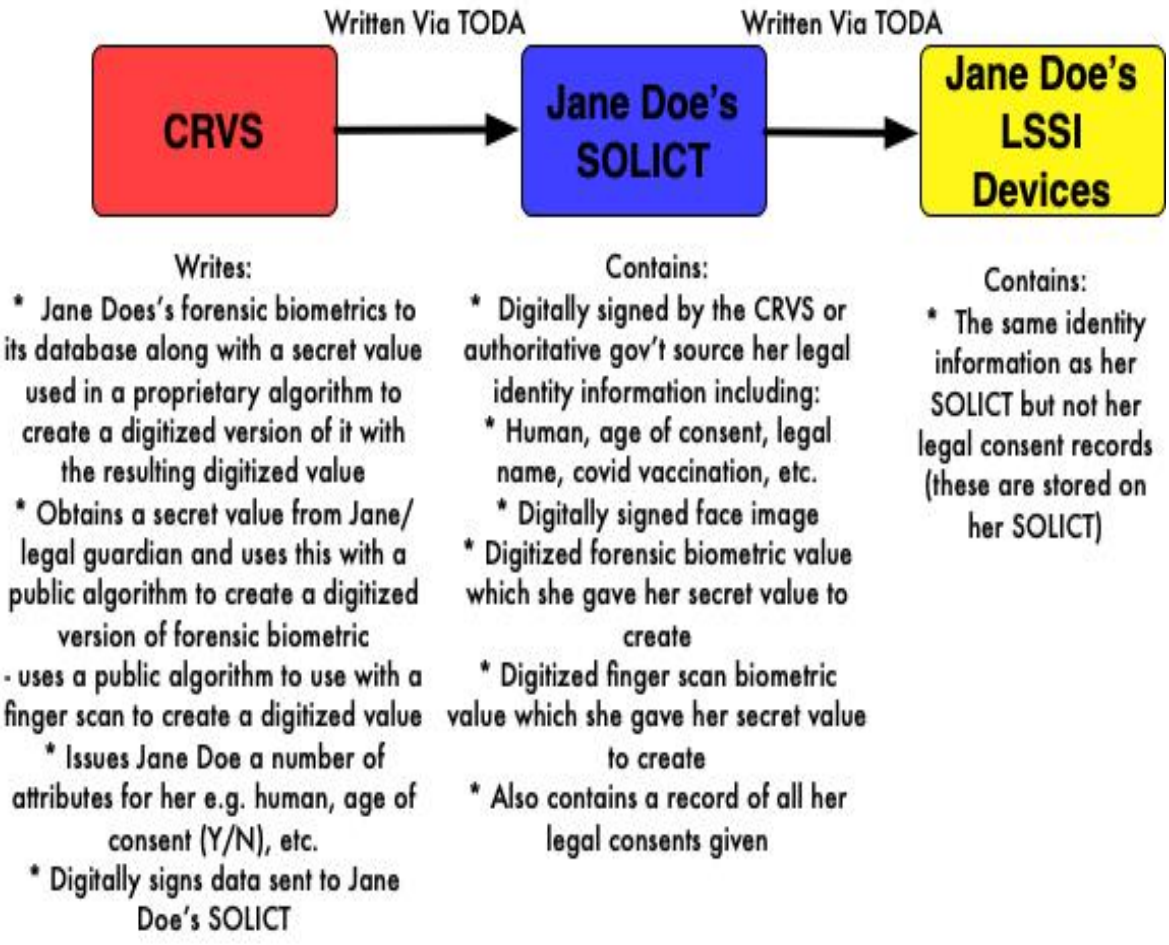
The CRVS will then write to Jane Doe's SOLICT (Source of Legal Identity & Credential Truth). However, the biometrics it writes to the SOLICT will be using another algorithm, which is publicly known along with a secret value. The secret value used for this will be selected by Jane or her legal guardian. The CRVS will take the value, calculate the digitization value, and write this, as well as the actual algorithm, to her SOLICT.

Further, the CRVS will also take a finger scan (which is different than obtaining her fingerprints). This can be used for authentication. The same process used above for writing Janes biometric to her SOLICT will be used. The CRVS digitally signs all the above.

Thus, Jane now has in her control the following:

- Her finger scans, plus her face image, using a secret value only Jane knows, digitally signed by the CRVS, along with the algorithm used to calculate it, which she can use to authenticate herself, without the government being involved
- Her forensic biometrics (fingerprints and iris) plus her face image, which is calculated by the CRVS using a secret random number only the CRVS knows, digitally signed by the CRVS
- Her SOLICT writes this to her LSSI devices

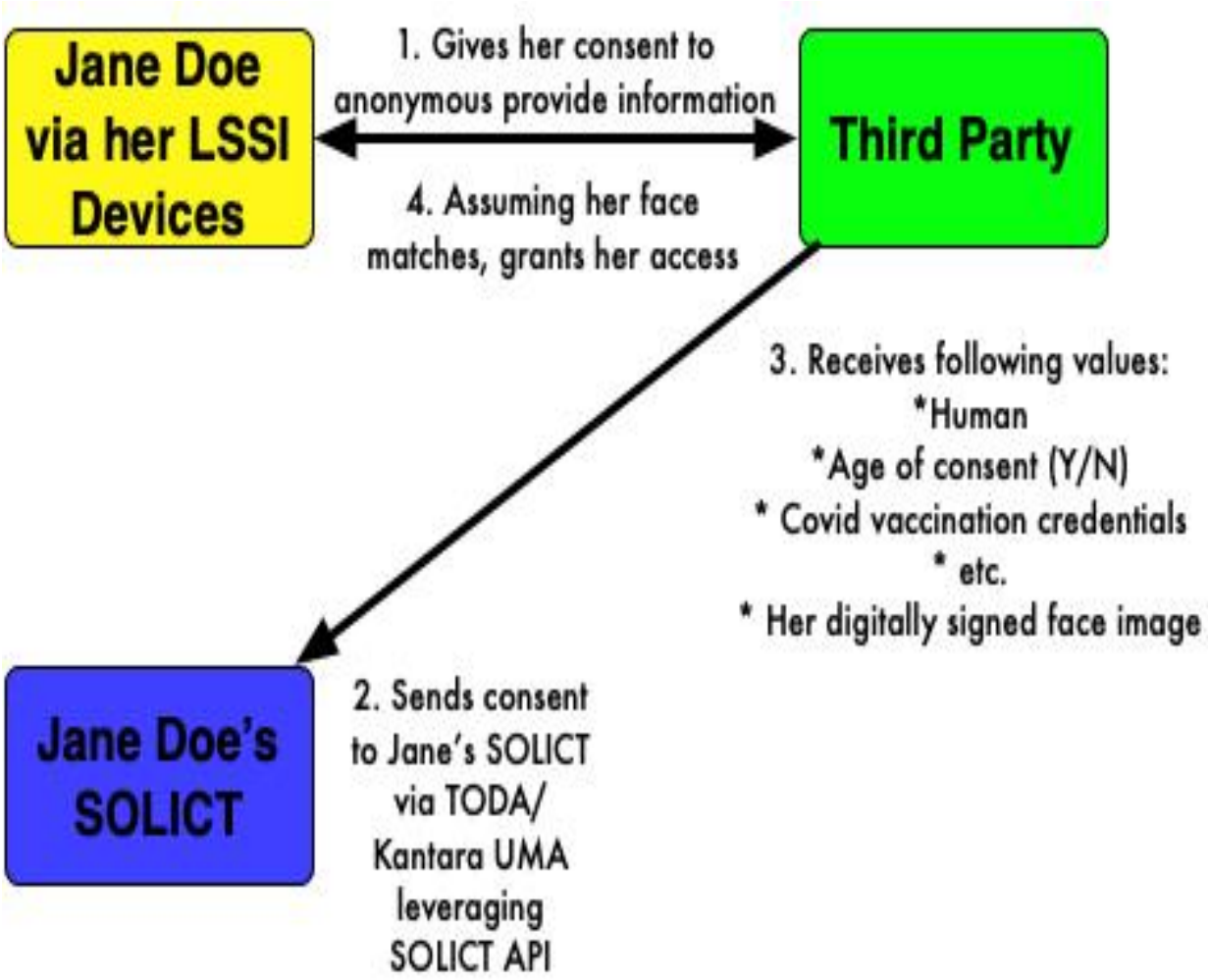
Step 1: Issuance of Legal Identity



Step 2. Anonymously Proving Her Age of Consent, Covid Vaccination, Etc.

Jane can now use these where, when, and how she pleases, with her consent. She can easily, anonymously prove she's a human, above or below age of consent, she's received her Covid vaccinations, etc.

Step 2: Proving Identity/Credentials, Legally, Anonymously

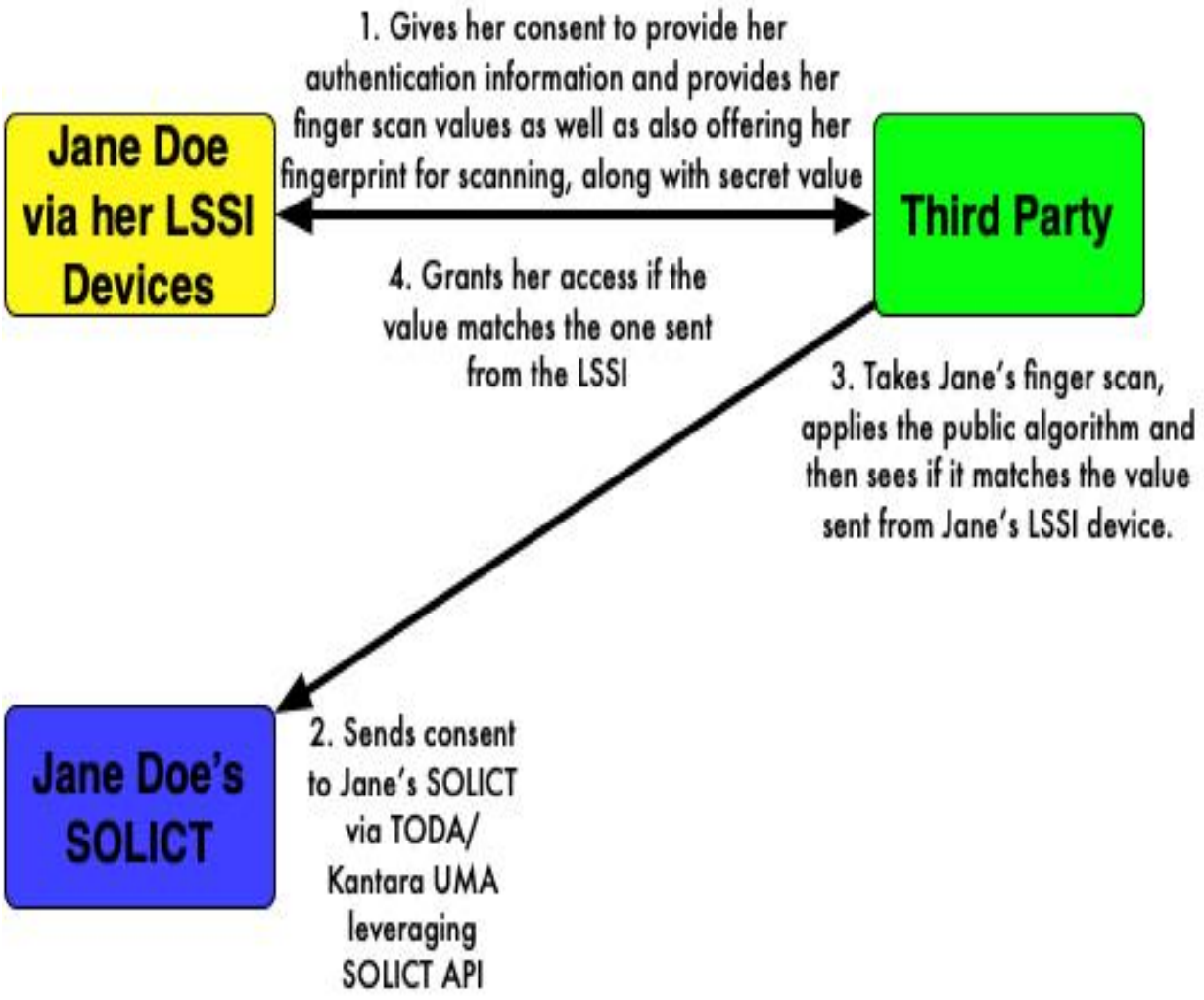


Note: For the above the third party optionally could make a quick electronic trip to validate the digital signature sent by the authoritative identity and credential source.

Step 3: Jane Authenticates With a Third Party

She can present the fingers scans to authenticate herself. The party obtaining her fingers cans, asks Jane to input her secret value, then quickly calculates the finger scan number, and compares it to the one on Jane's LSSI devices. If it matches the party can also compare the face image on her SOLICT/LSSI devices to the Jane's face. It now has a moderate degree of assurance it's Jane Doe they're interreacting with.

Step 3: Authenticating as Jane Doe



Note:

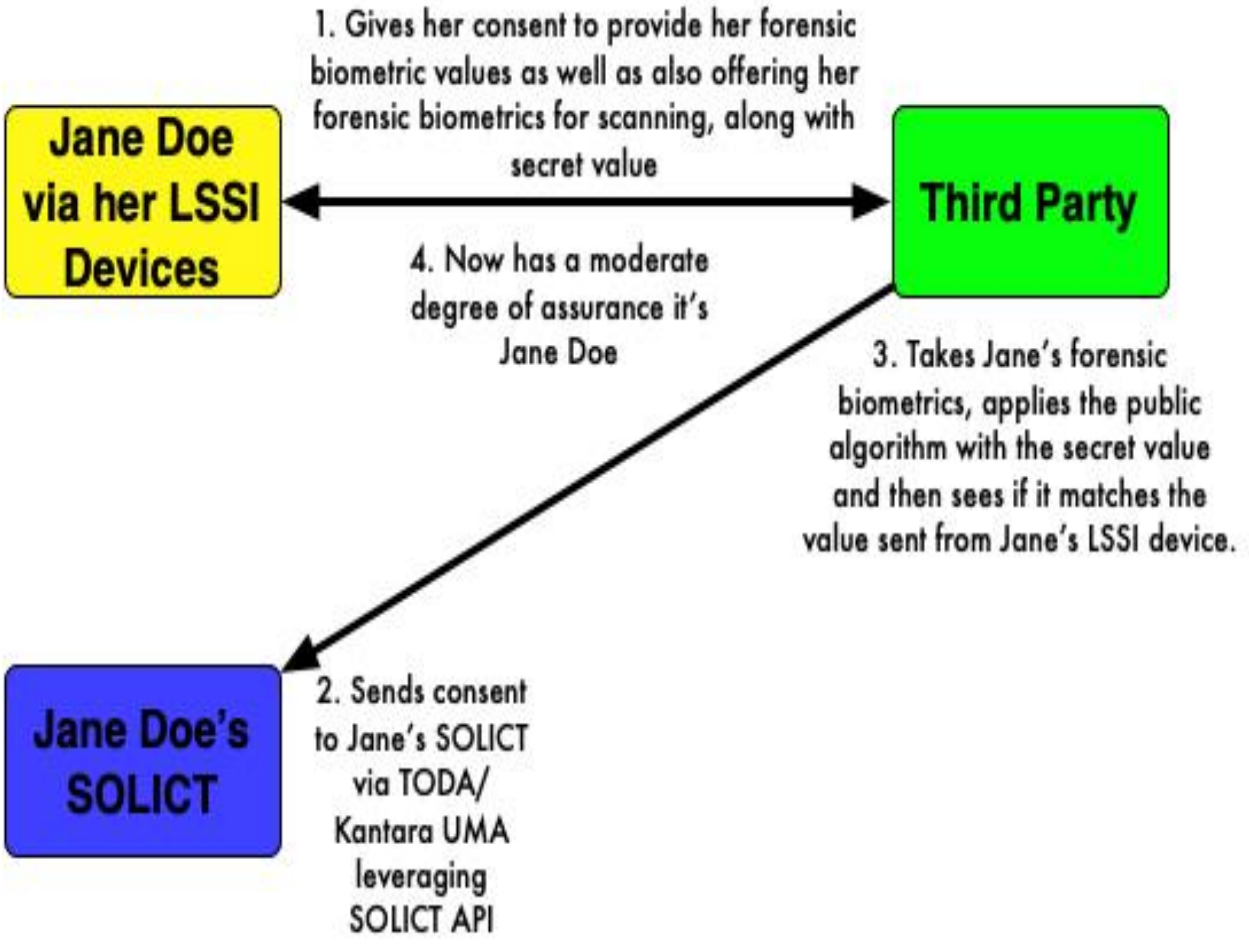
1. For the above the third party optionally could make a quick electronic trip to validate the digital signature sent by the CRVS
2. There will be a different version of this type of authentication, using an iris scan

Step 4: Increased Identity Assurance

If a third party wants a higher level of assurance it's Jane, it can, with her consent:

- Obtain her forensic biometrics along with getting Jane to enter in her secret value
- Then process this using the public algorithm
- The value obtained must be the same as the one in Jane's SOLICT/LSSI device
- Assuming it is, and her face matches the digitally signed one on the card, the party now has a higher degree of assurance it's Jane.

Step 4: Moderate Assurance Proof She's Jane Doe



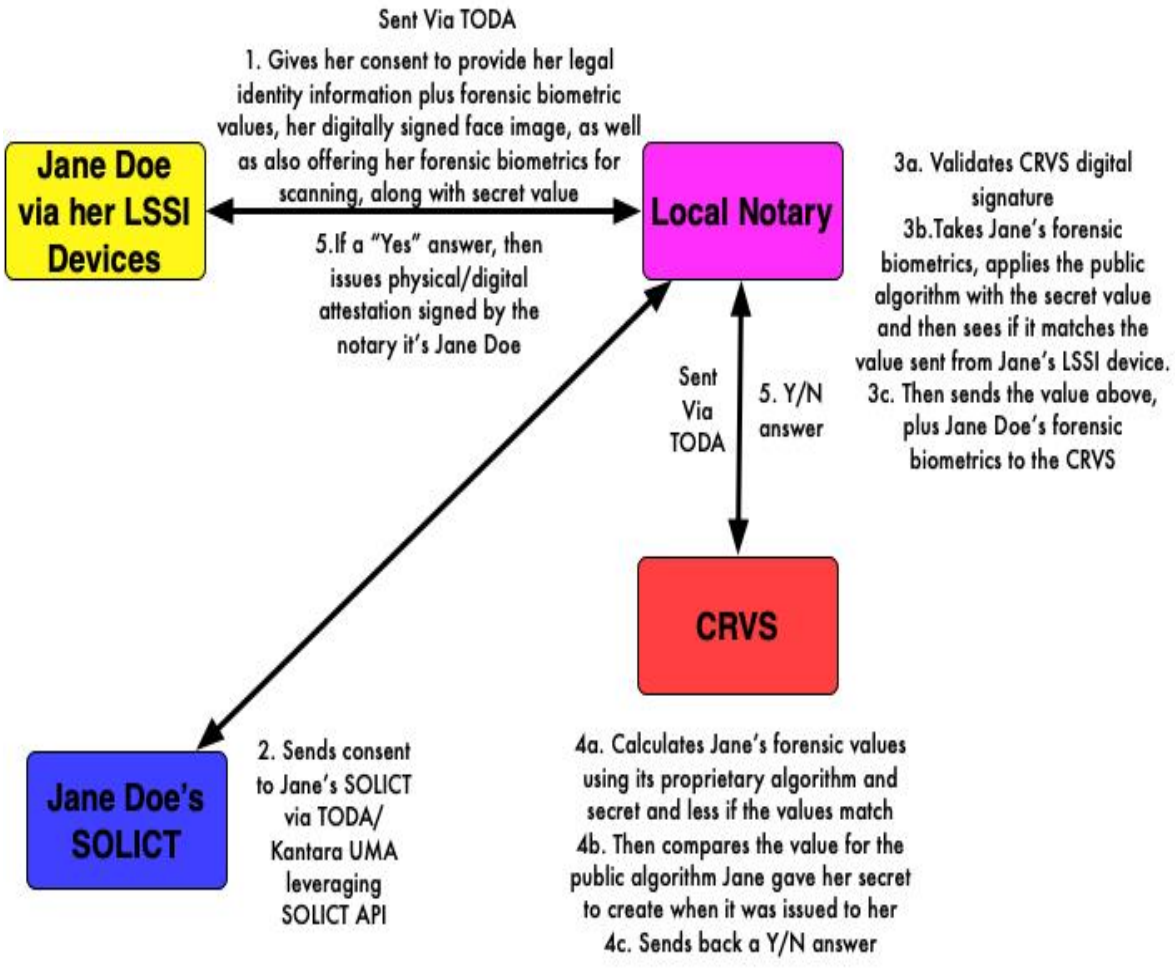
Note: For the above the third party optionally could make a quick electronic trip to validate the digital signature sent by the CRVS.

Step 5: High Identity Assurance it's Jane

If the party wants an even higher level of assurance, it's Jane, it can ask Jane to go to a local notary. This entity can obtain, with Jane's permission, her forensic biometrics, plus her secret. It will then do the following:

- Calculate, using the public algorithm, the value of her biometrics and compare this to the one on the card
- Send the biometrics to the CRVS plus her value from her calculated biometrics using the public algorithm
- The CRVS then calculates Jane's biometrics using their own secret value, compares it to the one in the CRVS system, then compares the value sent by the notary for Jane's secret value. If both match up, there's now a very high degree of assurance it's Jane Doe

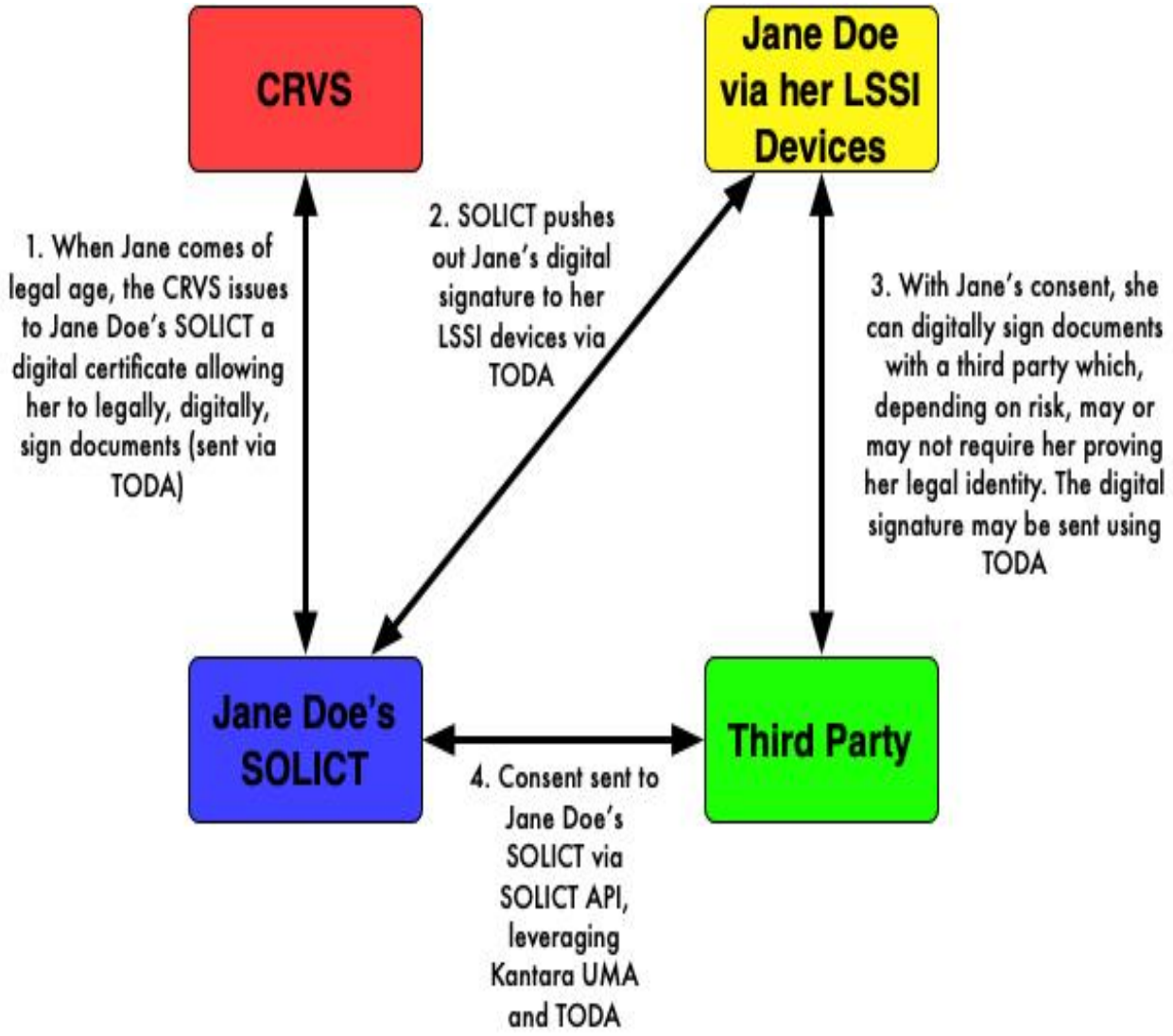
Step 5: High Assurance Proof It's Jane Doe



Step 6: Jane Digitally Signs Documents

When Jane comes of legal age, the local CRVS jurisdiction would issue her, via her SOLICT, a government issued certificate allowing her to legally sign documents. Jane's SOLICT then pushes this out to her LSSI devices. Now Jane Doe can legally sign documents. The third party may accept her digital signature or, depending on risk, also require her to prove her legal identity.

Step 6. Jane Digitally Signs Documents



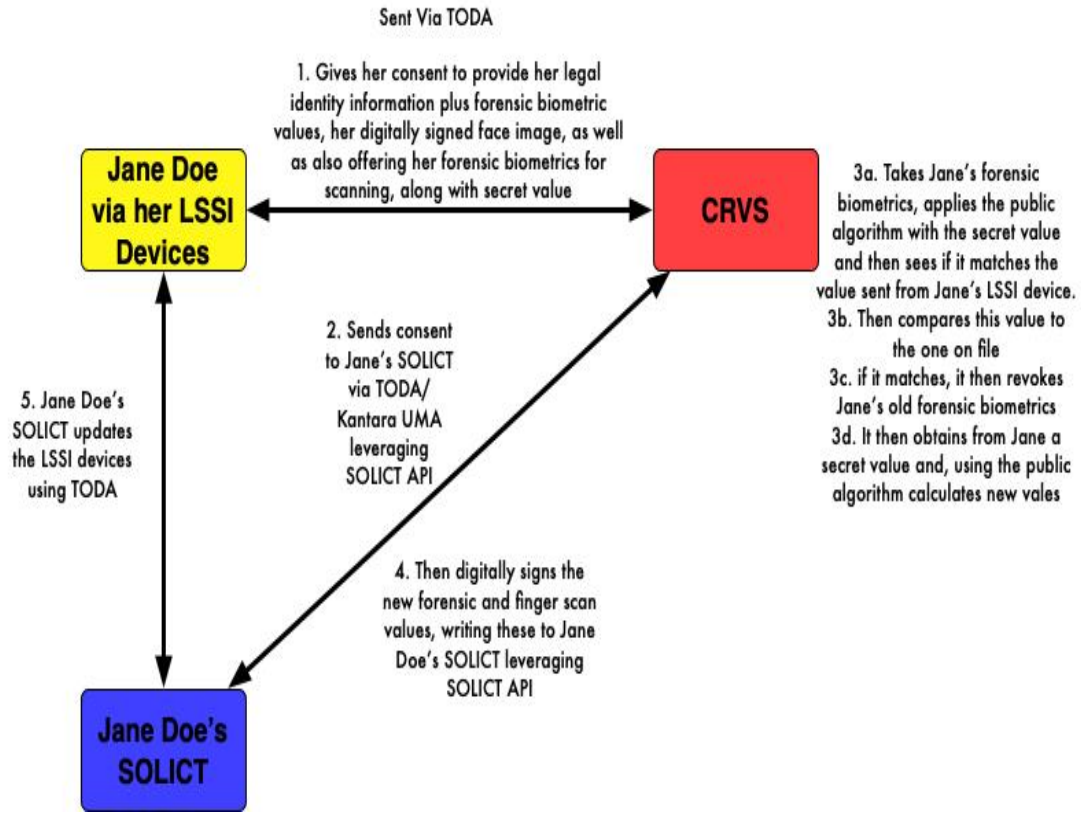
Step 7: Revoking and Reissuing Jane's Biometrics

If Jane Doe's biometrics are maliciously obtained, when Jane realizes this, she can go to the local CRVS. The CRVS would:

- Prove her identity as above
- Assuming it matches, the CRVS would then revoke Jane's old biometric value it issued to her SOLICT
- Obtain a new secret from Jane and calculate a new biometric value
- Digitally sign this, and write it to her SOLICT
- Jane's SOLICT in turn updates her LSSI devices
- Jane is now once again in control of her biometrics and legal identity
- The old values won't work when criminals try to use them

This is used in this article, "[An Identity Day in the Life of Jane Doe]".

Step 7: Revoking and Reissuing Jane's Biometrics



Note: If Rud's ideas won't work, then the CRVS would cancel its digital signature used for Jane's biometrics and use a different digital signature to resign them, which is written to Jane's SOLICT

All the above is privacy by design.

Vision - Core Smart Digital Identities of Us

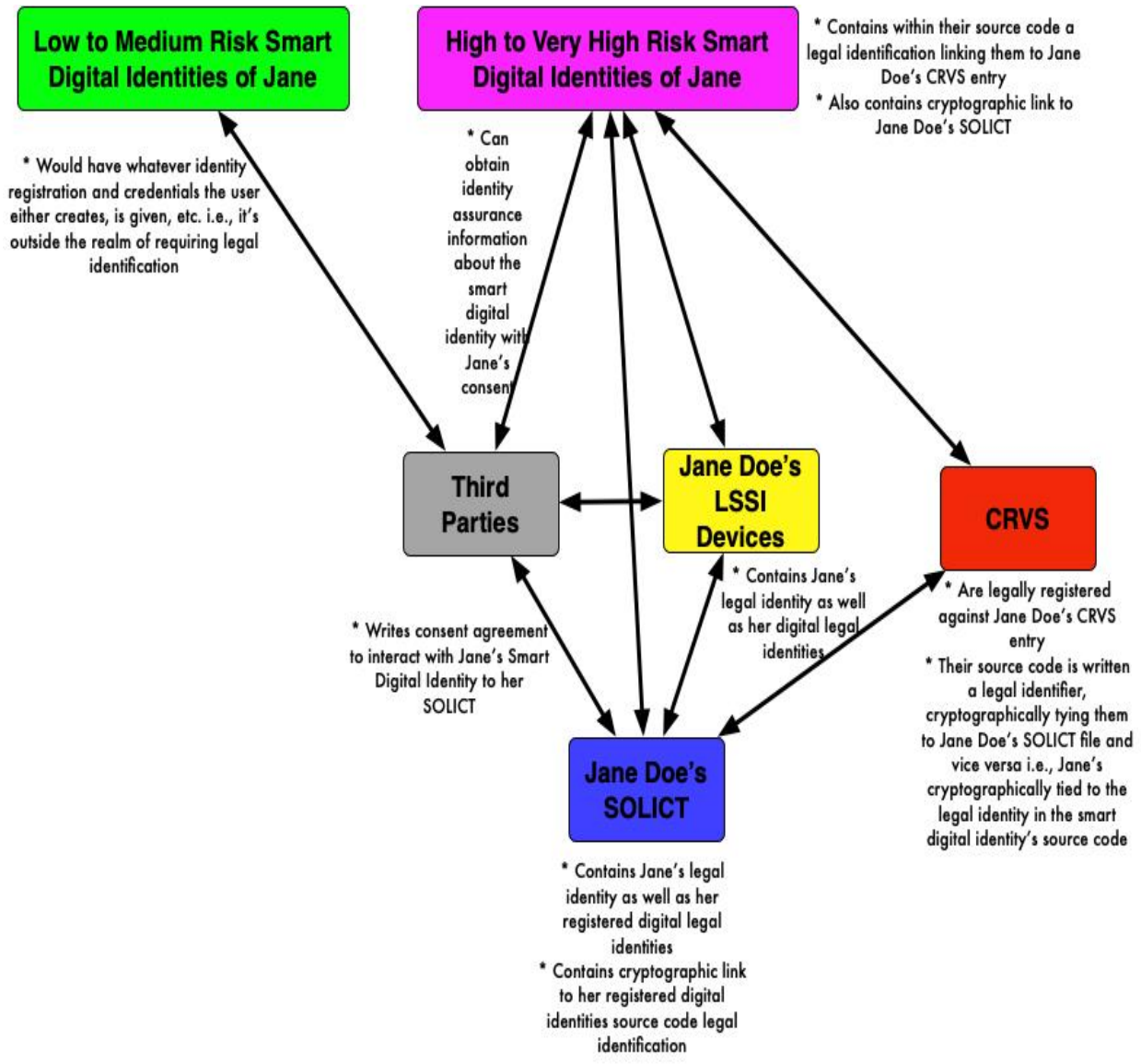
Background:

I strongly suggest readers skim these articles before reading on:

- "**AI Leveraged Smart Digital Identities of Us**"
- "**Kids & Digital Identities**"
- "**Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy**"
- "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**"
- "**The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom**"
- "**Digital Identities, Risk, Insurance & Death**"
- "**Digital Twins, Virtual Selves, Identity, Security & Death**"

Bottom line – We're rapidly creating increasingly smart digital versions of ourselves, which can make decisions on our behalf, and live on long after we've died. This brings with it a requirement, where risk warrants it, to legally tie these entities to our legal physical identity within the CRVS. As the next diagram depicts, the interaction between these entities, third parties and us is potentially complex.

Smart Digital Identities of Us Vision:



Note: Not included in this diagram is the potential use of Jane Doe's PIAM to manage, on her behalf, her smart digital identities, and their interaction with third parties.

Vision - Core AI Systems/Bots Legal Identity

Background:

I strongly suggest the reader skim these articles and documents prior to reading this doc:

- **"The Challenge with AI & Bots - Determining Friend From Foe"**
- **"A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings"**
- **"Legal Identity Vs. Legal Personhood"**
- "Decentralized AI – Risks, Legal Identity, Consent & Privacy"

Major Challenges:

As noted in "A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings" determining exactly how a legal identification can be securely inserted into an AI system/bots source code is not trivial. There's:

- Different programming languages
- Sub-second speeds to validate and/or write a new legal unique identifier to the underlying source code
- Security implications of writing to the underlying source code such that it can't be easily manipulated
- Standards to be used
- Constantly changing these standards based on new rapidly emerging attack vectors caused by this curve
- Significant performance concerns given the rate of legal identity creation of AI systems and bots i.e., hundreds of thousands to millions or more per second
- Significant security concerns about Evil Inc.'s and malicious states doing denial of service type attacks on the CRVS by overloading the systems with AI system and bot legal identity registrations and/or validation lookups
- Electricity and system availability as CRVS systems operate in real time 24x7x365 (skim "**When Our Digital Legal Identity Trust Goes Poof!**" and "**AI Power Consumption Exploding**"
- Etc.

Years ago, I realized:

- **Writing to the source code was the main stumbling block to creating legal identities or AI systems and bots**
- **Followed by political challenges in being able to let local jurisdictions keep control of their legal identity laws**
- **Followed by security challenges in keeping it all up to date as the tech change curve rapidly increased and addressing performance/denial of service type attacks**
- **Followed by AI power consumption**

Vision:

Coding

In the cost architecture I created a separate cost centre titled, "**AI/Bots Writing to Source Code Legal Identity/Credential Registration Subcomponent Costs**". This assembles the best and brightest coders, business process, security, and legal experts to come up with a solution framework. It might require a new programming language.

Security

The new global, independent, well-funded non-profit's job is to do 24x7x365 threat analysis against the entire legal identity framework including writing to the source code.

API's

The cost architecture has a separate cost centre titled, "**API**". This addresses the problem of being able to quickly, securely access the legal identifiers.

Standard CRVS Systems

Legal identities of AI systems and bots is managed by the new age CRVS system to new global standards. Thus, it still allows local state/provincial jurisdictions to keep control but integrate into the global system operating at what I call "warp speed".

Performance & Security

The design teams MUST address the security challenges outlined above, proven out by lots of testing. Then the non-profit must continually evaluate risks from new types of attacks including new denial of service type attacks.

Electricity& System Availability

The new CRVS systems must be designed for at a minimum 99.999% availability and have enough power supplies to operate at high load demands. It also must be able to withstand sun GMD (geomagnetic disturbance) EMP (electromagnetic pulse) and HEMP (high altitude electromagnetic pulse) events.

Summary

There's lots of new ground to be broken in creating the new age AI system/bot legal identity system. As shown above, it's complex.

Vision – Rethinking CRVS (Civil Registration Vital Statistics) Systems

Background:

As described in Problem #1 in "**Legal Identity Problem Statements**" the current CRVS systems are totally antiquated. Problem #2 shows the whopper sized hundreds of billions of dollar costs around the planet from crappy legal identity systems.

The largest challenge with rethinking old CRVS systems isn't technical. It's political. As stated in problem #1, legal identity is frequently managed at the local state/provincial level. Thus, there are literally hundreds of such jurisdictions on the planet, each wanting to keep control of their legal identity laws and regulations. Thus, I realized any new architecture must allow for local control while plugging into a global system.

The arrival of AI systems and bots (both physical and digital) when risk rises, also requires legal identity registration. Skim these three articles:

- "**AI Leveraged Smart Digital Identities of Us**"
- "**New AI Laws & Regulations Requires Legal Identities**"
- "**AI & Governments**"

Then there's this tech change curve to consider. Hypothetically, it means EACH HOUR/DAY, new attack vectors are being created against not only the tech used in legal identity, but also the governance, business processes and end users (be they human, AI systems or bots). I realized most jurisdictions don't have the resources, expertise, or budgets to continually address this. Thus, this too must be addressed in any new CRVS architecture.

CRVS Vision:

The CRVS legal identity architecture for humans and AI systems/bots laid out in these two docs shows how all the above challenges are addressed:

Humans:

- "**Rethinking Human Legal Identity**"

AI Systems/Bots:

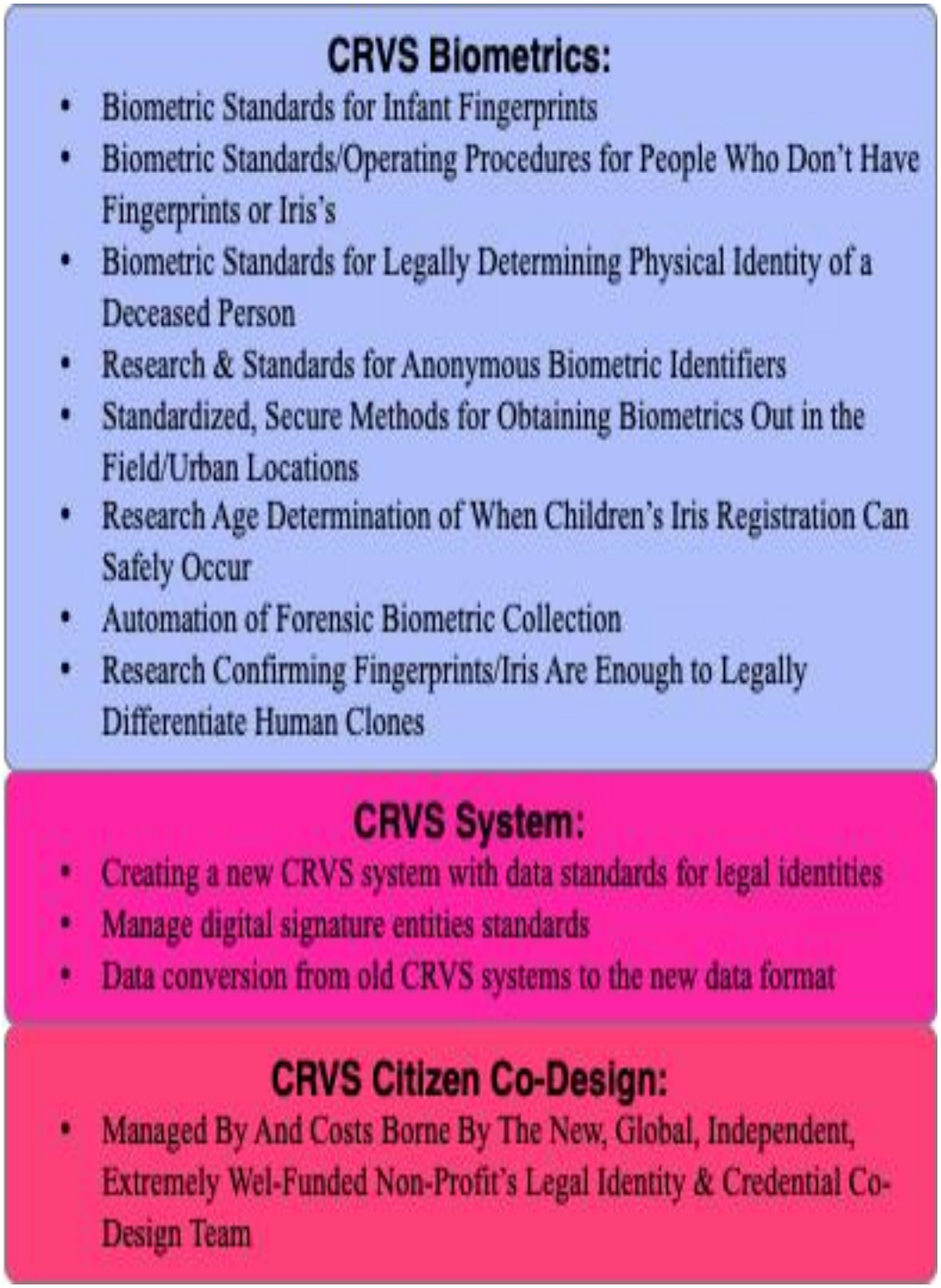
- "**Creating AI Systems/Bots Legal Identity Framework**"

The CRVS is built to new global legal identity standards, overseen by the new, global, well-funded, independent non-profit.

One of its jobs is to do 24x7x365 threat analysis against the legal identity tech, governance, business processes, and end users. A high threat must be responded to by governments, companies, enterprises, and entities within hours. Thus, this brings current industry best practices to the world of legal identity.

CRVS High-level Cost Centre & Subcomponent Architecture Diagrams:

You'll see it's complex, requiring lots of different subcomponent cost centres.



Smart Digital Identities of Us:

- API
- PIAM
- TODA LSSI
- Smart Digital Identities Co-Design Interface For Humans
- SOLICT
- Smart Digital Identities Legal Identity Relationships Including Hives
- Smart Digital Identities Legal Authorization Rights
- Authoritative Credentials Source
- Smart Digital Identities Legal Identity & Credential Written To Source Code

AI Systems/Bots:

- AI Systems/Bots API
- AI Systems/Bots PIAM
- AI Systems/Bots TODA LSSI
- AI Systems//Bots SOLICT
- AI Systems/Bots Authorization Rights
- AI Systems/Bots Legal Identity & Hive Relationships
- Writing To The Source Code Legal Identifiers & Credentials
- Authoritative Credentials Source
- CRVS
- AI Systems/Bots Both Digital And Physical)

Legal Identity & Hive Relationships:

- SOLICT/LSSI Devices API
- PIAM Consent Agreements/Contracts With Third Parties
- SOLICT to LSSI Devices Via TODA File
- Legal Identity & Hive Relationships Co-Design
- SOLICT Stores Legal Identity Relationships
- Transfer to SOLICT via Digitally Signed TODA file
- Graph Databases Store Relationships Cross-Linking Between Different Entities
- Legal Identity Hive Relationship Standards
- Authoritative Data Source CRVS

Authorization Rights:

- SOLICT/LSSI Devices API
- PIAM Manages Legal Authorization Rights
- Transfer from SOLICT To LSSI Via TODA File
- Co-Design Standards For Accessing Authorization Rights
- Transfer via TODA from CRVS to SOLICT
- Digital Signature Signing Of Authorization Rights
- Legal Authorization Rights Standards

CRVS API:

- API Gateway
- Audit Trail
- API IAM (Identity Access Management)
- API Clients Internal/External
- API Backend
- API Applications/API Rules
- API Co-Design
- CRVS Authoritative Sources Databases

CRVS Data Centres:

- Electrical Supply/Consumption Plan and Processes
- Sun EMP/HEMP Event Plan/Processes
- Physical/Cyber Security Management/Processes
- Disaster Recovery Plan
- Backup Strategy/Processes
- Processes Updating Servers/Apps/Network
- Servers (Physical & Cloud)/Data/Network
- Availability - 99.999%

CRVS Governance Laws/Regulations:

- Co-Design Standards For Citizens Wanting To Interact With Their CRVS Department
- Ability For CRVS to Digitally Sign Legal Identity Information
- Ability For CRVS To Send Legal Identity To SOLICT Via TODA
- Biometric Standards Used In Human Legal Identities
- Standards For Human Legal Identities Registered In CRVS
- Standards For AI Leveraged Smart Digital Identities Of Humans Registered In CRVS
- Standards For AI Systems And Bots Legal Identity Registration
- Standards For Legal Identity/Hive Relationships Stored Within CRVS
- Standards For Legal Authorization Issued By CRVS
- Security Standards For The CRVS System
- Archival Period For An Entity's Records
- Management Abilities To Access The CRVS System
- Notaries Abilities To Access The CRVS System
- Abilities Of CRVS To Query All Other CRVS Systems
- Specify Actions From Threat Responses Issued By The Non-Profit
- Notification Systems For Events Like death, Etc.
- Availability Of The CRVS System

Global, Independent, Non Profit:

- Manages API Standards
- 24x7x365 Threat Assessments
- Manages Notary Standards For Legal Identity & Credentials
- Manages PIAM Standards
- Manages LSSI Device Standards
- Manages SOLICT Databases
- Manages SOLICT Standards
- Manages Credential Issuance Standards
- Manages Legal Authorization Standards
- Legal Identity & Credential Co-Design Team
- Manages Legal Identity Hive Relationships Standards
- Licenses CRVS Software To Jurisdictions & Credential Issuance Standards to Credential Bodies
- EMP/HEMP Power Supply
- Manages CRVS Software/System
- Manages Digital Signature Entity Standards
- Manages Legal Identity Standards For Humans, AI Systems and Bots
- Governance Co-ordination/Advisory

Vision - Common Credential Issuance Standards

Background:

Today, on the planet, there are literally thousands of credential bodies, each doing "their own credential issuance thing". I realized while creating the architecture, each body is still going to want to be in control. **HOWEVER, I ALSO REALIZED THEY WERE INCREASINGLY VULNERABLE TO ATTACKS CAUSED BY THIS CURVE AGAINST THE CREDENTIALS.**

Skim this, "**Verifiable Credentials For Humans and AI Systems/Bots**".

Credential Vision:

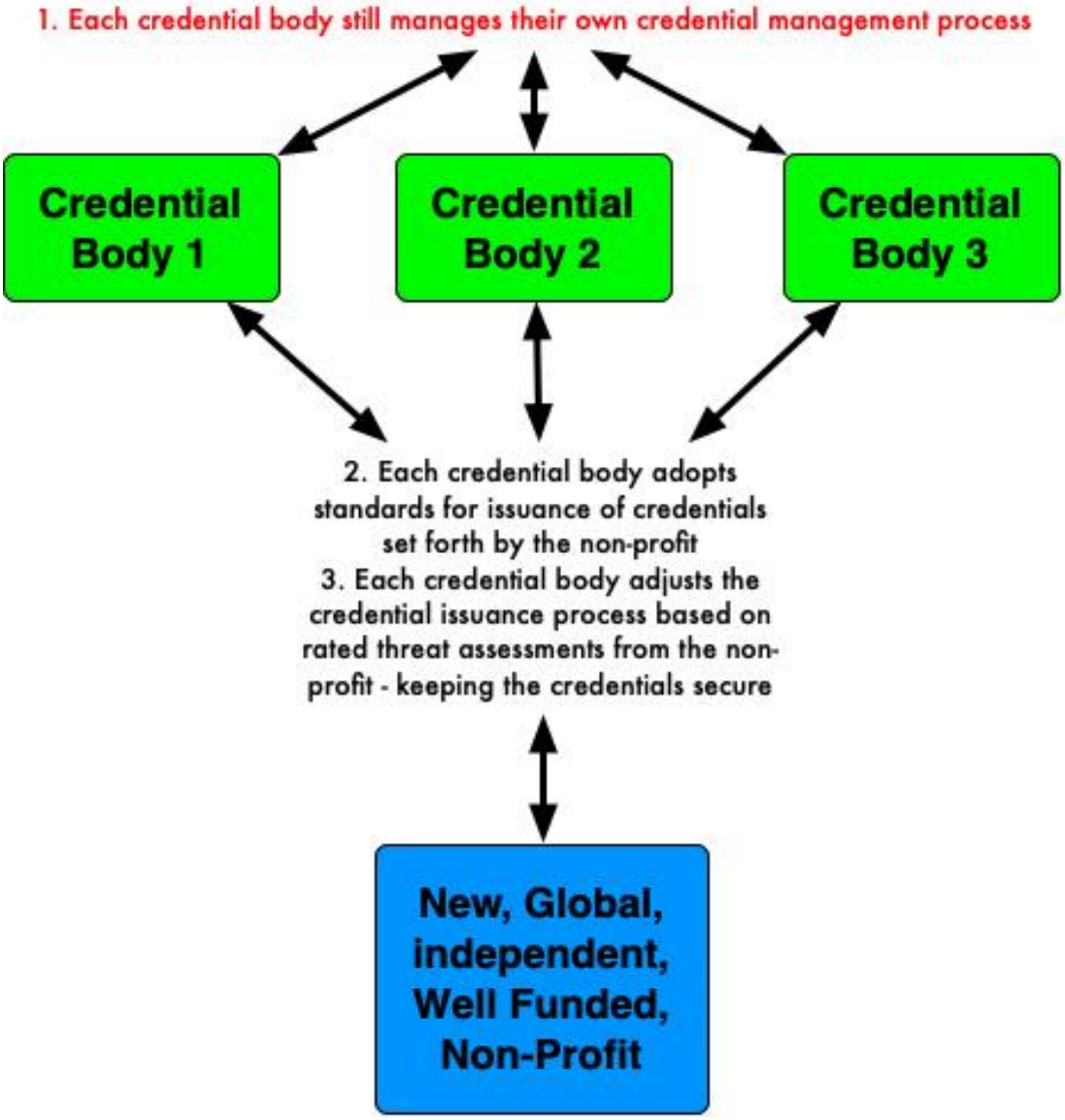
Thus, I architected the new, global, independent, well-funded, non-profit, to take over standards and threat assessments against the actual credential issuing process (**NOT THE ACTUAL CREDENTIAL MANAGEMENT PROCESS EACH CREDENTIAL BODY WANTS TO PROTECT**). **Thus, it's politically palatable for the credential bodies**.

They'd have to:

- Adopt the credential issuance standards set forth by the non-profit
- Update it based on risk threat assessments from the non-profit

The result? People, AI systems and bots, companies, governments, and enterprises, have strong confidence in their credentials both physically and digitally. Credential issuance bodies can still manage their own credential processes.

Credential Example: Global, Independent, Well Funded Non-Profit and Credential Authorities



Vision: Proving Legal Identity Relationships and Hives

Background:

Today on the planet we use antiquated paper-based systems to prove legal identity relationships like:

- Parent/child
- Legal guardian/child
- Power of attorney/person
- Etc.

These are easily frauded and don't work locally/globally digitally. It's a mess. Skim this, "**Legal Identity Relationships**".

Add to this the arrival of "hives". To see an example of a "bot hive" watch this video. Here's the coming challenge. Hypothetically, Jane Doe:

- Via one or more of her AI leveraged, smart digital identities could belong to a hive
- Which one or several AI systems might also belong to
- Along with one or more digital bots
- With one or more physical bots
- Along with one or more IoT devices

Where the risk warrants it, the hive will require legal identification as well as legally identifying its members. Here's the next challenge:

- Members of the hive might come and go in seconds, minutes, hours, days, weeks, months, or years
- To see an example of what's coming skim this article about nanobots, "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**"

Vision:

When architecting this, my vision was to leverage new toolkits allowing:

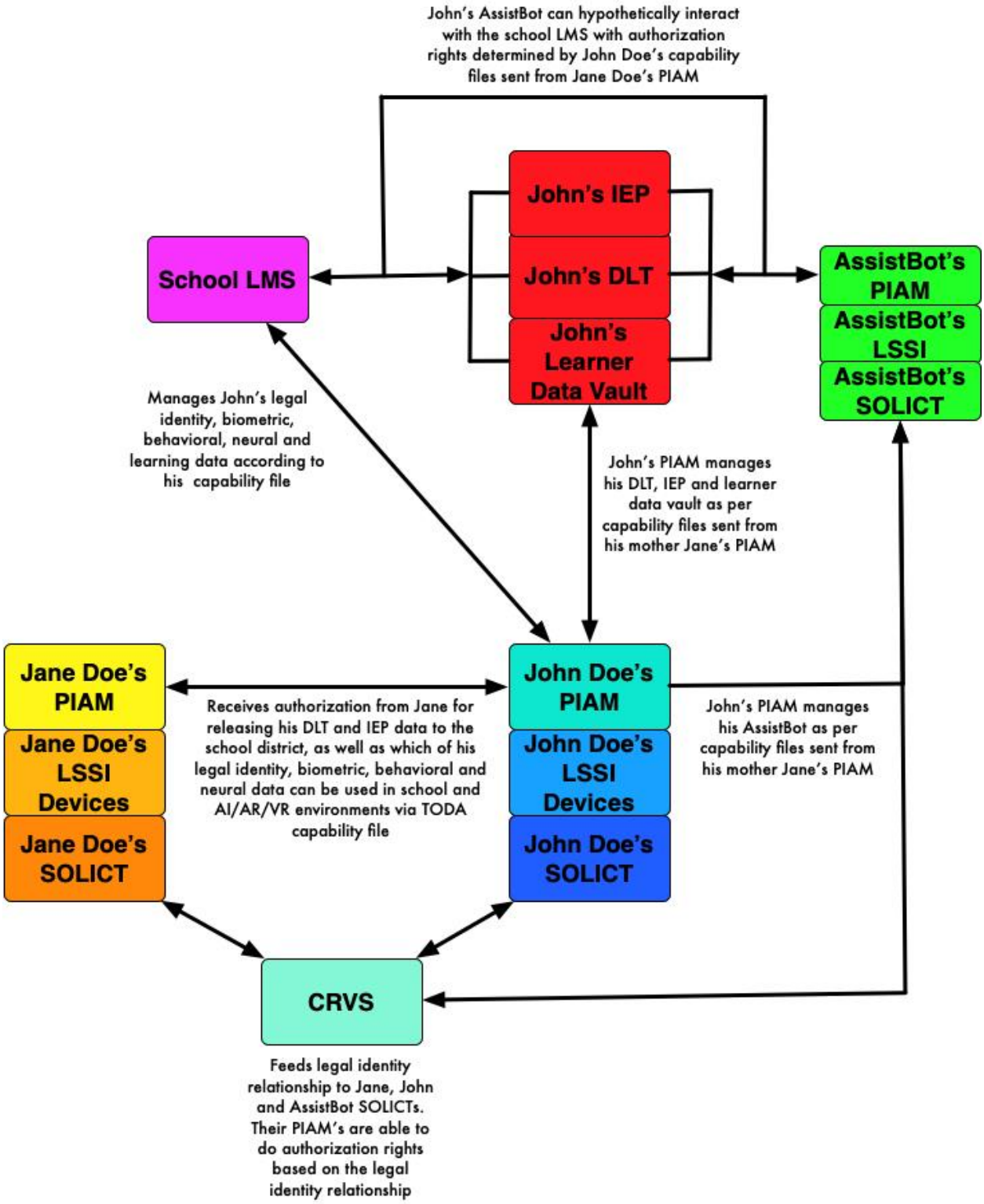
- CRVS to leverage Graph based databases to rapidly manage complex, fast changing entity relationships
- TODA to send to the entity's SOLICT and on to their LSSI devices, the legal identity relationships, such that the entity could now manage, on their own, who they'd release the hive relationship to.

I strongly recommend readers read "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

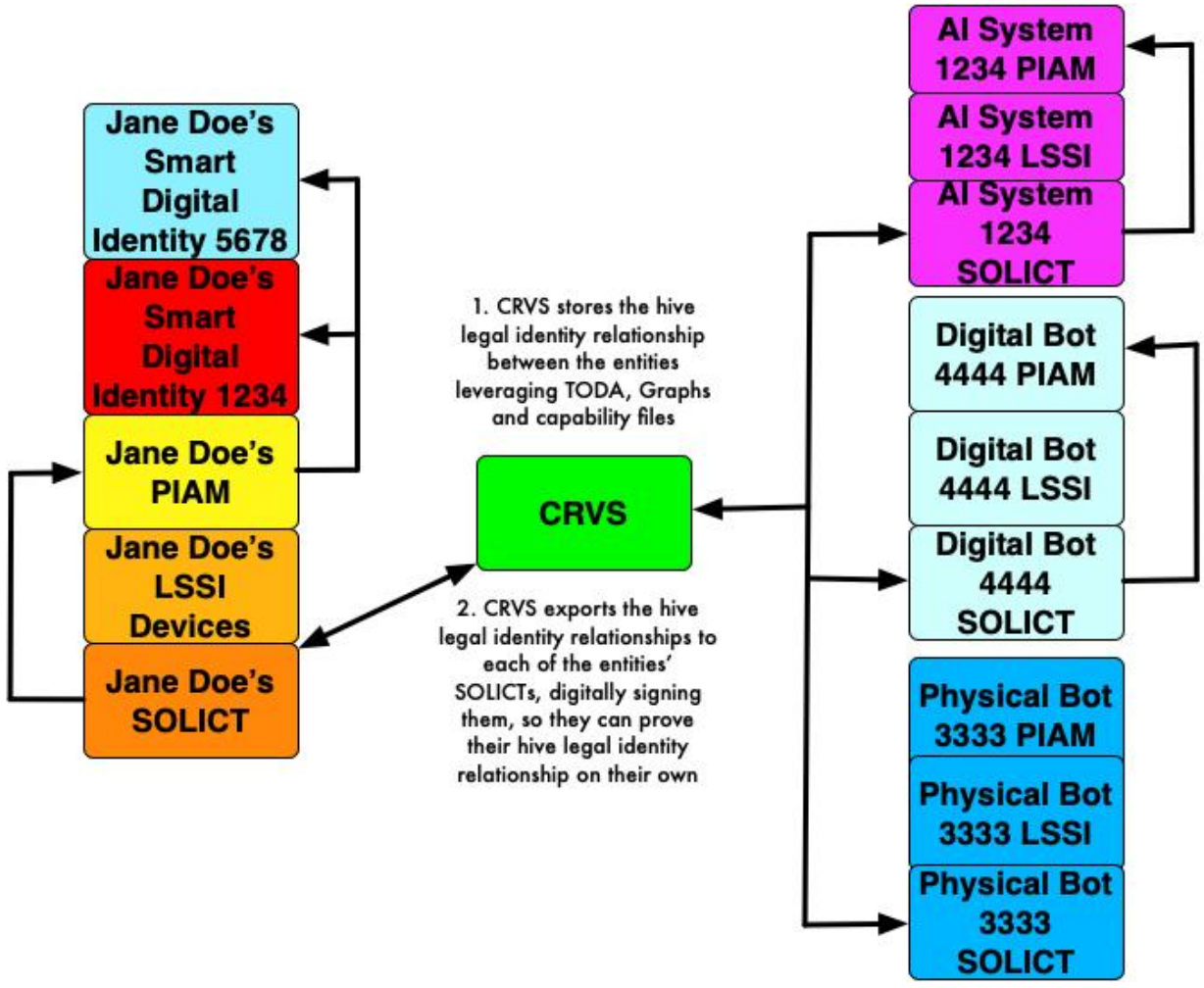
The Legal Identity Relationship and Hives Cost Centre can be found here. Legal identity/hive relationships standards are managed by the non-profit.

Here's two examples of the "legal identity/ hive relationship vision":

Examples: Proving Legal Identity & Hive Relationships:



Hive Legal Identity Relationships:



Vision: Authorization Rights

Background:

Skim these two articles on AI/AR/VR environments in a global classroom:

- "**Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy**" -
- "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**"

It has a student, John Doe, who has his learning assistant bot "AssistBot", with a human teacher, Sally Goodteacher, and two teaching assistant bots, BobBot and PattyBot. Further, authorization contracts need to be created:

- Between not only John's parent Jane Doe, for him and his AssistBot with the school district
- But also, with school districts creating the AI/VR global learning environment
- All specifying what legal identity data can be used by Sally Goodteacher, BobBot, PattyBot and AssistBot
- Also specifying how the data is used, stored, shared, archived, and terminated

So, a human, or an AI system, physical and/or digital bots will require authorization rights, which depending on risk, must be spelled out in contracts. My dumb question is how will this be done in a secure, scalable manner?

Which led me to a protocol called TODA, to rethink how not only contracts are sent from one party to another, but also to begin to create authorization rights standards, leveraging TODA capability files. Skim this article "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

.

The suggested strategy is to only focus on legal identity authorization like:

- Parent, like Jane Doe, being authorized by the CRVS to manage a child's legal identity like John Doe
- A human, like Jane Doe, being authorized by the CRVS, to manage an AI system of bot's legal identity, like AssistBot

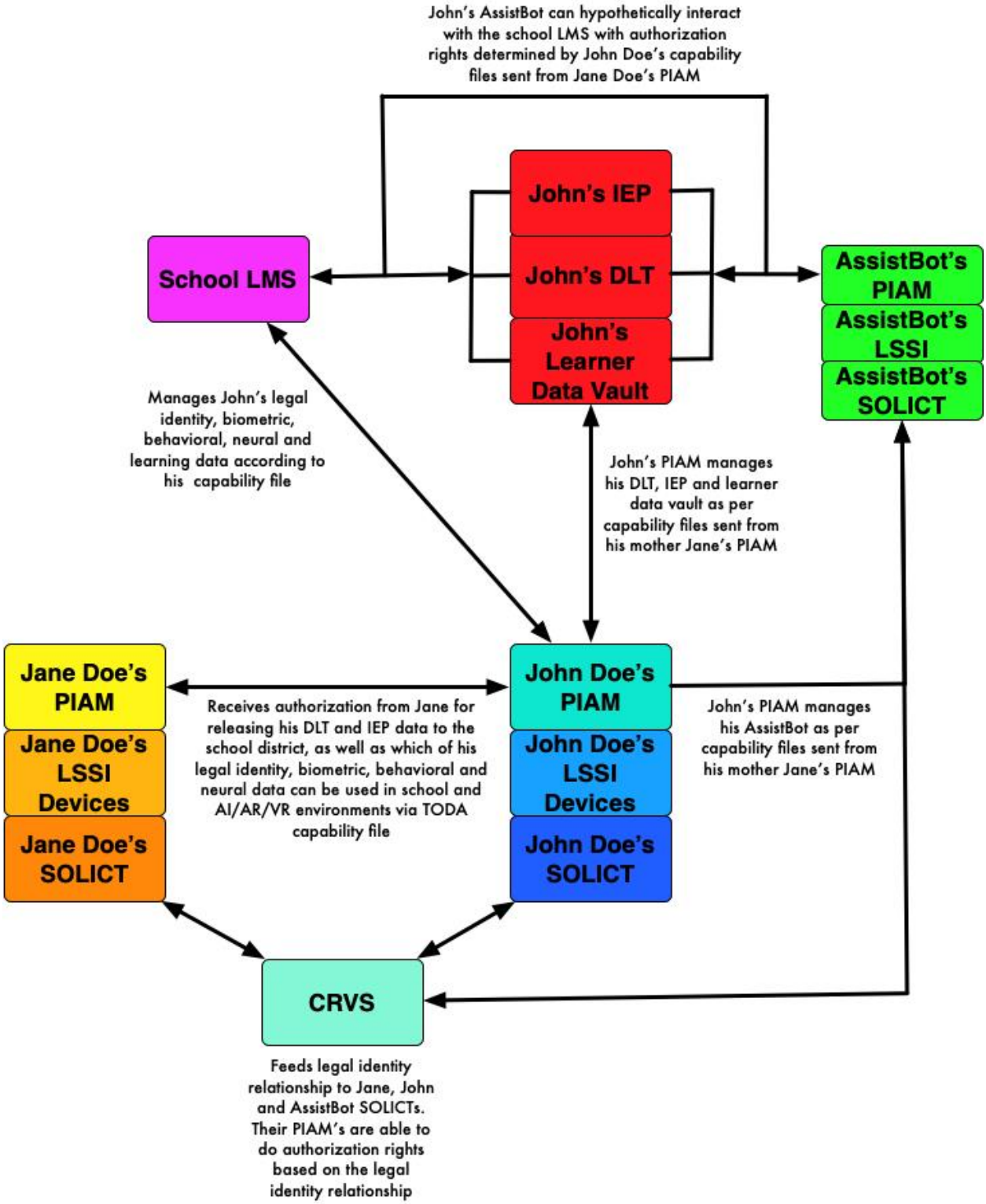
If an Evil Inc. leverages this tech change curve, they can potentially gain access to an entity's authorization rights, with which they can create havoc.

Thus, it requires the global, non-profit to do two things:

- **Continually do threat analysis against the authorization standards and API**
- **Continually update the authorization standards based on threat analysis**

Here's the link to the Authorization Cost Centre. Here's **the link to the non-profit's Authorization Standards Cost Centre**.

Authorization Example:



Vision: SOLICT (Source of Legal Identity & Credential Truth)

Background:

Let's hypothetically say a malicious state wants to target Jane Doe. They could delete her CRVS entry, her national ID entries, etc. Jane would effectively be screwed in proving she's Jane Doe. The same applies to AI systems and bots entities legal identities.

My premise? As the planet madly digitizes, it gives malicious governments the ability to remove us from their databases, thus effectively screwing us in proving who we are. It also gives Evil Inc.'s of the planet new toolkits to use to cause us "digital death". Skim these:

- "**Death & Digital Identity**"
- "**Kids, Death & Digital Identities**"

Then, there's the issue of where we store all our consents. In this rapidly digitizing planet, how will Jane Doe be able to prove on X date, at Y time, she gave Z consent for her legal identity, credentials and personal biometric/neurodata to be released? She'll literally have thousands or tens of thousands of them from when she was born to her death.

Vision:

The SOLICT, a database each of us managed, exists outside a jurisdiction's control. Thus, Jane could hypothetically go to a local notary outside the jurisdiction and prove her legal identity as in **Step 5 High Identity Assurance Proof**..

When the notary can't find her on the CRVS system, a different business process would kick in. Jane would have to apply to the global, independent, non-profit, via the notary, to confirm the validity of her SOLICT. This would involve the non-profit checking the dates when the local jurisdiction created Jane Doe's legal identity and confirming it, via the Toda file, a secret value they wrote to her SOLICT file, within the SOLICT. Assuming it passes, then the local notary could write a physical and digital attestation it's Jane Doe.

The SOLICT also acts as a repository for all her consents from cradle to grave. This then gives Jane the ability, if she lives in a jurisdiction like the EU, to enact **GDPR's Article 17, "Right to be Forgotten'**, requesting removal from the database.

Note however, introducing SOLICT brings with it new whopper sized challenges. **Read the SOLICT Cost Centre section of this document** to learn my concerns about performance and security.

The **SOLICT operates to global standards set forth by the global, non-profit**. The **SOLICT databases are also managed by the non-profit**.

SOLICT Examples:

Scan the above **CRVS examples**, **Credential examples**, and **Legal Identity Relationship & Hive examples** to see how SOLICT works

Vision – LSSI (Legal Self-Sovereign Identity)

Background:

Today, on the planet, it's a legal identity mess proving an entity's identity. Skim "**Legal Identity Problem Statements**."

Today, we don't control our legal identities both physically and digitally. Instead, we rely on pieces of paper issued by a government (which are easily forged and frauded). There's no way for say Jane Doe to prove her smart, AI leveraged, digital identities which are legally registered against her physical legal identity.

Then there's people, like my 94-year-old mother, who no longer has mental faculties, or young or poor people with no access to tech or don't have the means to store pieces of paper. How can they easily prove their legal identities?

Add to this the legal identities of AI systems and bots. How can they prove their own legal identities?

Finally, how can an entity legally, anonymously prove they're a human or bot? Today, on the planet, this legal identity framework doesn't exist.

All the above was in my mind while creating the new legal self-sovereign identity (LSSI) architecture.

Vision:

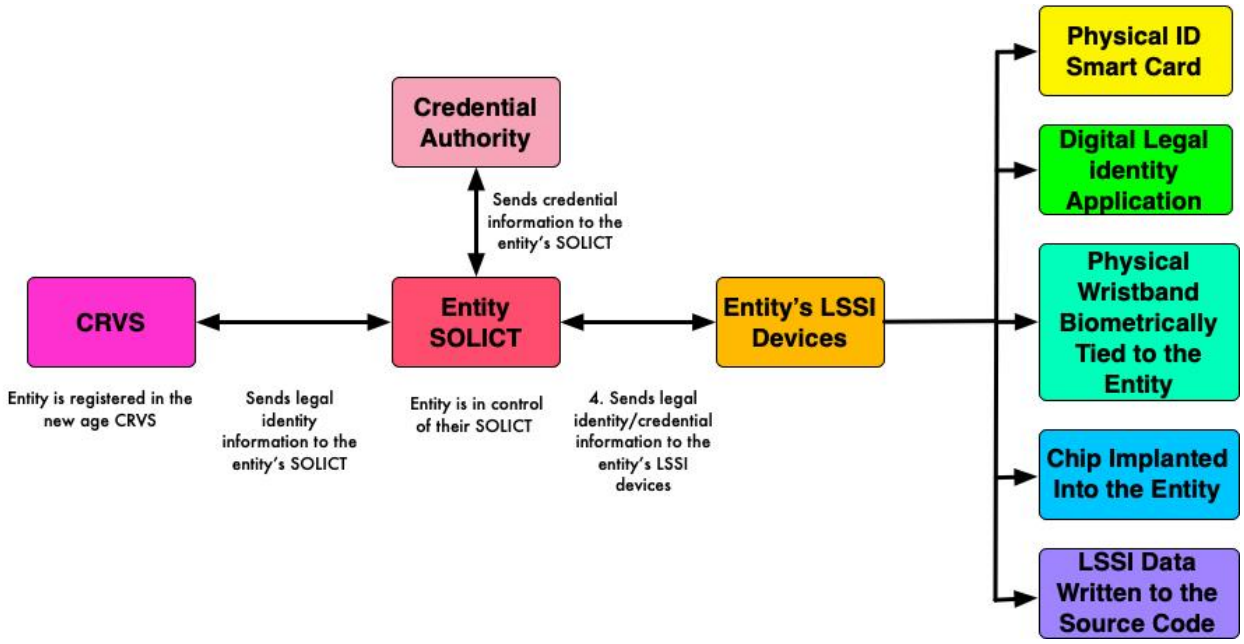
There are five different types of LSSI devices:

- Physical, smart legal identity card
- Legal identity digital application
- Physical wristband, containing the legal identity/credential information, biometrically tied to the wearer
- A chip implanted into the entity
- Writing legal identity and credential information to the source code of an entity

Thus, it meets the needs of all the above challenges. The source of truth for the LSSI device is the SOLICT. LSSI devices are fed their legal identity and credential data, from the SOLICT, via TODA files (skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" to understand TODA).

The LSSI Devices Cost Centre section can be found here. The LSSI devices **operate to global standards managed by the global, independent, non-profit**.

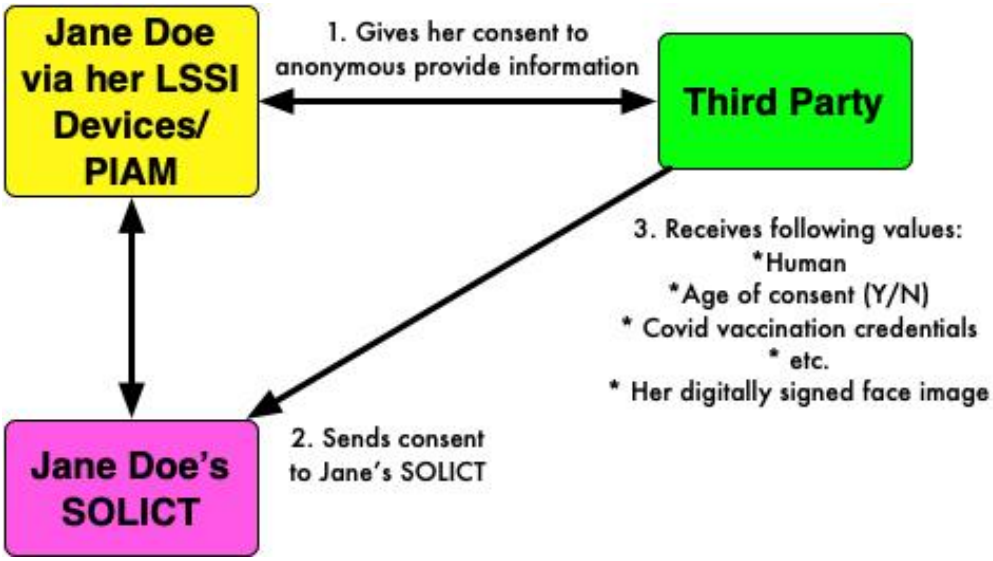
Here's a pic showing at the 100,000-foot level high level components:



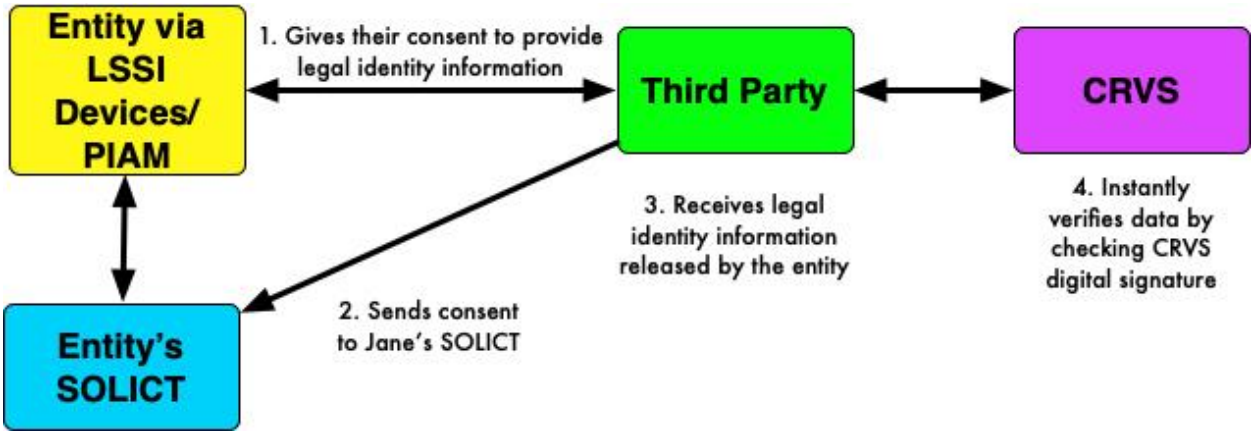
To see a day in the life article showing how Jane Doe leverages her LSSI devices skim. "**An Identity Day in the Life of Jane Doe**".

LSSI Examples:

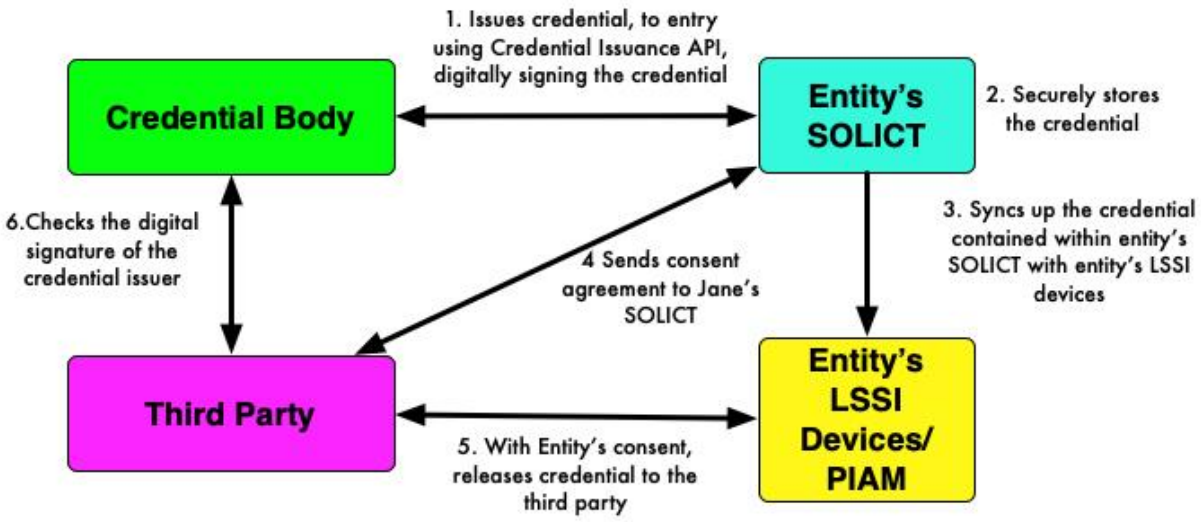
Legally, Anonymously Proving The Entity is a Human or Bot



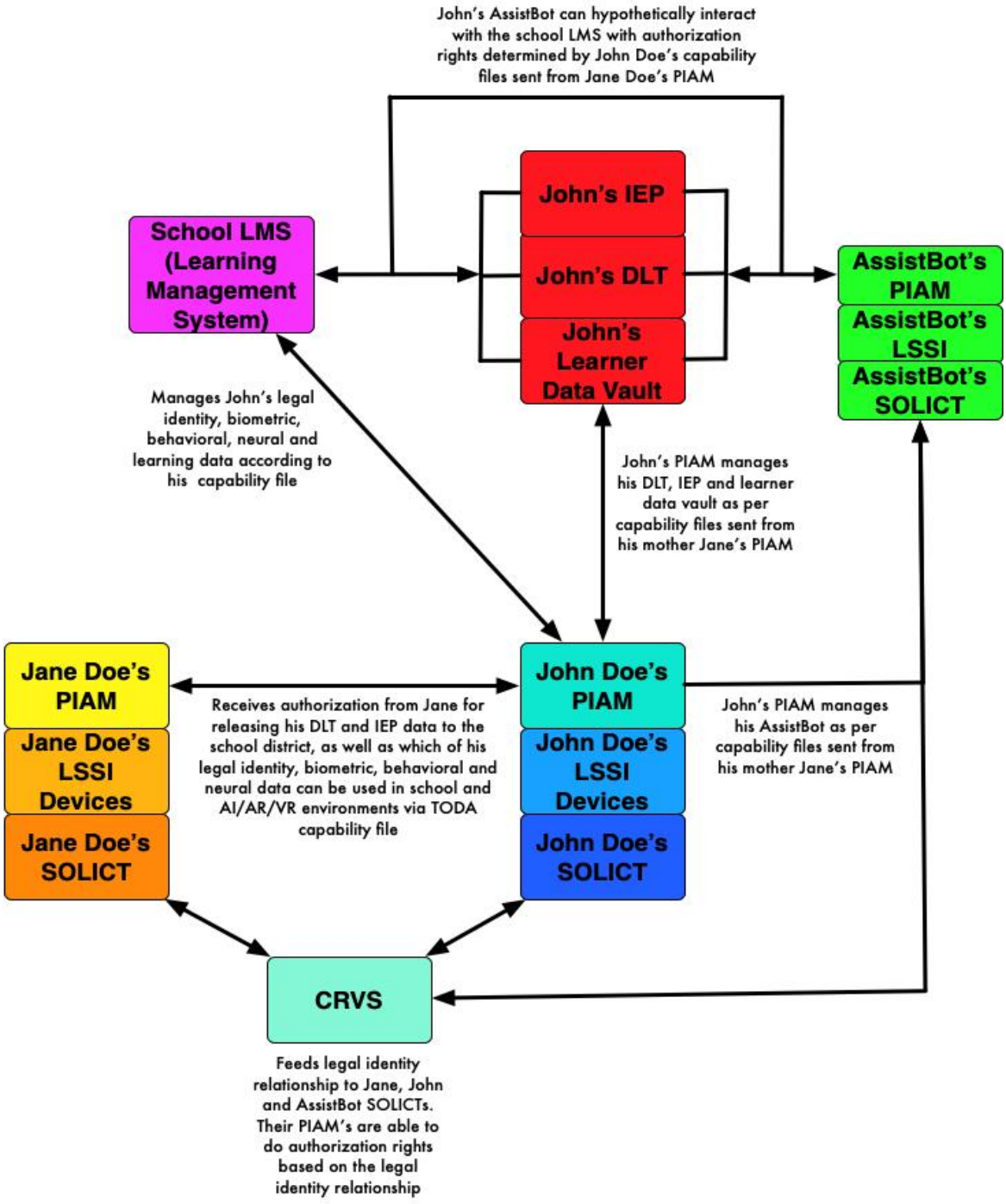
Proving An Entity's Legal Identity



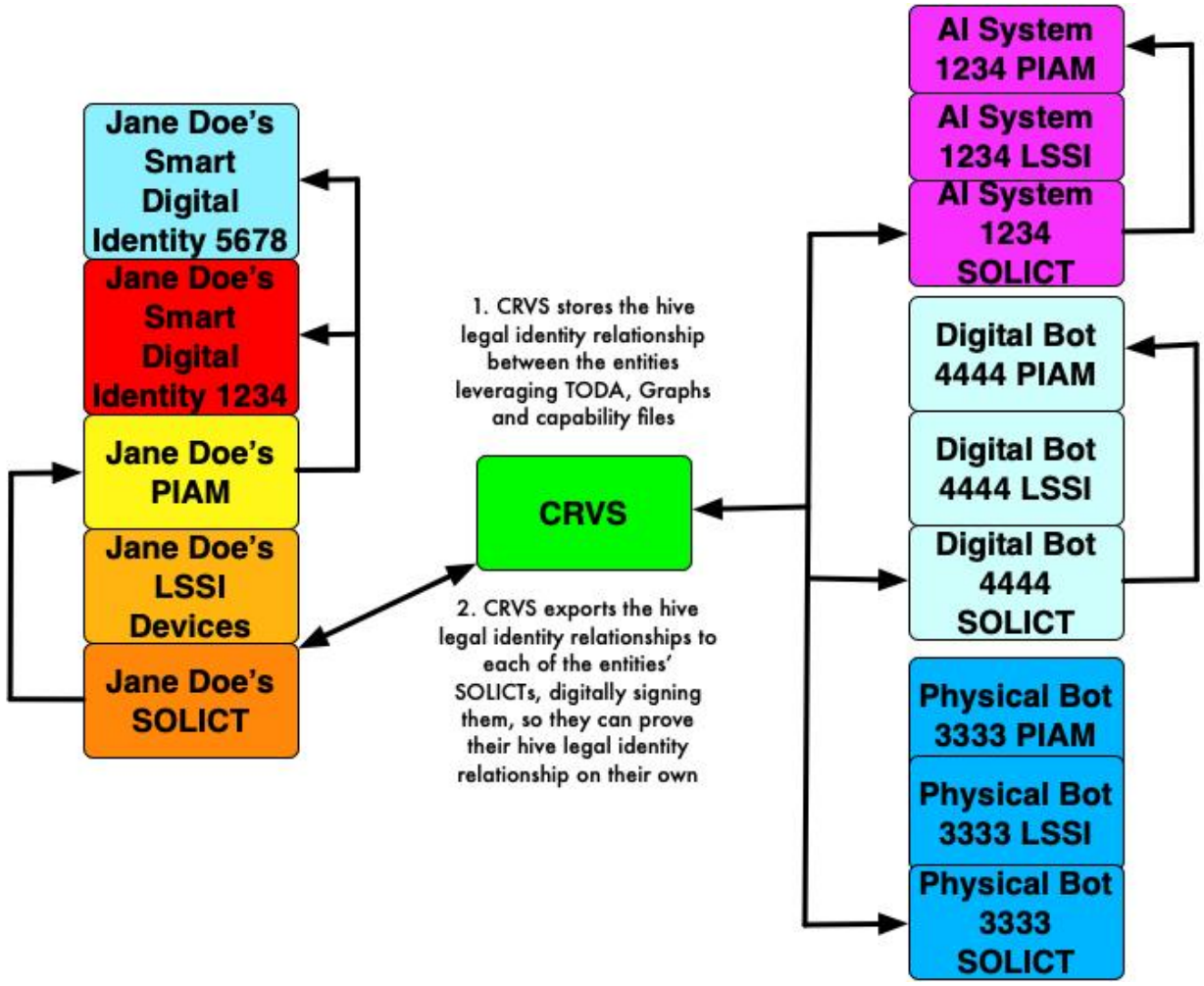
Proving An Entity's Credentials:



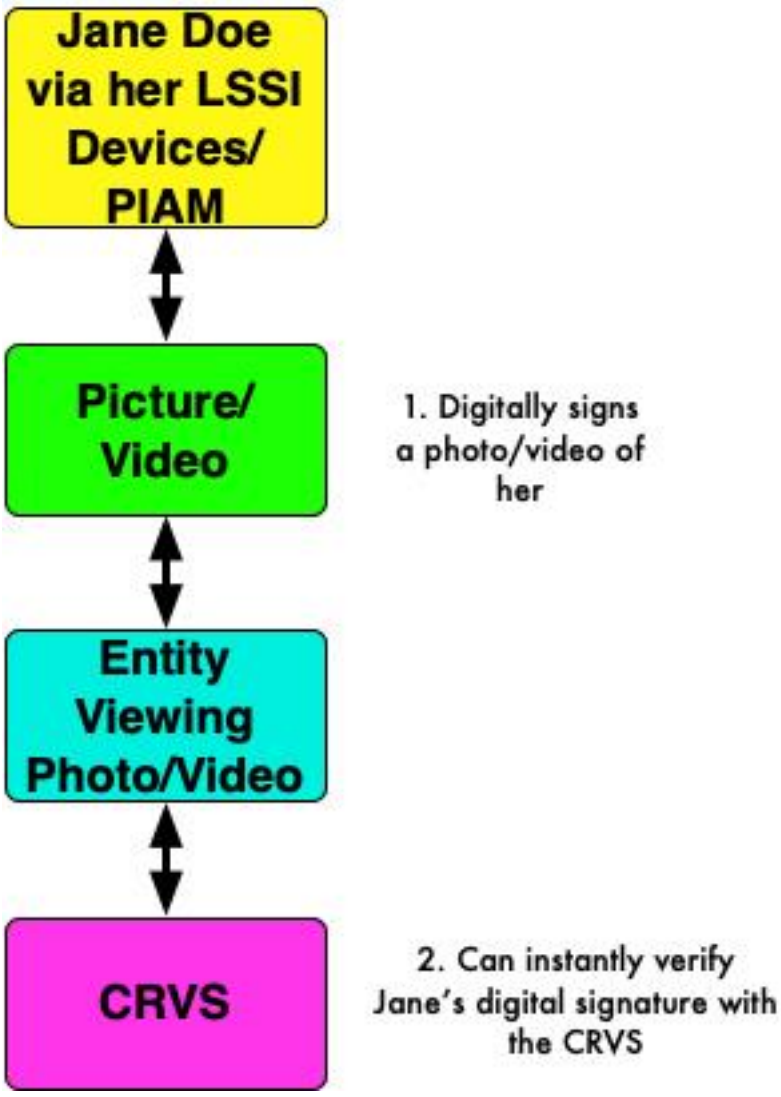
Showing Legal Identity Relationships & Giving Authorization



Proving Hive Relationships



Proving A Photo/Video of You Isn't a Deep Fake



Note: For legal minors, people who are managed by power of attorney, etc. their legal guardian can instantly digitally sign photos or videos, via their PIAMs on behalf of their kids, etc..

Vision – PIAM (Personal Identity Access Management)

Background:

In today's world, as people wear smart clothing, smart glasses, and cameras become miniaturized, simply walking down a street, a person will be rapidly identified. It creates a "very non-private world". Skim, "**Smart Cities - Contracts, Privacy, Data & Legal Identities**".

Vision:

To live privately in a non-private world requires new laws and regulations asking for our consent for our identity to be released. This in turn requires us granting our consents. Now come with Jane Doe walking down a street, wearing AI/AR glasses, where she's both in the online and offline world simultaneously. She'll likely be bombarded by requests for her to share her identity. She's not going to want to have to manually do this, which is why I created the concept of a PIAM.

It leverages AI for Jane to then pre-determine who she wants to share her legal identity and credential information to. If you skim, "**An Identity Day in the Life of Jane Doe**", you'll see how Jane's PIAM allows her to mostly live privately except with those third parties she wants to share her information with.

Now making this vision become a reality requires security standards, since the PIAM will become a prime point of attack by criminals. Further, given this curve, it means today's best security standards can quickly become tomorrow's turd. Which is why the architecture calls out for PIAM standards to be managed by the global, independent non-profit, which also does 24x7x365 threat analysis against it. Thus, the architecture constantly keeps the PIAM secure.

A person will use their PIAM to control their smart digital identities as well as any AI systems/bots they have a contractual relationship with. Yes, it's complex, which is why the PIAM cost centres start out with a series of small, rapid POC's and pilots to work our way through the many challenges in designing, implementing and maintain PIAMS.

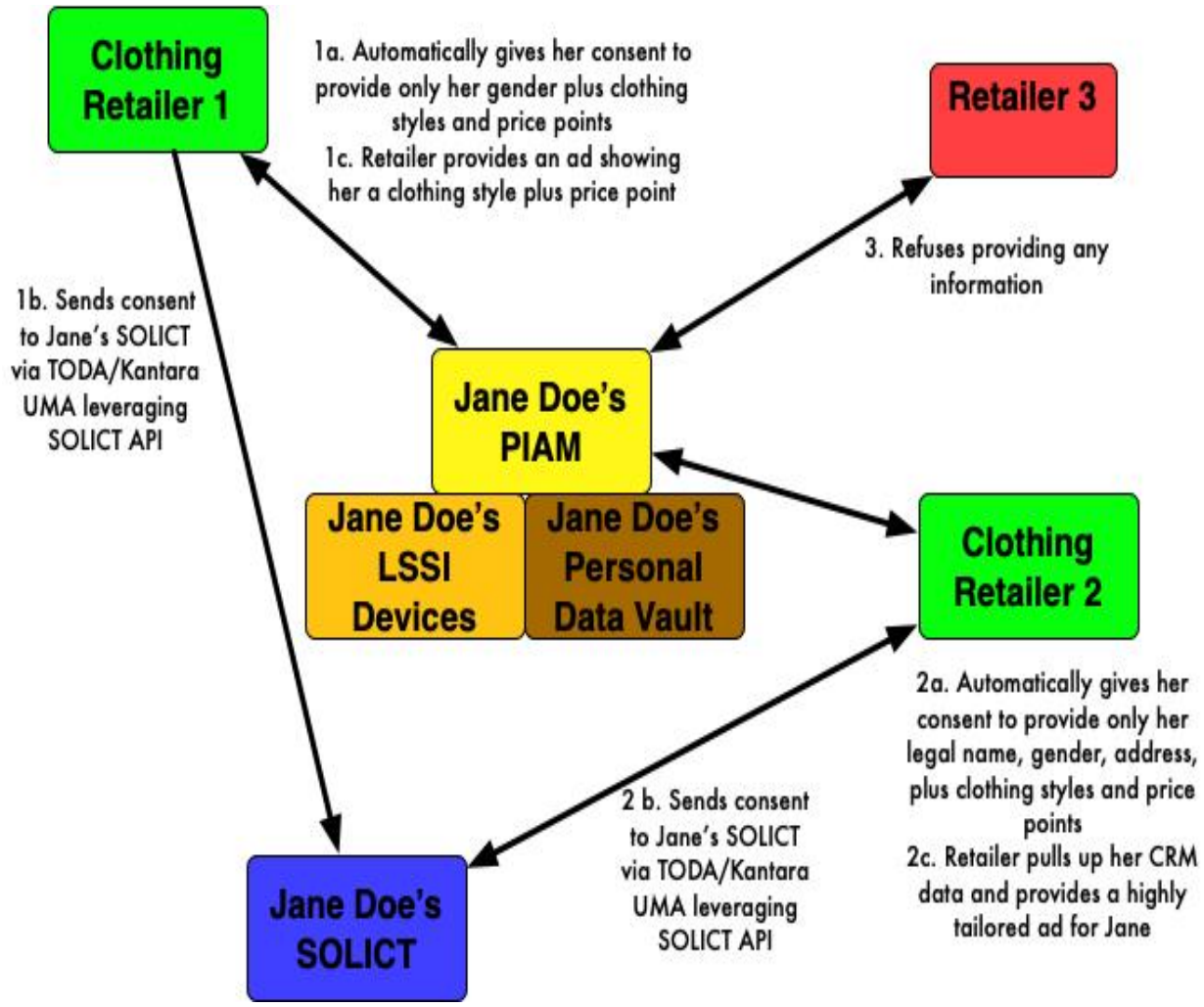
Finally, I can easily see where companies will want to produce PIAMS. Why? It puts them closest to their customer. My goal in creating the architecture is to adopt PIAM standards:

- Protecting a person's PIAM regardless of who provides it
- Allowing companies to innovate, leveraging AI, and rapidly feeding this back into PIAM standard changes

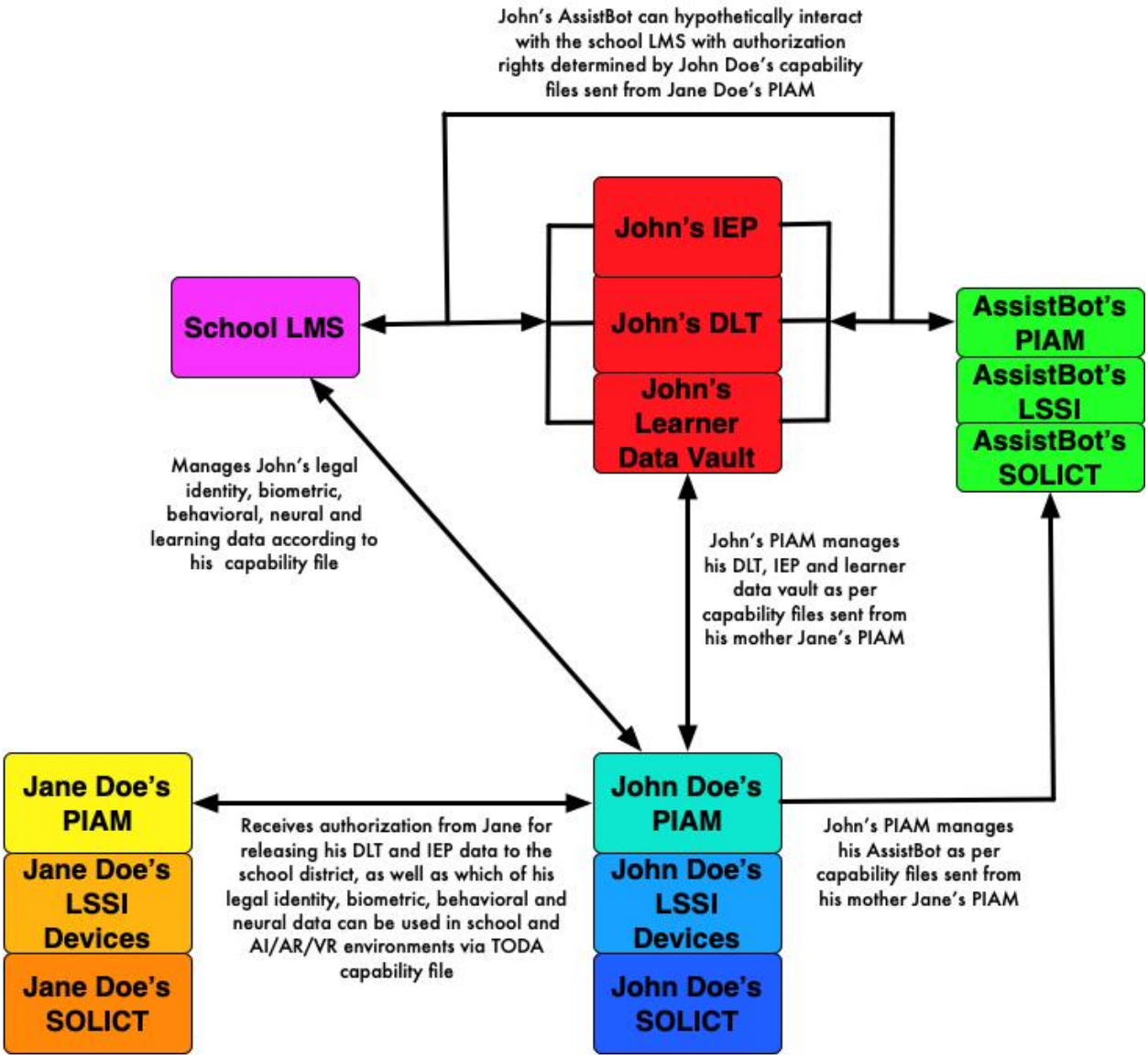
Here's the link to the PIAM Cost Centre. PIAM's operate to global standards, administered by the global, independent non-profit.

PIAM Vision Examples:

Jane Doe Walking Down a Shopping Mall

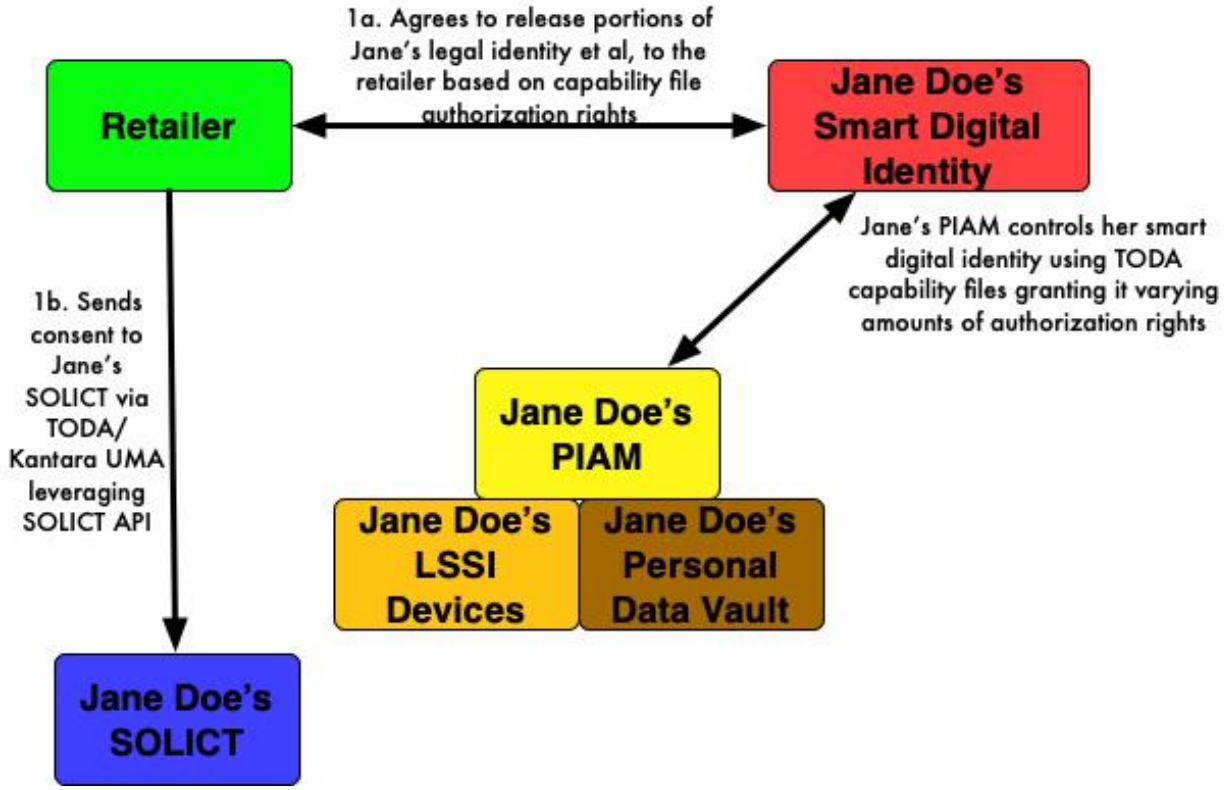


John Doe's in School



Note: The above example is only my best guess at use case workflows. As the design team works on this, they may decide to have Jane Doe's PIAM interact with the school LMS etc.

Jane Doe's Smart Digital Identity With a Retailer



Vision - Core New Learning Vision

Background:

Today's education system is mainly modeled on time. Typically, a student enters the education system at kindergarten, and then progresses to primary, secondary, and post-secondary levels, all based on time.

I wanted to:

- Change this model to one based on learning as the benchmark starting when the learner is a toddler, giving each learner a digital learning twin (DLT)
- Uniquely address each learner based on their learning abilities
- Leverage new types of AI, AR (augmented reality) and VR (virtual reality) learning environments which could be local/global
- Leave no learner behind on the planet regardless of their location, abilities to learn, etc.

I realized to achieve the vision requires a new legal identity architecture for humans, AI systems and bots.

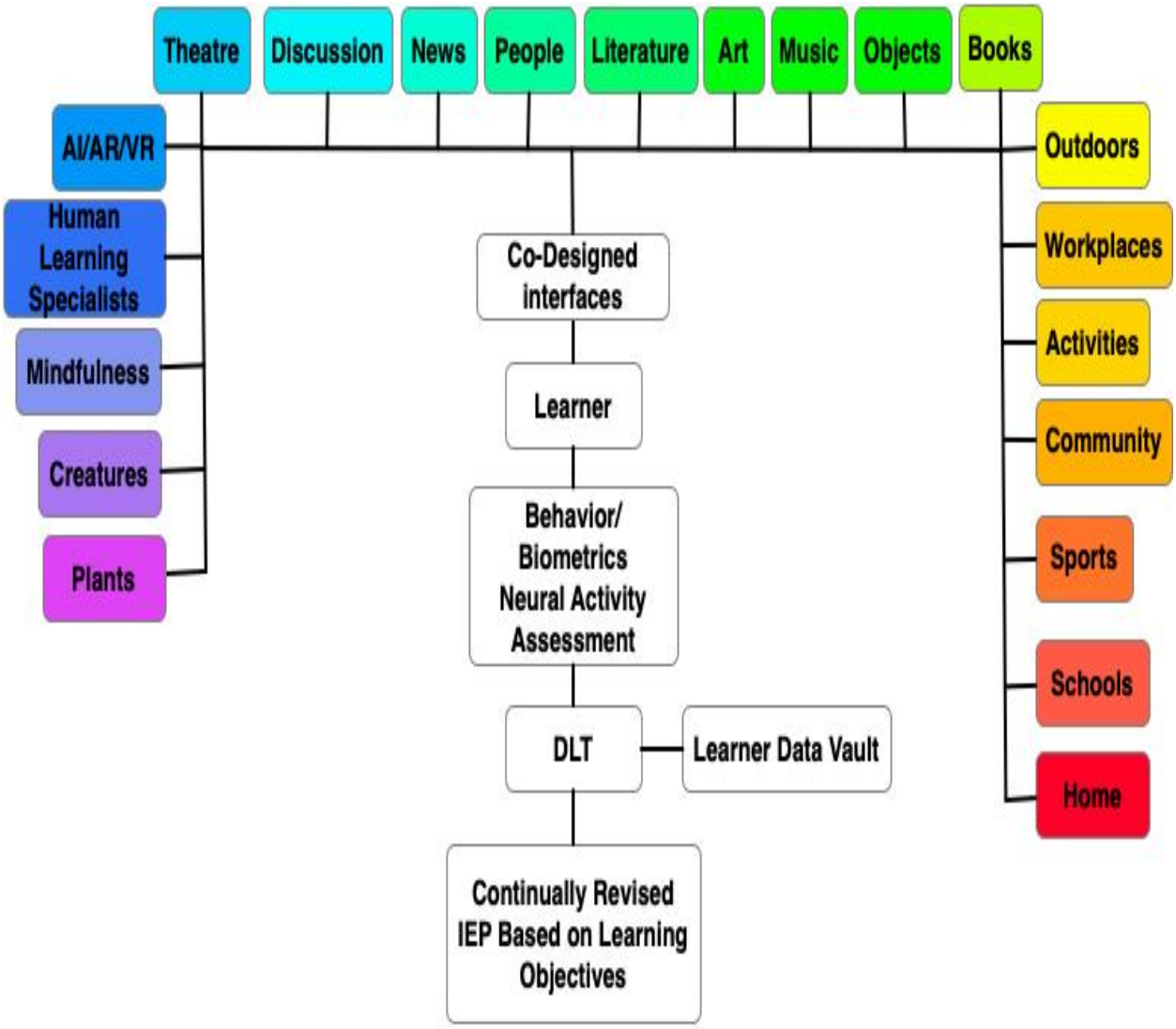
Vision:

Skim these two articles:

- "**Vision: Learning Journey of Two Young Kids in a Remote Village**"
- "**Sir Ken Robinson - You Nailed It!**"
- "**The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom**"
- "**My Learning Journey**"

IT'S VERY TRANSFORMATIONAL.

Core Learning Vision Diagram



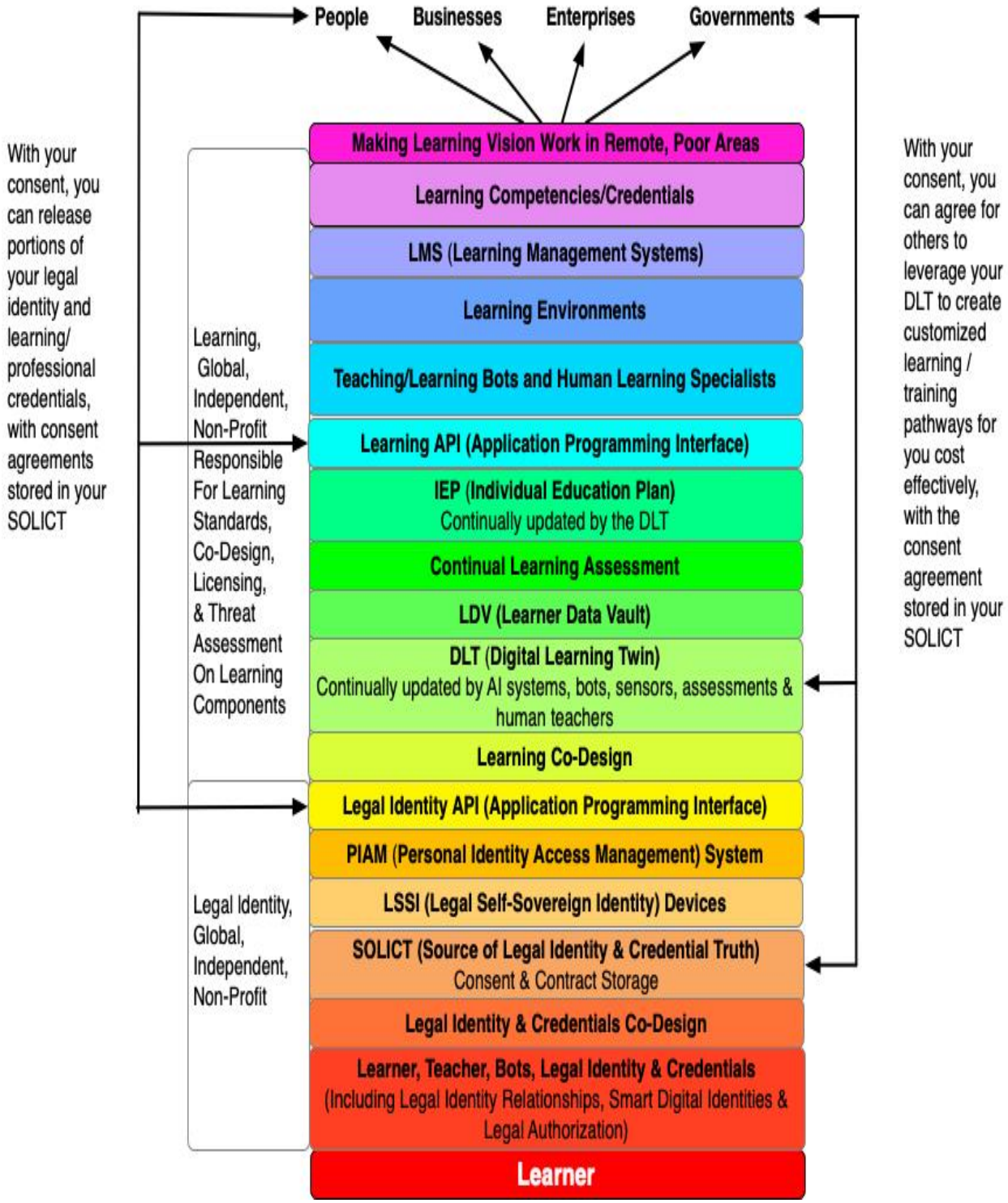
All the above leveraging a rethought legal identity framework for humans and AI systems/bots

Notes on Learning Vision:

1. The tech described above is just emerging allowing the vision to occur. As described throughout this document, my strategy is to crawl, walk and then run towards the vision i.e., don't paint an unreachable vision. Sections of the vision can be done in parallel cost centres. Thus…
2. Start with assessment and then, wherever possible, automate:
    a. Today there is about 3-5% of the population who are somewhere on the spectrum of ADHD/ASD
    b. Diagnosing them is currently expensive, time consuming, with learning strategies often calling for one on one instruction which is cost-prohibitive in many school districts
    c. Thus, it's a great place to start with leveraging existing research/work on automating assessments, along with bringing in new tech like behavioral/biometric data and neural activity to create more fine-grained assessments
    d. Then leverage co-design to create new learning interfaces for them
3. Leverage existing learning assistant bots to assist these types of learners, widening out the use of them:
    a. This can begin in both the home and school
    b. It can provide greater one on one time with the learner, continually taking in data and refining the IEP (Individualized Education Plan)
4. In addition to urban pilots, pilot the above in poor and/or remote parts of the planet:
    a. No one should be left behind in this learning tsunami wave just starting to strike our planetary shores
    b. You'll see I've created a separate cost centre devoted to this
5. Create the beginnings of a DLT/IEP:
    a. The computing power is just arriving allowing this to occur in limited ways
6. Leverage existing work on standardizing secondary and post-secondary credentials:
    a. This is required to create a global learning system with globally recognized credentials
7. Most importantly leverage co-design throughout the entire learning architecture to ensure all learners, regardless of their abilities or disabilities learn in ways that are best for them
8. All the above crawling steps can begin without the rethought human and AI system/not legal framework
    a. However, note the legal framework is required to achieve the vision mid-term

Vision - Learning Vision Architecture/Cost Centres Diagram:

You'll see it's complex, requiring lots of different subcomponent cost centres:



Vision – Co-Design 'Nothing About Us Without Us'

Criticality of Co-Design

As I see it, the architectures have two important, critical challenges:

1. **Creating a continually secure architecture for registering digital entities at transactional speeds**
1. **Creating citizen interfaces, designed from the ground up, enabling all citizens, regardless of their abilities or disabilities, to understand and use their SOLICT, LSSI devices, PIAM, DLT, IEP & LDV easily and securely. As well they must be able to easily work with local notaries. Without this, the architectures won't work in the field.**

Thus, co-design is a mission critical component of the architecture.

Background

Architecture:

The architecture for legal identity and learning will give every person on the planet their own:

- **SOLICT** – Source of Legal Identity & Credential Truth, which is a database the person manages
- **LSSI devices** – Legal Self-Sovereign Identity Devices including:
    - Smart card
    - Digital application
    - Physical wristband
    - Chip implanted into them
- **PIAM** – Personal Identity Access Management service
    - Which is AI leveraged, allowing the person to preset and manage their consents for release of portion of their legal identity and credentials
- **DLT** – Ai leveraged Digital Learning Twin for each learner, which in turn generates…
- **IEP** – Individualized Education Plan for each learner, with all learning data stored in
- **LDV** – Learning Data Vault which is a database the learner manages

Legal Identity Relationships:

There will be a variety of different types of legal identity relationships between entities e.g. parent/child, legal guardian/person, power of attorney/person, etc. Thus, the architecture enables someone with legal authority to manage another entity's consents for releasing portions of their legal identity and credentials, as well as their learning data.

Central Storage of Consents:

All consents given by an entity or, by an entity which has legal relationship abilities to make decisions on behalf of another entity, will be stored in the entity's SOLICT from cradle to grave. It's hypothetically possible, based on existing local privacy laws and regulations, for an entity to go back in time, via their SOLICT, identify a consent they gave, and now ask for it to be revoked.

The Challenges?

Each person on the planet will need to be able to:

- Understand the components above
- Make their decisions
- Execute them

People With Disabilities

UN CONVENTION ON THE RIGHTS OF PERSONS WITH DISABILITIES

Article 21 - Freedom of expression and opinion, and access to information
States Parties shall take all appropriate measures to ensure that persons with disabilities can exercise the right to freedom of expression and opinion, including the freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice, as defined in article 2 of the present Convention, including by:
(a) Providing information intended for the general public to persons with disabilities in accessible formats and technologies appropriate to different kinds of disabilities in a timely manner and without additional cost.
(b) Accepting and facilitating the use of sign languages, Braille, augmentative and alternative communication, and all other accessible means, modes and formats of communication of their choice by persons with disabilities in official interactions;
(c) Urging private entities that provide services to the general public, including through the Internet, to provide information and services in accessible and usable formats for persons with disabilities.
(d) Encouraging the mass media, including providers of information through the Internet, to make their services accessible to persons with disabilities;
(e) Recognizing and promoting the use of sign languages.

All The Above Results in the Following Challenges:

1. **Given the wide variety of abilities, communication, understanding, age, ethnicity, etc. how can this be designed such that it works for everyone?**
2. **How can the design, logic, and various techniques/interfaces be kept up to date as this tech change curve rapidly unfolds?**
3. **How can it work for people with disabilities?**

ENTER CO-DESIGN…

Co-Design - With Us, For Us

Introduction:

Co-design is a process that answers these following questions:

1. What decisions are being made?
2. Who will decide?
3. What's the decision-making process?

MOST IMPORTANTLY IT INVOLVES THE ACTUAL USERS AND OTHER NON-IT EXPERTS IN THE END-TO-END DESIGN, POC'ING, PILOTING, ROLLOUT AND ONGOING SUPPORT. THIS IS SOMETHING INFORMATION TECHNOLOGY AND THE GOVERNANCE PROCESS GENERALLY DON'T UNDERSTAND.

IT'S CRITICAL TO THE SUCCESS OF THIS ARCHITECTURE. WHICH IS WHY I LIKE THE TERM ASSOCIATED WITH CO-DESIGN, "WITH US, FOR US".

What's The Decision-Making Process - 5 Phases

1. Phase I – What Project?
    a. Identify methods to be used
    b. Team required
    c. Time required
    d. Determine money to be budgeted
    e. All of which leads to team methods
2. Phase II - What is?
    a. Determine current situation
    b. Learn from a wide diversity of people with lived experience
    c. What do these people see as the opportunities?
    d. All of which leads to determining strong opportunities to do something different and better
3. Phase III – What If?
    a. Determine early ideas into strong concepts and new solutions
    b. Using multiple rounds of feedback from the people most likely to be impacted by them
4. Phase IV – What works?
    a. Taking the concepts and turning them into solutions which are rapidly prototyped with people most affected
    b. Learn what works, what doesn't work using live feedback
5. Phase V – Keep it up to date
    a. As this tech change curve unfolds, and political/socio-economic changes occur, the above process needs to continually re-occur to keep the end-to-end system up to date

Learning From Others Who've Gone Before Us

I strongly urge readers to read **"Nadia – Politics, Bigotry, Artificial Intelligence".** Why?

Background:

In 2015-2016, the outcome of the Australian Federal Government Budget was that the NDIA (National Disability Insurance Agency) achieved $143 million funding for enterprise systems and new capabilities such as Artificial Intelligence and predictive analytics. This included $8.9 million over 2 years for an 'omni-channel' avatar (which would become Nadia), digital innovation, and ongoing funding for an in-house co-design team.

Here's what happened. The Australian federal government:

- Created a co-design team
- Which created Nadia
- Did pilots with Nadia
- Then inappropriately expanded the concept to all of government
- Listened to big tech which was proposing chat bots which wouldn't work as advertised with the target audience
- Then politically wrapped up Nadia with a failed project, Robodebt
- And killed it
- Without understanding the consequences to thousands or more of their disabled citizens who couldn't work with call centres and complex websites to be serviced
- Then vilified some of the people involved in the innovative program
- Years later, they still don't have a Nadia type program for disabled people to understand and interact with their disability services

It's a classic case of how to not manage an innovative initiative.

Their Business Case Had These Innovative Features:

"The business case emphasised the obligation to provide a contextualised user experience. Under the NDIS Act, the contents of any notice, approved form or information given, or regulations or rules must be explained to the maximum extent possible to the person in the language, mode of communication and terms which that person is most likely to understand.

The omni-channel concept related to a suite of augmented capabilities that would respond and reflect the preferences and the way people behave and communicate.

The business case illustrated what this meant by way of several examples and scenarios. For example, that a person with cognitive disability might require images and avatars rather than text, in order to understand the content on the website. A user with visual impairment might require text-to-speech, voice translation, AusLan video, high contrast content, or magnification. A contextualised experience would support people with various disabilities and with a range of augmented servicing capabilities, which was the omni-channel. This augmented experience would be co-designed with participants, families, stakeholders, and advocates. To my knowledge, there had never before been a business case for government service delivery that

included avatars, pictograms, adaptive interfaces, gesture control, voice translation and text-to-speech, AusLan video and proactive support."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 33). Kindle Edition.

Their Vision:

"Far from the political exhortations about the Nadia technology not being ready or mature enough, what is illustrated and described throughout this book, is that the technology already existed, and the component technologies were being used. There were no new technology inventions needed. The breakthrough innovation was in the co-design process driven by people with disability. For the first time, instead of people having to adapt to systems, this was the realisation of the vision to have systems adapt to people and so go some way to achieving the objectives of the Convention."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 48). Kindle Edition

"Co-design is the only way to understand the human experience and dimensions of risk and innovation, in complex servicing systems. Involving the people who have the most at stake. And from an innovation perspective, co-design reveals insights making possible the design of something that has never been designed before. "

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 63). Kindle Edition.

"Co-design is not an activity to be outsourced to consultants via periodic reference groups. Co-design is not an IT function. User testing and hackathons are not co-design. Co-design involves designing the service in context, led by people who have the expertise and lived experience to know what is being observed."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 69). Kindle Edition.

Their Ethics:

In my submission (number 33) to the Australian Senate Joint Standing Committee on the NDIS (JSCNDIS) Inquiry into Independent Assessments[36] (aka RoboNDIS), I explained my interpretation of the relationship between co-design and ethics. Co-design is essential to an ethics framework. 'An ethics framework cannot understand risk or safeguard human rights if the end-to-end human experience does not systematically influence design. This is what co-design does. It challenges assumptions, paradigms, and biases. Without co-design, the introduction of bias is inevitable.' The human is out of the loop: the single most significant cause of system defects and failures. With the human out of the loop, privacy by design is also impossible.
Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 51). Kindle Edition.

Their Design:

"The solution design hub capability[61] was a network of physical smart spaces co-designed with and for people with disability; this network was unique in the Australian Public Service and research indicated the only one of its kind in Australia."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 83). Kindle Edition

"Nadia's personality was co-designed and co-created with the community, and university psychology faculty supported the definition of Nadia's manner. Nadia's personality was designed to be warm, informative, and calm. The personality determined aspects of Nadia's look. There was a balance required to achieve an informative, friendly persona, avoiding the extremes of being perceived as bureaucratic or too informal. Psychologists' input was that Nadia should not be stern looking as this could be off-putting for most people and would not achieve the level of engagement and trust desired. Certainly, there was feedback from the community that Nadia was initially a bit too stern looking, so the mannerisms and gestures needed to be adjusted. University psychology faculty supported the co-design with people with intellectual disability, so that the words, expressions, and conversational tempo was empathetic and natural. The positive expressions such as smiles, head gestures, facial movements, and mannerisms were co-designed to be inclusive and not startle people with intellectual disability or cognitive disability. The tone and tempo of the voice were important for the coherence of the personality."

"Importantly, from a governance perspective, psychologists played a preeminent role far beyond that of any IT roles. The role of personality in a cognitive conversational system was neither understood nor accepted by the traditional IT government bureaucracy, as evidenced by the blistering and defective whole-of-government commentary in this area.[54] In my opinion, the emergence of AI powered digital humans has given rise to new horizons of design, involving the preeminent role of psychologists and story design. AI powered digital humans as uniquely human-like conversational interfaces, will generate a massive demand for psychologists skilled in these areas."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 75). Kindle Edition.

"Different Avatars. From the outset, it was envisaged that there would be a range of different avatars, representing community diversity, as well as non-humanlike characters such as superheros and cartoons. Specifically during co-design, there was a desire expressed by Indigenous people participating in the co-design, for an Indigenous male persona and Indigenous female persona to reflect the community served."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (pp. 99-100). Kindle Edition.

"PART IV: Building Nadia's Brain

Upfront, three fallacies are challenged. The first fallacy is that large data sets are required. The second fallacy is that crowd sourcing training leads to better performance. And the third fallacy, is that building the corpus is an 'IT' activity.

"The language and conversational models developed were co-designed, so that people with disability including people with intellectual disability, could understand the information in their context. The corpus is not a randomised collection of information on a topic."

"A lifecycle approach means that an operating model is necessary: this is not set and forget. And the thoughts and emotions that shape these patterns, can only be discovered via co-design. No amount of crowdsourcing with the general population will discover these patterns and emotions."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (pp. 138-139). Kindle Edition.

"Organisations and especially government and healthcare, provide information that is complex and bureaucratically constructed, in rigid structured formats. People have been forced to adapt to this rigidity and if they can't, too bad. The end result is the default common patterns (and costly patterns) of conversations in these servicing domains; patterns of interactions where people suffer to understand and translate the miasma of this bureaucratic complexity. These inflexible patterns are unfortunately universal. Co-design documents these patterns within the particular context (in this case the NDIS); deconstructs the complexity; localises the language; and then constructs conversation modules. Psychologists played a pivotal role in the development of the natural language model and the drafting of dialogue, with the cognitive platforms systematising the capture of meaning. Localisation of language was more about concepts, context, accessibility, idioms, and synonyms than literal translation. Contextual conversation patterns in servicing domains as applied to cognitive systems will fundamentally explode decades old industrial scale servicing models, enabling localization."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 141). Kindle Edition.

"Dialogue: The Golden Thread. The conversation dialogue model which built upon the Q&A corpus, comprised of specific conversation patterns; domain specific patterns (in this case, disability, and the NDIS); client service protocols; and dialogue navigators. Randomly diving off and trying to build or script a conversation without this level of context and co-design, is not sustainable or repeatable, and it will lack the necessary safety guardrails which exist in human-to-human service delivery models. Beyond that, randomness does not achieve the golden thread of understanding and information transference. There are several different conversation patterns in servicing domains, and co-design determines how these are applied to support our ability to understand where we are 'located' within a conversation."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (p. 149). Kindle Edition.

Bounded systems, such as Nadia and the Digital Human Cardiac Coach, are designed to drive intelligence depth in a particular domain (such as disability services, cardiac health) as well as natural language context. That is, how ordinary people who are not experts and potentially experience disadvantage or disability, actually talk about a topic. As a bounded system, Nadia was co-designed to have contextual conversations and able to determine intent from a corpus of thousands of elements and natural language expressions. These contextual conversations are interactions through which people gain understanding of a topic or issue, not just a simple question-and-answer pair. Most people even in the general population don't seek information via perfectly crafted questions using correct bureaucratic terminology.

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (pp. 156-157). Kindle Edition.

"Localisation through co-design is also incredibly important to achieve information transference. For example, local words, idioms, phrases have a particular meaning in a geography or community which often do not literally translate. Localisation also relates to program specific words and phrases which are defined in legislation. For example, the words and phrases used by the NDIS would not necessarily translate with the same meaning even to other English-speaking countries. Local words, idioms, phrases and even concepts for different communities, are also often accompanied by other mannerisms and expressions to convey meaning. However, the important point to be made here is that there is no short-cutting this process given that the dialogue model not only supports the digital human conversations, but conversations via other omni-channel interfaces."

Johnson, Marie. Nadia: Politics | Bigotry | Artificial Intelligence (pp. 162-163). Kindle Edition.

Yes, there's a lot of lessons to learn from the above.

Applying This to The Legal Identity & Learning Architectures

At the 100,000-foot level, there's lot of lessons to be learnt from Nadia which can be applied to what this architecture delivers.

1. Bounded content – explaining choices:
    a. The various architectural pieces are constrained by legal boundaries
    b. Thus, the co-design process must not try and solve telling the person what decision to make
    c. It must leave the choice up to the person BUT explain the choices in ways the citizen can understand re-releasing portions of their legal identity, credentials and learning data to
    d. SO, THE VARIOUS INTERFACES THAT WILL BE CO-DESIGNED MUST NOT BECOME A PRIVACY ADVISOR, ETC.
2. Assist the citizen in executing their choice
    a. Given the extremely wide, diverse population around the planet the architecture addresses, it must enable each citizen to execute their choice
3. Assist the citizen in hypothetically going back to see consents they granted, or were granted on their behalf by those with legal identity relationships, to understand this
4. To create a combination of permanent and temporary citizen co-design groups that are integrally plugged into, from day one, with the legal, business processes, technical, governance, support and security design teams
5. To create "design hubs" such that all members of the co-design teams can participate
6. To do rapid POC (proof of concept) and pilot work with not only the permanent co-design team but also with a wide variety of different types of users
    a. Learn what works, what doesn't work, and then redo until it all works as advertised for all people
7. To create rapid update processes with the co-design team when unexpected tech changes or whatever occur, requiring immediate or near immediate changes
8. Ensuring that the funding country or countries buy into the above before commencing work i.e., IT MUST NOT BE MANAGED LIKE NADIA WAS

Note: There will be a central co-design team for the legal identity architecture (Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre) and a separate central co-design team for the learning architecture (Learning Non-Profit – Co-Design Subcomponent Cost Centre).

Within this architecture cost centre doc, many different cost centres will have co-design costs which in turn are linked to the central co-design cost centres. The central co-design costs thus will have initial low and high guesstimates. These costs will be firmed up by the central co-design teams.

Finally, note within this document, I discuss initially combing the co-design teams for legal identity and learning. It makes sense from an expertise, budget and resource perspective. However, note I haven't done this in this version of the cost centre document and spreadsheet.

Cost Centres

Notes on Cost Centres:

1. **There 294 cost subcomponent centres contained within this document.**
2. **HOWEVER, note that many of them have their costs borne by cost centres located within the two new, global, independent, very well-funded non-profits. Thus, within this doc as well as the spreadsheet, cost centres are cross-linked to the actual cost centre bearing the funding.**
3. **Also note that several cost centres are shared between the two new non-profits to maximize resources and expertise while reducing budget costs.**
4. As you read through each of the cost centres below, you'll see it referring to potential team members and expertise. Most, but not all of them, require similar types of people. Thus, it makes sense to operationalize these cost centres under one similar type of management and project team, with sub-teams assigned to address each specific cost centre. LOTS of cross-polinization of ideas and expertise is possible via this approach.
5. I also note that many of these cost centres could conceivably take lots of time and costs in developing solutions. My point? Drive the teams to a very clear set of deliverables, with heavy emphasis on quickly proving out ideas in POC (proof of concept environments), and then rapidly testing them out in the field. Time is of the essence.
6. Not included in the cost centre team recommendations are the following:
    a. Project and program managers
    b. HR, Payroll, etc.
    c. Why? I can easily see how these resources can be leveraged across numerous projects. Thus, I've intentionally left them out until the teams are formed
    d. Then wise allocation of these types of resources can occur
    e. HOWEVER, within the Excel spreadsheet, note most cost centres have a combination of experts and operating costs. Thus, the cost of the additional personnel above will be absorbed in the operating costs.
7. This version of the Word cost centre document and accompanying Excel spreadsheet has been substantially edited. Why?
    a. When I recently read Marie Johnson's excellent book on co-design, "**Nadia – Politics, Bigotry, Artificial Intelligence**", I realized most of the entire architecture must be based on leveraging co-design. So, as you read through this document, you'll see me including co-design in the vision, co-design experts as part of most teams, and co-design cost centres within each non-profit.
    b. I wanted to give readers of the spreadsheet an explanation of my logic used in creating the cost guesstimates. So, within the Excel spreadsheet for each subcomponent cost centre bearing costs, you'll see notes with an explanation of how I came to the cost guesstimate. You'll also see how I believe experts will change my cost guesstimates.
    c. I wanted to maximize resources and expertise for cost centres while reducing costs. Thus, within this document and the Excel spreadsheet, you'll see me combining teams across not only different cost centres, but also between non-profits. For some cost centres I haven't done this but suggest it's possible.
    d. All the above resulted in a reduction of approximately $4 billion in costs.

Cost Centre: Rethought CRVS (Civil Registration Vital Statistics)

Background:

As described in the problem #1 in "**Legal Identity Problem Statements**" existing CRVS systems today are mostly antiquated. They have:

- No global data standards
- No ability to query all CRVs systems to confirm an identity
- Use paper which is easily frauded
- Can't digitally show legal identity relationships between people e.g., parent/child
- Can't legally, anonymously prove you're a human, and above or below age of consent
- Aren't anywhere near ready to address rapidly emerging smart digital identities of us
- Are unprepared for the arrival of AI systems and bots, both physical and digital, requiring legal identities
- Have no technical ability to differentiate human clone legal identities

.

Having said this, on the good news front:

- There's the emergence of OpenCRVS which is currently deployed in Bangladesh and Zambia
- Tech has emerged allowing us to rethink legal identity. Examples include:
    - TODA & Graphs. Skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"
    - Database development allowing for the hypothetical possibility of creating one database per person for their source of legal identity & credential truth – Skim, "**Give Each Person Their Own Source of Legal Identity & Credential Truth Database (SOLICT)**"
    - Infant fingerprints are now possible – skim Infant Fingerprints section of this document

On the bad news front:

- I've written about how with the implementation of the new CRVS/SOLICT/LSSI/PIAM framework, will increasingly make it difficult for criminals and malicious states easily masquerade as another legal identities. This means the price points for fake identities will rise. As this occurs, the value of successfully attacking a CRVS system increases. Thus, I can easily see them, registrars out in the field, etc. becoming a prime attack vector into the legal identity framework
- This curve, means each hour, new attack vectors are being created not only against the tech used in a new legal identity framework, but also the governance, business processes and end user. My underlying premise is most governments around the planet don't have the resources, expertise, and infrastructure to deal with this

- The costs from identity fraud are what I call "whopper sized" – skim Problem #2 in "**Legal Identity Problem Statements**"
- The arrival of AI systems and bots means, depending on risk, they require legal identities. Watch this video, "**The AI Dilemma**" to see what's on our front doorstep. Then skim "**AI, Bots & Us - Examples of Rapid Change**" to see examples of AI systems and bots currently in use on the planet.
- Finally, as the planet madly digitizes, including CRVS systems, they become prone to being taken down by sun GMD EMP events or by HEMP attacks (skim this article, "**When Our Digital Legal Identity Trust Goes Poof!**" The chances of a sun GMD event this decade is 1 in 8

ADDING IT ALL UP, ONE CAN CONCLUDE THE PLANET IS IN A LEGAL IDENTITY MESS.

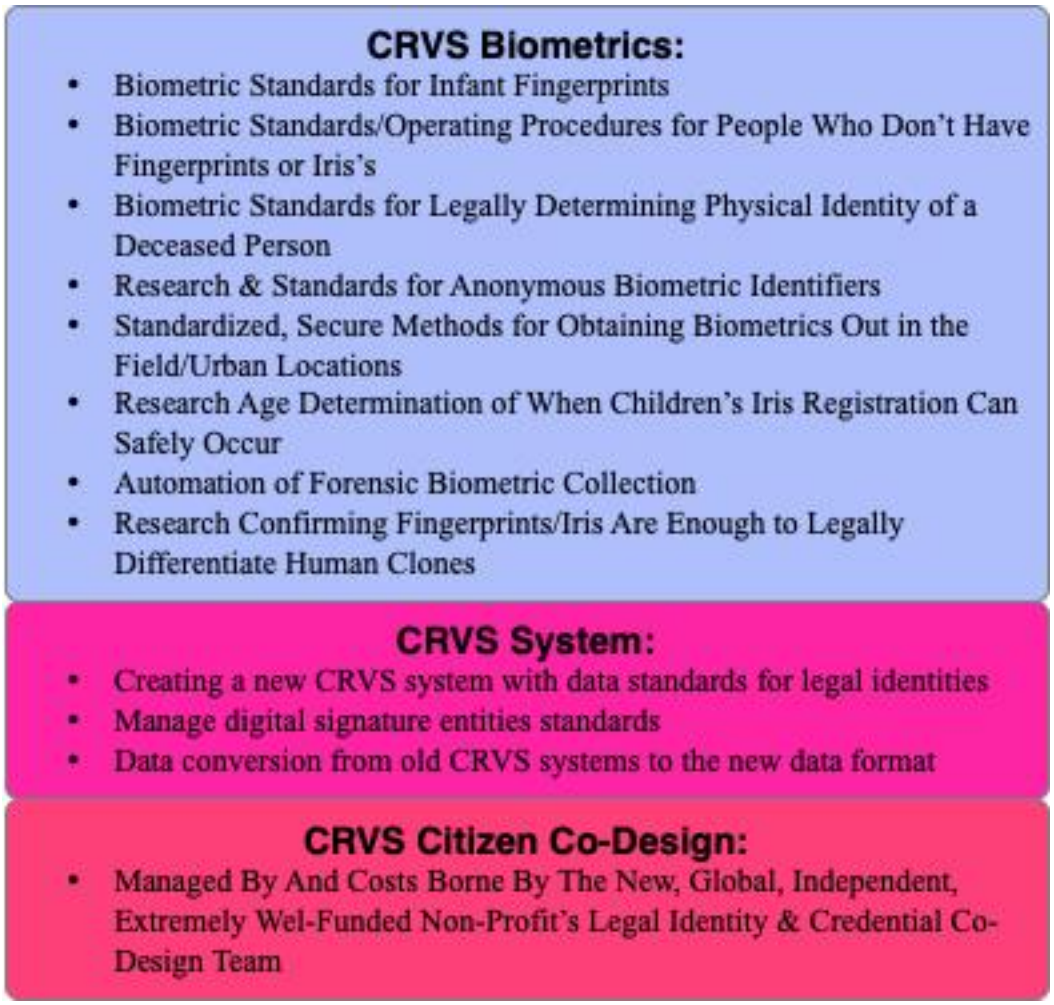
The challenge in architecting a solution for this is the highly jurisdictional control over legal identity e.g., state/province. It means any solution must still allow local control, but export out the data in such a way, it's globally usable, both physically and digitally, from cradle to grave, for every person on the planet. Further, it must be secure 24x7x365.

FINALLY, ANY CRVS SYSTEM MUST BE BUILT SUCH THAT ALL CITIZENS, REGARDLESS OF THEIR ABILITIES OR DISABILITIES CAN USE IT.

That's what the architecture delivers.

CRVS Subcomponent Cost Centres:

Displayed as a series of pics from the bottom up…



Smart Digital Identities of Us:

- API
- PIAM
- TODA LSSI
- Smart Digital Identities Co-Design Interface For Humans
- SOLICT
- Smart Digital Identities Legal Identity Relationships Including Hives
- Smart Digital Identities Legal Authorization Rights
- Authoritative Credentials Source
- Smart Digital Identities Legal Identity & Credential Written To Source Code

AI Systems/Bots:

- AI Systems/Bots API
- AI Systems/Bots PIAM
- AI Systems/Bots TODA LSSI
- AI Systems//Bots SOLICT
- AI Systems/Bots Authorization Rights
- AI Systems/Bots Legal Identity & Hive Relationships
- Writing To The Source Code Legal Identifiers & Credentials
- Authoritative Credentials Source
- CRVS
- AI Systems/Bots Both Digital And Physical)

Legal Identity & Hive Relationships:

- SOLICT/LSSI Devices API
- PIAM Consent Agreements/Contracts With Third Parties
- SOLICT to LSSI Devices Via TODA File
- Legal Identity & Hive Relationships Co-Design
- SOLICT Stores Legal Identity Relationships
- Transfer to SOLICT via Digitally Signed TODA file
- Graph Databases Store Relationships Cross-Linking Between Different Entities
- Legal Identity Hive Relationship Standards
- Authoritative Data Source CRVS

Authorization Rights:

- SOLICT/LSSI Devices API
- PIAM Manages Legal Authorization Rights
- Transfer from SOLICT To LSSI Via TODA File
- Co-Design Standards For Accessing Authorization Rights
- Transfer via TODA from CRVS to SOLICT
- Digital Signature Signing Of Authorization Rights
- Legal Authorization Rights Standards

CRVS API:

- API Gateway
- Audit Trail
- API IAM (Identity Access Management)
- API Clients Internal/External
- API Backend
- API Applications/API Rules
- API Co-Design
- CRVS Authoritative Sources Databases

CRVS Data Centres:

- Electrical Supply/Consumption Plan and Processes
- Sun EMP/HEMP Event Plan/Processes
- Physical/Cyber Security Management/Processes
- Disaster Recovery Plan
- Backup Strategy/Processes
- Processes Updating Servers/Apps/Network
- Servers (Physical & Cloud)/Data/Network
- Availability - 99.999%

CRVS Governance Laws/Regulations:

- Co-Design Standards For Citizens Wanting To Interact With Their CRVS Department
- Ability For CRVS to Digitally Sign Legal Identity Information
- Ability For CRVS To Send Legal Identity To SOLICT Via TODA
- Biometric Standards Used In Human Legal Identities
- Standards For Human Legal Identities Registered In CRVS
- Standards For AI Leveraged Smart Digital Identities Of Humans Registered In CRVS
- Standards For AI Systems And Bots Legal Identity Registration
- Standards For Legal Identity/Hive Relationships Stored Within CRVS
- Standards For Legal Authorization Issued By CRVS
- Security Standards For The CRVS System
- Archival Period For An Entity's Records
- Management Abilities To Access The CRVS System
- Notaries Abilities To Access The CRVS System
- Abilities Of CRVS To Query All Other CRVS Systems
- Specify Actions From Threat Responses Issued By The Non-Profit
- Notification Systems For Events Like death, Etc.
- Availability Of The CRVS System

Global, Independent, Non Profit:

- Manages API Standards
- 24x7x365 Threat Assessments
- Manages Notary Standards For Legal Identity & Credentials
- Manages PIAM Standards
- Manages LSSI Device Standards
- Manages SOLICT Databases
- Manages SOLICT Standards
- Manages Credential Issuance Standards
- Manages Legal Authorization Standards
- Legal Identity & Credential Co-Design Team
- Manages Legal Identity Hive Relationships Standards
- Licenses CRVS Software To Jurisdictions & Credential Issuance Standards to Credential Bodies
- EMP/HEMP Power Supply
- Manages CRVS Software/System
- Manages Digital Signature Entity Standards
- Manages Legal Identity Standards For Humans, AI Systems and Bots
- Governance Co-ordination/Advisory

Other Cost Centres Dependent Upon This Cost Centre:

- Legal Identity & Hive Relationships - Authoritative Entity Data Source – CRVS Subcomponent Cost Centre
- Legal Identity & Hive Relationships - Transfer to SOLICT (Source of Legal Identity & Credential Truth) Via Digitally Signed TODA File Subcomponent Cost Centre
- Notaries - CRVS - Authoritative Source for Human & AI System/Bot Legal Identities, Legal Identity/Hive Relationships & Authorization Rights) Subcomponent Costs
- DLT - Learner Legal Identity Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

CRVS Biometric Technology Subcomponent Cost Centres

Very Important Note:

The experts required for most of the biometric subcomponent cost centres below are very similar. Thus, it might make sense to combine several of the cost centres into one centrally managed. This maximizes expertise and resources while minimizing costs. I have NOT done this for this version of this cost centre document and spreadsheet.

Biometric Standards for Infant Fingerprints Subcomponent Cost Centre:

Background:

- Good news the technology now exists and has been piloted. Skim the following:
  - Dr. Anil Jain - **Infant-Prints: Fingerprints for Reducing Infant Mortality** -
  - UCSD's KidPrint
  - Gates foundation - "**Biometric recognition of newborns and infants by non-contact fingerprinting: lessons learned**"
- Bad news – no existing standards or biometric databases for infant fingerprints exist
- These need to be rapidly created to spur vendors to conform to them and offer vendor choice to CRVS systems

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Biometric Standards for Infant Fingerprints Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Discuss with Dr. Anil Jain, and the Gates Foundation the deliverables required
  - For each one estimate type of resources required, timelines and costs
  - Create a team composed of the following:
    - Infant biometric experts
    - Field experts handling death registrations in the field
    - Legal experts
    - Business process experts
    - Security/red team experts
    - CRVS experts
    - Global, independent non-profit experts
    - Notary experts
    - Lesson learnt experts
- Create standards
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Biometric Standards/Operating Procedures for People Who Don't Have Fingerprints or Iris's Subcomponent Cost Centre:

Background:

Careful thought must be given to people who don't have fingers and eyes or, lose them during their lifetime i.e., the proposed CRVS system discriminates against them. Thus, biometrics with a low ERR rate must be:

- Identified,
- Determine which ones to use
- How they'll be obtained in a standardized manner both in urban centres and out in remote areas
- If they can be used post death to identify a person
- Etc.

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Biometric Standards/Operating Procedures for People Who Don't Have Fingerprints or Iris's Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Create a team composed of the following:
        - Forensic pathologists
        - Biometric experts
        - Field experts handling death registrations in the field
        - Legal experts
        - Business process experts
        - Security/red team experts
        - CRVS experts
        - Global, independent non-profit experts
        - Notary experts
        - Lesson learnt experts
- Determine the efficacy of using the alternate biometrics to legally identify a person
- Based on the above, create modified standards and operating processes
- POC the above to see how it works, amend and retest until the results are standardized
- Pilot it within 1-3 jurisdictions
- Create standards
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Biometric Standards for Legally Determining Physical Identity of a Deceased Person Subcomponent Cost Centre:

Background:

The advent of a legal identity framework leveraging forensic biometrics like fingerprints and iris, offers the ability to leverage these at time of death. I note that depending on the condition of the body at death, along with the availability or lack thereof of fingers and eyes, these may or may not be useful in determining the legal identity of the deceased.

Thus, it's included as a separate cost centre to agree on existing standards for use of fingerprints and iris at time of death. As well, for poor or remote parts of the planet, my strategy is to leverage and/or develop tech allowing a local doctor or coroner, tools to assist them in their job.

The end goal of this cost centre is to leverage standards for medical use of fingerprints and iris, after death, if available to confirm the legal identity of the person, by being able to query all CRVS systems around the planet.

Finally, I note when human clones appear in our societies, legally determining then when they've alive as well as dead will also be required. Fingerprints and iris are two potential ways to legally differentiate Jane Doe 1,2,3,4 etc.

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Biometric Standards for Legally Determining Physical Identity of a Deceased Person

Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Create a team composed of the following:
    - Forensic pathologists
    - Biometric experts
    - Field experts handling death registrations in the field
    - Legal experts
    - Business process experts
    - CRVS experts
    - Global, independent non-profit experts
    - Notary experts
    - Security/red team experts
  - Determine the efficacy and existing standards of using fingerprints and iris scan post death to determine the legal identity of the person
  - Based on the above, create modified standards for the following processes:
    - Medical death
    - Business
    - Legal processes for determining the legal identity
    - Security
  - Also adopt or create new tech allowing low-cost rugged biometric readers to be used out in the field and/or poor or remote parts of the planet
- POC the above to see how it works, amend and retest until the results are standardized
- Pilot it within 1-3 jurisdictions
- Modify based on the pilots and then rapidly scale
- Create standards
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Research & Standards for Anonymous Biometric Identifiers Subcomponent Cost Centre:

Background:

In Rud Bolle's 2015 paper, "**Anonymous Biometric Identifiers – Revisited**" it discusses using an algorithm with a random number to create revocable, re-issuable biometrics. **If it can be shown to work, it has the potential to radically change how biometrics are used for both authentication and identity verification**. That's why I'm so keen on finding funders to rapidly do the research and determine if it's possible out in real life.

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Research & Standards for Anonymous Biometric Identifiers Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Review with Rud Bolle to get his perspective on complexity
  - Review with leading biometric research experts to get their perspective on complexity
  - Then create deliverables, resources, costs, and timeline estimates to do the research/testing
  - The team should include the following types of people:
    - Biometric experts
    - Field experts handling biometric registrations in the field
    - Legal experts
    - Business process experts
    - Security/red team experts
    - Standards experts
    - CRVS experts
    - Global, independent non-profit experts
    - Notary experts
    - Lessons learnt experts
  - Depending on the outcomes of the research, POC's will be created, learn what didn't work, what worked, and then move to small, controlled pilots
  - Then rapidly scale
- If the work is successful, the rapidly create a new standard
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Note: The budget allocates lots of money over three years to prove it out. If it doesn't work in real life, then it will be killed. If it does work, then the funds are there to rapidly scale.

Standardized, Secure Methods for Obtaining Biometrics Out in the Field/Urban Locations Subcomponent Cost Centre:

Background:

During the Covid pandemic, much work has occurred to obtain people's biometrics at a distance. The deployment of this new CRVS/SOLICT/LSSI/PIAM framework means the use of fingerprints and iris scans for legal identification will substantially increase planet wide. This brings with it new challenges, since in many parts of the planet, a person's legal identity registration and obtaining their forensic biometrics will occur in remote locations.

That's why I created this cost centre. My strategy is to:

- Collate current best practices around the planet for obtaining fingerprints and iris scans, as well as also obtaining a person's face image
- Determine standard operating requirements for both urban and remote locations
- Do a gap analysis to determine any gaps in tech, governance, and business processes
    - If so, then quickly fund work to address the gaps
- Create standard operating procedures (SOP's) for CRVS staff, registrars et al to use
- Create training materials for this
- Rapidly scale planet wide
- Have the red teams continually look for new attack vectors against the SOP's
    - When they find them, rate the threat, and respond accordingly

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Standardized, Secure Methods for Obtaining Biometrics Out in the Field/Urban Locations

Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Review with leading biometric research experts, as well as security experts to get their perspective on complexity
  - Select experts based not only on their knowledge but also some with field location experience
  - Then create deliverables, resources, costs and timeline estimates to do the research/testing
  - The team should include the following types of people:
    - Biometric experts
    - CRVS experts
    - Field experts handling biometric registrations in the field
    - Legal experts
    - Business process experts
    - Security/red team experts
    - Global, independent non-profit experts
    - Notary experts
    - Lessons learnt experts
- Create standards
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Age Determination of When Children's Iris Registration Can Safely Occur Subcomponent Cost Centre:

Background:

Research needs to be done to determine when a child's iris scan can safely and easily occur. Based on this, standard operating procedures need to be developed e.g., doing them at "X" age when vaccinating, first year of school, etc.

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Age Determination of When Children's Iris Registration Can Safely Occur Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Do a paper review on age determination of when it's possible to do iris registration on young children
  - Based on the review either:
    - Create draft standards on when iris can be safely obtained in young children or,
    - Create deliverables, resources, costs and timeline estimates to do the research/testing
- The team should include the following types of people:
  - Iris Biometric experts/researchers
  - Field experts handling biometric registrations in the field
  - Legal experts
  - Business process experts
  - CRVS experts
  - Global, independent non-profit experts
  - Security/red team experts
  - Notary experts
  - Lesson learnt experts
- Create standards
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Automation of Forensic Biometric Collection Subcomponent Cost Centre:

Background:

I'M NOT A BIOMETRIC EXPERT. Having said this, I believe it's possible to do anonymous biometrics (refer to the cost centre). It will likely require standardized methods for obtaining the fingerprints/iris scans such that they can be used with the random number in an algorithm to consistently produce the same digitized number. One of the ways to create consistent biometric registrations will likely be leveraging automation to do this.

Research needs to be done examining ways to automate collection of forensic biometrics to lower costs and increase verification accuracy/reproducibility of them. That's why I've included this cost centre section. Biometric experts may have a different view than mine. Here is my guesstimate on this cost centre.

Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Automation of Forensic Biometric Collection Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Discuss with the academic and biometric industry communities the potential requirements
  - Then create deliverables, resources, costs and timeline estimates to do the research/testing
- The team should include the following types of people:
  - Automation experts
  - Biometric experts
  - Field experts handling biometric registrations in the field
  - Legal experts
  - Business process experts
  - Security/red team experts
  - CRVS experts
  - Global, independent non-profit experts
  - Notary experts
  - Lesson learnt experts
- Create standards if applicable
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

Research Confirming Fingerprints/Iris Are Enough to Legally Differentiate Human Clones Subcomponent Cost Centre:

Background:

In 2005, I was thinking about a sheep named Dolly i.e., the first mammal cloned in 1996. I was wondering when human cloning appeared, how we'd legally differentiate them? This led to an email discussion with Sir Alex Jefferies, inventor of using DNA for forensics. We both agreed our existing CRVS systems were antiquated requiring use of biometrics. Alec told me that if the clones were genetic twins, biometrics would have to be used, since the DNA would be identical.

At the time, it wasn't possible to obtain a child's fingerprints at birth. In early 2006, I wrote on own my first paper, "**The Challenges with Identity Verification**". In it I proposed use of DNA in the CRVS. I took criticism from others who didn't like the ideas of governments having national DNA databases with which they could potentially profile people. After contemplation, I agreed with the critique.

Fast forward to 2016. In China, the CEO of a large cloning company, Boyalife, currently working towards cloning 1 million cows a year, publicly stated they could clone humans but weren't. At which point, I realized the human cloning genie was out of the bottle. Not all countries signed the 2005 UN agreement on human cloning. I knew at some point in the not-so-distant future, people would clone humans.

Thus, reresearch needs to occur such that CRVS registration procedures using fingerprints and iris to differentiate identical DNA clones of Jane Doe 1,2,3,4, etc. will stand up in a court of law.

Research Confirming Fingerprints/Iris Are Enough to Legally Differentiate Human Clones Subcomponent Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre

Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Do a research literature search to determine what research has been done to date on differentiating clones
  - Then discuss with the research and legal community potential requirements to address any gaps
  - Then create deliverables, resources, costs, and timeline estimates to do the research/testing
- The team should include the following types of people:
  - Cloning experts
  - Biometric experts
  - Field experts handling biometric registrations in the field
  - Legal experts
  - Business process experts
  - Security/red team experts
  - CRVS experts
  - Global, independent non-profit experts
  - Notary experts
  - Lesson learnt experts
- Create standards if applicable
- Transfer management of this to the Non-Profit - Manages Legal Identity Standards

CRVS System Subcomponent Cost Centre:

Background:

CRVS systems must be rethought from the ground up, including creating legal identity data standards for:

- Humans (and forensic biometrics for humans)
- AI systems and bots

There are two strategic options, which will directly affect costs:

- Leverage OpenCRVS or,
- Build a new one

Option 1: Leverage OpenCRVS

Plan International has already built an OpenCRVS system, which is currently deployed in Zambia and Bangladesh). Thus, at first glance, this seems the likely place to begin. However, I don't know the following which must be analyzed and considered:

- Data standards
    - I've been told they use HL7 for their data standards
    - This may or may not be fine. What do I mean by this?
    - I haven't yet found what each CRVS jurisdiction around the planet's data standards are
        - Let's hypothetically assume many aren't to HL7 standards
    - Thus, implementation political objections will hypothetically occur when we show up pitching a new CRVS system which uses different data standards then the ones currently used
        - This potentially could be a showstopper, since adopting a HL7 standard might require political changes to laws/regulations and/or social/cultural changes
    - Further, many different business and different level of government and enterprise communities around the planet will consume the SOLICT/LSSI data from the LSSI device TODA file
        - Their systems might or might not be compatible with HL7 data standards and/or other data standards used in CRVS jurisdictions
        - This too could potentially become a showstopper if business communities aren't willing to support the TODA LSSI file standards

- End to end security
  - SOLICT/LSSI creates a CRVS system which becomes a prime target of malicious states and criminals attack vectors
    - Thus, it's highly likely the existing code used will likely have to change after going through a line-by-line coding review
  - End to end security standards need to be applied
    - Thus, existing coding for administrators, registrars, etc. will likely have to be altered
  - Bad news - The initial cost for developing this will likely be high due to the requirement to bring in a wide variety of highly skilled experts
  - Good news – once we have the initial standards, they can be used in subsequent deployments at low cost regarding the actual standards
    - However, depending on the situation on the ground in each jurisdiction, actual implementation costs might be low to high dollar amounts
  - Thus, Plan Internationals Open CRVS system must be analyzed to determine security gaps between what they have today and desired end state security
- Digital app standards
  - Plan International already has a digital interface
    - However, I'm not sure if they will be amenable to changing their existing user interface
  - They also print physical birth certificates
    - I'm not sure if they'll be amenable to altering this to a SOLICT/TODA file both physically and digitally
- Governance model
  - I see the governance being done by a global, non-profit, whose job it is to:
    - Create standards
    - Do 24x7x365 threat assessments
    - Enforce the threat level responses via licensing agreements with jurisdictions and end users
  - I don't know how Plan International/OpenCRVS.org will respond to these
- Existing jurisdictions will have to be migrated
  - I'm not sure how both Plan International and the two jurisdictions will respond to a migration plan
- Legacy data
  - They have a legacy data import function which I'm not sure yet how it works
  - I'm not sure how they'd react when we say we want to automate converting paper and old data structures to the new CRVS data standard
- Creating standardized interfaces with other jurisdictional identity consuming apps
  - OpenCRVS has existing interfaces for other departments/ministries identity systems e.g., health, etc.
  - As per above, the interfaces need to be to agree upon standards and then a code review done to ensure it meets security standards
  - Further, I have an underlying premise that biometrics SHOULD NEVER LEAVE THE CRVS SYSTEM
  - I don't know how Plan International will feel about all the above

- Creating standardized CRVS roll-out costs
  - I'm sure OpenCRVS has standardized roll-out processes of some sort, which I don't know
  - However, I'm proposing establishing biometrics as part of the roll-out, as well as developing security standards for out in the field
  - I'm not sure how Plan International will react to this
- Modify Open CRVS to accept smart digital identities
  - As per pages smart digital identity section of this document, the CRVS system must be designed, where risk warrants it, to register smart digital identities of us, tying them to our underlying legal physical identity
  - I'm not sure how Plan International will react to this
- Create within the CRVS a framework for registering and managing legal identities of AI systems and bots
  - As per pages AI systems/bots section of this document, the CRVS must be designed to register and manage legal identities of AI systems and bots
  - I'm not sure how Plan International will react to this
- Create co-designed citizen interfaces as laid out within this document enabling all citizens, regardless of their abilities or disabilities to interact with their:
  - CRVS jurisdiction including their legal digital signature
  - SOLICT
  - LSSI devices
  - PIAM
  - AI agents/smart digital identities
  - Legal authorization rights
- **Bottom Line**:
  - Very careful study must be done to assess the willingness of Plan International to agree to substantially modify their OpenCRVS system along with the associated costs
  - I'm hoping they'll be amenable or,
  - It may be more cost effective to build it from scratch (see next section)

Option 2: Build a New CRVS System

In parallel to the activities to discuss with Plan International about converting their OpenCRVS system, should be activities to cost estimate building the new CRVS system from scratch.

Suggested Strategy:

- First determine what each jurisdiction around the planet's CRVS data
- Then stand back and consider the end game we're driving at i.e., widespread quick global adoption of a SOLICT/TODA LSSI file
- Then create a strategy which delivers the goods so to speak
- This might include:
    - Adopting HL7
    - Creating a new standard
    - Creating free adaptor type programs which can rapidly convert the SOLICT/LSSI TODA file standard to a different format
    - Etc.
- Then sit down with Plan International to discuss
    - All the above will likely impact costs

REGARDLESS OF WHICH OPTION IS SELECTED, THE NEW CRVS MUST OPERATE TO NEW GLOBAL, LEGAL IDENTITY STANDARDS FOR HUMANS, AI SYSTEMS AND BOTS. Which is where the new, global, independent non-profit comes into play. Skim "Cost Centre - Global, Independent Non-Profit" of this document.

Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

CRVS - CRVS Systems Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to quickly staff a team including:
  - CRVS system experts from the UN and from the Canadian IRDC "Centre of Excellence for Civil Registration and Vital Statistics Systems"
    - By leveraging this time and costs can be quickly shortened to create a global spreadsheet on existing CRVS jurisdictional data standards
  - Law experts on CRVS laws and regulations
  - Biometric experts
  - Database experts
  - AI systems/bots' experts
  - Red team/security experts
  - Connectivity experts
  - Network experts
  - Business process experts
  - Plan International Open CRVS experts
  - Co-Design experts
  - Notary experts
  - Lessons learnt experts
- Create requirements document for the new CRVS
  - Include notary use cases and use cases where a person claims they don't know their place and date of birth
    - Skim "Cost Centre Rethought Notaries"
- Then do an analysis on Plan International's Open CRVS (assuming they're willing)
  - Do a time, work effort and cost analysis
- In parallel, do a build from scratch an analysis
  - Do a time, work effort and cost analysis
- Both the above options require creation of use cases for identity collisions with business processes addressing them which will likely extend across different CRVS jurisdictions
- Come to a decision with 1-3 jurisdictions and funders
- Begin doing small POC's to rapidly prove out sections of the CRVS
  - Learn what doesn't work, what works and quickly redesign
- Create data standards for legal identity data and vital statistics
  - This will be borne in the "Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Standards Subcomponent Cost Centre" section of this document
- Pilot the new CRVS in 1-3 jurisdiction
  - Learn what works and doesn't work in the real world
- Quickly scale
- Transfer this to the global, independent, non-profit

Note:

The costs for either option will be high. Thus, I've created low and high budget scenarios with the low having 200 people to a high of 500 people per annum. I've also allocated large amounts of operating costs ranging from a low of $400 million per annum to a high of $700 million. Experts will change these guesstimates to realistic costs.

CRVS – Manage Digital Signature Entities Standards Subcomponent Cost Centre:

Background:

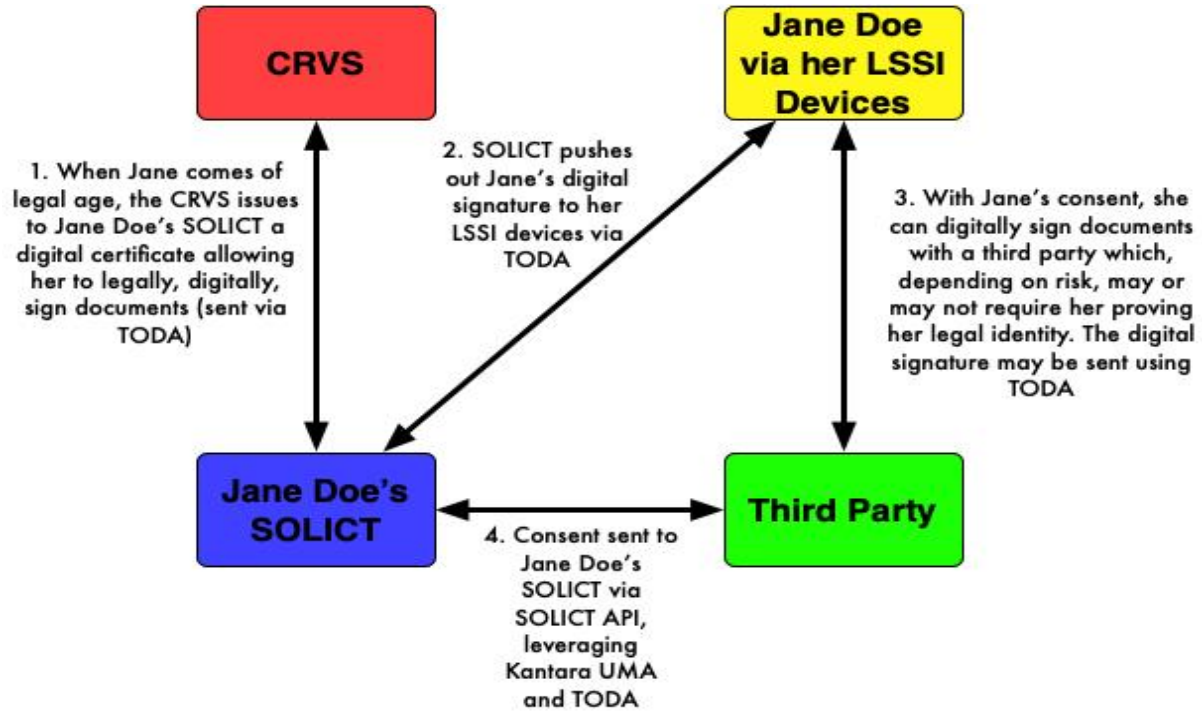
In 1999 Estonia create their "**Identity Document Act**", which requires people 15 years and older to supply their biometrics to then obtain an identity card. They then took this information and leveraged it via the internet using an architecture called X-Road.

Part of their design strategy was to leverage a strong identity assurance of their citizens (via their biometrics) and give adults a digital certificated issued by the state, enabling the citizen to digitally sign documents. Today, over 900 million digital signatures have been used by Estonians, with 91.6 % of the population using the internet regularly. 99% of public services are offered to citizens as e-services.

My strategy is to go beyond what Estonia has pioneered. Today, young children are online, there's now smart digital versions of us appearing, as well as an explosion of AI systems and bots. Thus, from cradle to grave, both physically and digitally, I want to enable legally registered entities around the planet to control their own legal identity and legal digital signature, and use it, anywhere, anytime, as, and when they please, with their consent.

An underlying component therefore is creating a digital signature for each entity on the planet, which is backed by a solid legal identity, which is interoperable, globally recognized.

Vision:



To make this vision a reality requires not only the CRVS, SOLICT, LSSI components but also the ability for the local CRVS to issue digital certificates to a person's SOLICT enabling them to digitally sign documents. That's why I created this subcomponent cost centre.

Finally, a critical factor is citizens, regardless of their abilities or disabilities, to:

- **Understand what their legal digital signature is**
- **Understand how they can use it via their LSSI devices and/or PIAM**

This is where co-design becomes a mission critical piece of the puzzle.

CRVS – Manage Digital Signature Entities Standards Subcomponent Costs:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre, the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre, section of this document.

.

CRVS Data Conversion From Old CRVS Systems to the New Data Format Subcomponent Costs:

Background:

I've been in government CRVS centres where there's boxes stacked from floor to ceiling containing CRVS records. I've also worked for a government where their CRVS data exists in old mainframe systems. I've also heard of other jurisdictions using old PC computers/servers containing CRVS records.

As I see it, after convincing a jurisdiction's political leadership to convert over to the new CRVS/SOLICT/LSSI, PIAM legal identity framework, there's the challenge of enabling them to convert their old data quickly, cost-effectively, efficiently, and securely to the new format. How can this be done?

Bots Plus Automation:

I can see both physical and virtual bots being used to do this. Hypothetically, they can quickly convert old paper-based systems, mainframes et al to digital. It needs to rapidly be POC (proof of concept), mistakes learnt, retested, piloted, and then designed to rapidly scale, securely, cost effectively.

My strategy is to have funders and the global, independent, non-profit offer to a jurisdiction signing up for the new CRVS system, either free or very low cost, use of bots et al to do the conversion to the new system. It removes cost arguments against signing up to implement the new CRVS system.

I'm not saying it all will be easy. What I am saying is the tech now exists to begin leveraging this to rapidly convert old data to a new format. That's why I've broken it out into this subcomponent cost centre.

CRVS Data Conversion From Old CRVS Systems to the New Data Format Subcomponent Costs:

To accurately estimate the costs the following needs to be done:

Create a preliminary budget to:

- Determine high-level requirements
- Find jurisdiction each having one of the following characteristics:
    - Very chaotic paper-based system in the back office i.e., while the present system might be fine, going back 100 years results in wall to ceiling storage of paper-based records in various state of condition
    - A jurisdiction having good paper-based records, in good condition, for the last 100 years
    - A jurisdiction having an old-style PC based CRVS system with assorted paper-based records going back 100 years
    - A jurisdiction having mainframe-based records
- This determines the potential scope of work
- The end state should be to try to automate much of the conversion, rapidly, to a high degree of accuracy, securely, at a low cost
- Budget for creation of a team of people, as a sub-set of the CRVS system including:
    - CRVS experts
    - Legal experts
    - Standards experts
    - Document conversion leveraging AI and machine learning experts
    - Robotics experts – both physical and virtual
    - Researchers in the above fields
    - Business process experts
    - Security/red team experts
    - Notary experts
    - Lesson learnt analysts
- The team's deliverables MUST INLUDE creating a crawl, walk, run strategies i.e., discuss what we can do:
    - "Out of the gate" to get started
    - Parallel, rapid research efforts required to automate
    - Walking steps
    - Running steps
    - Assemble deliverables for each phase, resource requirements, timelines, and costs
- Do rapid POC's, learn what didn't work, what worked, and quickly learn from it
- Do small, tightly controlled pilots in real life to again learn from it
- Rapidly scale
- Transfer management of this to the global, independent, non-profit

CRVS Citizen Co-Design Standards Cost Centre

Background:

When a citizen wants to interact with their CRVS department, it can be bewildering to some. Why? They might have to realize they'll be required to fill in forms for obtaining their registrations, obtaining birth, gender change, name change, marriage, or death certificates or, in the new age CRVS, prove their legal identity relationships with other humans and/or entities, etc.

As per the earlier section of this doc, "**Vision – Co-Design 'Nothing About Us Without Us'**", it lays out why use of co-design, from the outset of design, is critical in delivering government services to the citizen, regardless of their abilities or disabilities. Thus, rather than each local CRVS jurisdiction invent their own citizen interfaces physically and digitally, for accessing records like their birth certificates, gender/name change, marriage/divorce, death, etc., it makes much more sense for the new, global, independent, non-profit to use co-design to create this. As well, it also makes sense for the non-profit to continually update it as this tech change curve occurs and/or new security attacks occur against a CRVS.

All the above is what this cost centre addresses.

CRVS Citizen Co-Design Standard Cost Centre:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS – Smart Digital Identities of Us Subcomponent Cost Centres:

Background:

Skim "**AI Leveraged Smart Digital Identities of Us**". We're in the early days of a major paradigm shift as smart, AI leveraged, digital identities of us are leveraged at home, in the workplace, etc.

The challenges of writing to the smart digital identities source code is exactly the same as for AI systems and bot (refer to the "AI/Bots Source Code Legal Identity/Credential Registration Subcomponent Costs" section of this document).

Smart, AI leveraged digital identities (sometimes referred to as "AI agents") of us can also acquire credentials to work on our behalf. Skim "**Entity Management System**" to see an example of a smart, AI leveraged medical digital identity of nurse or Doctor Jane Doe requiring medical certification. The challenges of issuing credentials to a smart, AI leveraged digital identity will likely be part of issuing them to a physical person (refer to the Credential Standards Body Governance Subcomponent Cost Centre).

All consents given for our smart, AI leveraged, digital identities will be stored in our SOLICT (Source of Legal Identity & Credential Truth)(refer to the SOLICT - Authoritative Identity/Credential Sources Cost Subcomponent).

A person might choose to delegate sections of their authorization rights to one or more of their AI leveraged, smart digital identities (refer to the Legal Authorization Rights Cost Centre).

The AI leveraged, smart digital identity of a person will have as part of it interaction with a person's LSSI (Legal Self-Sovereign Identity) (refer to the LSSI Devices Cost Centre).

All our AI leveraged, smart digital identities will be managed by our PIAM (Personal Identity Access Management) system (refer to PIAM Cost Centre).

Each citizen on the planet, regardless of their abilities or disabilities needs to be able to:

- Understand what their smart digital identities are
- Be able to make decisions on what rights to grant their smart digital identities
- Then to have their LSSI/PIAMS instantly and securely be able to execute this
- Refer to Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

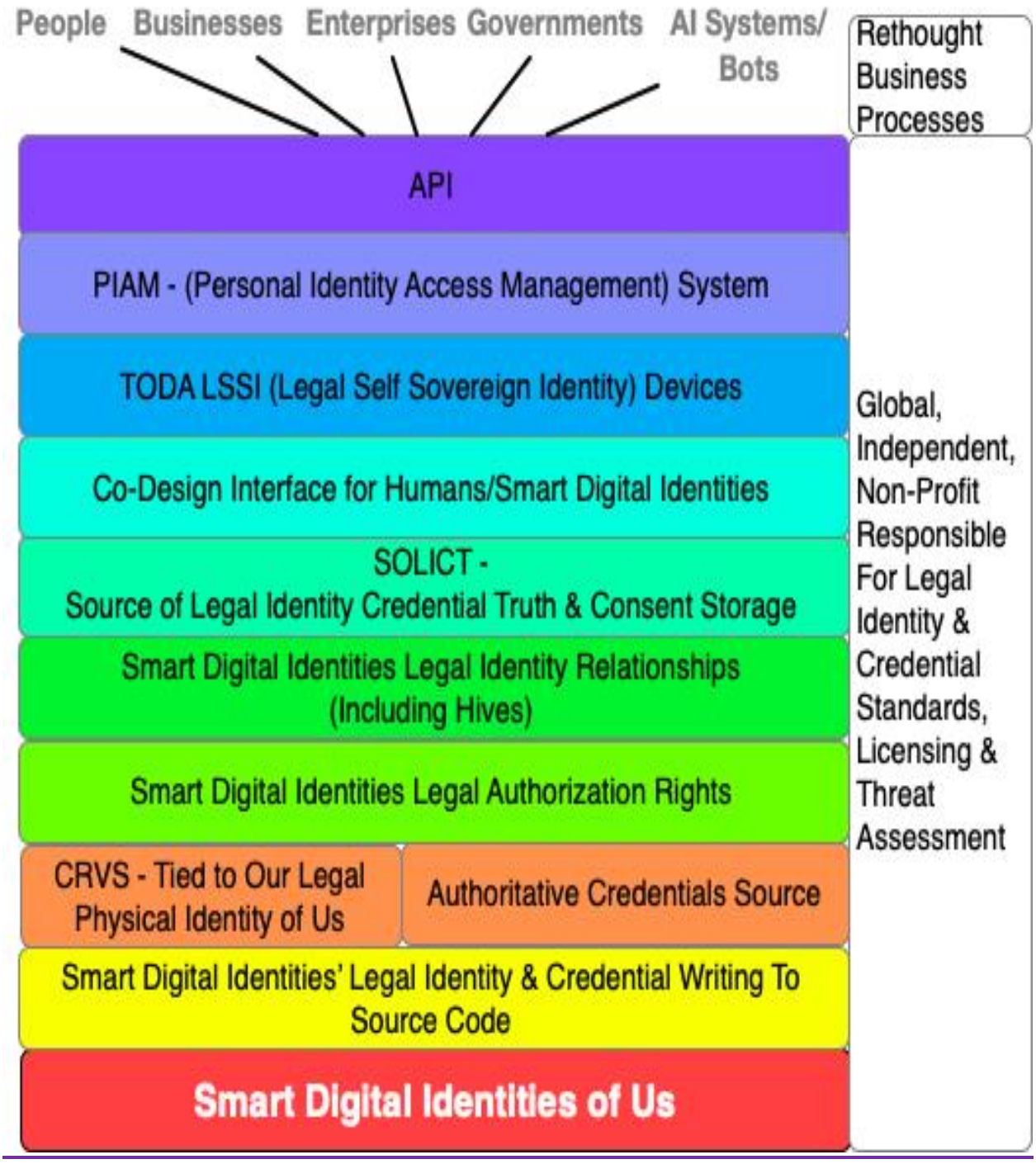
Access to the AI leveraged, smart digital identity will be via the API (refer to the API Cost Centre section of this document).

I note the complexities of these types of entities will likely quickly evolve due to this curve. Thus, so too will the legal complexities in managing these entities.

As I see it, the challenge is quickly establishing legal identification standards, business processes, tech for registering the identities, and integrate this with our SOLICT's, LSSI and PIAM's. As well, new laws and regs will have to be created addressing things like:

- Legal identification status for smart digital identities of us
- Tying these identities to our underlying legal physical identity
- Termination processes for these identities after we die
- Working with insurers and regulators to address the growing threat of digital death

Smart Digital Identities of Us Subcomponent Cost Centres Diagram:



Smart Digital Identities' Legal Identity & Credential Writing To Source Code Subcomponent Cost Centre:

Background:

Read "**AI Leveraged Smart Digital Identities of Us**". It shows a whopper sized wave of change approaching how businesses, enterprises and people do things, leveraging a smart AI enabled digital identity. Depending on risk, it requires abilities to register smart digital identity against the underlying legal physical identity. How will this be done?

High Level Requirements:

The CRVS systems must be able to do the following when we are required to register smart digital identities of us:

- Use business and technical processes to be able to securely query the smart digital entity to see if it already has a legal identity or not
- If it does, it must do a search across all CRVS systems around the planet to confirm the identity is unique
- **If it doesn't, then the business and technical processes to securely write the legal identification into the source code of our smart digital identity - THIS ISN'T A TRIVIAL PROBLEM due to the types of source codes, doing it rapidly in real time from the CRVS, compiling the code, etc.**
- At the same time, the CRVS system must link the smart digital identity of us to our legal physical identity within the CRVS system
- As well, it must be able to write to our SOLICT the linkage to the new smart digital identity by cryptographically cross-linking, via a TODA file, the smart digital identities legal registration within the source code, to our SOLICT file
- Further, the CRVS must then write a TODA capability file to both our SOLICT and our new smart digital identity either one of the two options:
    - If we're of legal age and have sound mind, then giving us control over our smart digital identity of us
    - If we're under legal age or, not of sound mind, then granting our parent/legal guardian or whomever has power of attorney over us, control of our smart digital identity
        - In this case, the parent/legal guardian/power of attorney person's SOLICT files would be updated by the CRVS as well as cross-linking to our SOLICT as well as also writing the capability file to the smart digital identity
- Then we are free to manage the smart digital identity as we please
- Any changes to our legal state (i.e., we require power of attorney, or we die, etc.), then the CRVS system must be updated, under laws and regulations, to update our CRVS record, the smart digital identities records as well as any associated people e.g., legal guardians/power of attorney, etc.
    - When any of these changes are made, the associated SOLICT files and the smart digital identities legal registration files in the source code must also be updated
- When we die, under new laws and regulations pertaining to our smart digital identities, the

Smart Digital Identities' Legal Identity & Credential Writing To Source Code Subcomponent Costs:

Costs will be borne by the AI/Bots Writing to Source Code Legal Identity/Credential Registration Subcomponent costs section of this document since the technical processes are almost identical.

Smart Digital Identities Authoritative Credentials Source Subcomponent Cost Centre:

Background:

In "**Verifiable Credentials For Humans and AI Systems/Bots**", it discusses issuing credentials for our AI leveraged, smart digital identities. As I see it, here are some of the challenges:

1. The credential issuing authority determining if a smart digital identity has the same, reduced, or enhanced credentials than the physical person
2. Given this, determine credential lifespan for the lifetime of the person or their smart digital identity i.e., it might be the same, shorter, or longer
3. Based on this, then differentiating the credential issuance process to the person to new global standards set forth by the new, global, independent, well-funded, non-profit
4. The issuing authority must then validate the person they're issuing the credential to and/or their AI leveraged, smart digital identity and, or digital identities securely write the credential to their underlying source code
5. The person's SOLICT (Source of Legal Identity & Credential Truth), LSSI (Legal Self-Sovereign Identity) and PIAM (Personal Identity Access Management) systems must then be able to manage this
6. All done securely through the person's legal identity & credential API
7. All kept up to date from attacks generated by this curve against all the above
8. All the above is what this cost centre addresses.

Smart Digital Identities Credentials Subcomponent Costs:

The costs will be borne by the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document.

Smart Digital Identities Legal Authorization Rights Subcomponent Costs:

Background:

Read, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" - It explains the use of TODA capability files to extend authorization rights and delegation from one entity to another. The same applies to us and smart digital identities of us.

Thus, when we acquire a smart digital identity which requires legal identity registration, the CRVS will write into our SOLICT database a capability file giving us control over legal identity management of our smart digital identity. At the same time, the CRVS will also write a similar capability file to the smart digital identity's legal identity registration in the source code. Thus, us and our smart digital entity are now enabled to legally manage our own affairs.

One caveat to this is I don't think all our authorization rights we give our smart digital identities should be written to the legal identity registration source code. Why not? Let's use a trite example to illustrate this…

Jane Doe gives her smart digital identity authorization rights to purchase only bananas but not milk from a local store. In real life, the types of authorization granting to a person's smart digital identity will be very vast, potentially complex, and not all require legal permissions to do so.

So, my dumb questions to regulators, smart digital identity vendors, lawyers, privacy folks etc. are how will all of this be handled, stored, archived, and possibly terminated? I don't pretend to have all the answers. What I do know, is we must carefully step into this regarding what we write to the SOLICT, smart digital identities legal identity source code, LSSI and PIAMs. **I caution that early decision we make, will ripple through creating new business, legal and tech processes, which might rapidly become hard to undo.**

Finally, note that all citizens, regardless of their abilities or disabilities:

- MUST understand what a legal authorization right is
- Understand how to use them
- Then make decisions on their own
- With their LSSI devices and/or PIAM's instantly, securely executing this

Smart Digital Identities Authorization Rights Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Manages Authorization Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Smart Digital Identities Legal Identity Relationships (Including Hives) Subcomponent Cost Centre:

Background:

There are several challenges in creating the legal identity relationship within the CRVS system:

1. Creating business processes able to instantly verify entities' legal identities and their legal identity relationships between them
2. Securely creating interfaces into the CRVS system to input and register legal identity relationships
3. CRVS digitally signing each entity's legal identity relationship
4. Ability to perform the above functions at sub-second speeds under what I call "whopper loads" i.e., hundreds of thousands, millions to billions per second
5. Ability to export out the legal identity relationships for each entity to their SOLICTs leveraging TODA files
6. Ability to perform the SOLICT writing functions at sub-second speeds under what I call "whopper loads" i.e., hundreds of thousands, millions to billions per second
7. Ability to keep it all secure as this tech change curve hypothetically generates new attack vectors against the legal identity relationship framework each hour

It will increasingly be likely that smart AI leveraged digital identities of humans will create complex, legal hive relationships with AI system, bots, IoT devices and humans. Skim "**Jane Leverages Her AI Leveraged, Medical Digital Identity Which Is Part of a Hive At Work**" section in "**An Identity Day in the Life of Jane Doe**" to see an example of this.

It's critical that each citizen, regardless of their abilities or disabilities, understands what their smart AI leveraged digital identity is and what legal identity and hive relationships are. This is where co-design comes into play.

Smart Digital Identities Legal Identity Relationships (Including Hives) Subcomponent Costs:

- The costs associated with this will be borne by the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Smart Digital Identities SOLICT Subcomponent Cost Centre:

Background:

When the CRVS registers a smart, AI leveraged, digital identity or makes a change to the legal identity registration, it will write this not only to the CRVS database, BUT ALSO TO OUR SOLICT, as well as to the smart digital identity source code, cryptographically linking us to our smart digital identity and vice-versa. The same applies to credentials issued by credential authorities. Thus, the SOLICT is our source of legal identity and credential truth for us, but also for our smart digital identities of us. Any changes made to the:

- Legal identity of our smart digital identity MUST be written to our SOLICT by the authoritative CRVS system
- Credentials issued to our smart digital identity MUST be written to our SOLICT by the authoritative credential issuing system

I have serious concerns about the performance and security of the end-to-end AI leveraged smart digital identity system:

- Over time, I can see millions of AI leveraged smart digital identities of us being created, validated, and registered simultaneously meaning significant CRVS & SOLICT performance requirements
- Evil Inc.'s and malicious states leveraging this to create new denial of service type attacks against the CRVS and SOLICT system

Citizens, regardless of their abilities or disabilities, must be able to understand:

- **What a smart digital identity is**
- **What's written to their SOLICT about smart digital identities**

ALL OF WHICH MUST BE ADDRESSED BY THE:

- **RED SECURITY TEAMS**
- **THE NEW, GLOBAL, INDEPENDENT, WELL-FUNDED, NON-PROFIT AS THREAT ASSESSMENTS**

Smart Digital Identities SOLICT Subcomponent Costs:

The costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Smart Digital Identities Co-Design Interface for Humans/Smart Digital Identities Subcomponent Cost Centre:

Background:

It's easy to envision AI agents/smart digital identities of us doing many things on our behalf. What's not so easily understood, is how all citizens, regardless of their abilities or disabilities will:

- Understand what an AI agent/smart digital identity of them is
- What it can hypothetically do
- Then grant their consent to the AI agent/smart digital identity to act of their behalf
- Have their LSSI devices and PIAM's execute this securely and instantly on their behalf

THIS IS WHAT CO-DESIGN BRINGS TO THE TABLE. IT'S A MISSION CRITICAL PART OF THE ARCHITECTURE.

Smart Digital Identities Co-Design Interface for Humans/Smart Digital Identities Subcomponent Costs:

The costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Smart Digital Identities TODA LSSI Devices (Legal Self-Sovereign Identity) Subcomponent Costs:

Background:

AI leveraged, smart digital identities of us and our LSSI devices is complicated. Why? Let's use a very poor Jane Doe and her son john Doe as an example.

Both have little to no technology and wear a wristband, biometrically tied to each of them, containing their LSSI and credential information. HOWEVER, in the not-so-distant future, Jane can talk to her wristband. She might have gone to the local CRVS and registered an AI leveraged, smart digital identity of her, to assist her in managing an illness John has. She may or may not have also registered a similar AI leveraged, smart digital identity for John to monitor his health.

Jane might then talk to her LSSI wristband telling it to let her smart digital identity manage certain functions in John's health. This then triggers her PIAM to write a TODA capability file to her smart digital identity. It also writes a TODA capability file to John's PIAM and LSSI devices (how this will occur I don't know but I can see the drive for this making it happen such that John's LSSI wristband becomes updated). In turn John's smart digital identity receives its authorization rights from Jane, via John.

Pick any industry or situation on the planet and one can see the early beginnings of a major paradigm shift. The LSSI is the "front line" of the legal identity and credential system for a person or AI system/bot. It also requires co-design to enable the LSSI device to work for everyone. YES, IT'S COMPLICATED AND REQUIRES LOTS OF THOUGHT.

As noted in the prior section, co-design is critical in enabling all citizens, regardless of their abilities or disabilities to

- **Understand the AI agent's/smart digital identities LSSI devices**
- **Make decisions on their own**
- **And then have the LSSI devices able to execute their consent instantly and securely to the agent/smart digital identity**

Smart Digital Identities LSSI Devices Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Smart Digital Identities PIAM (Personal Identity Access Management) Subcomponent Costs:

Background:

Skim "**An Identity Day in the Life of Jane Doe**". It shows Jane Doe leveraging several different types of AI leveraged, smart digital identities throughout her day. Then skim "**AI Leveraged Smart Digital Identities of Us**" to see the massive paradigm shift heading towards us.

The use of AI leveraged, smart digital identities of us impacts design, use of PIAMs. It also impacts laws and regulations on managing use of PIAMS by AI leveraged, smart digital identities on our behalf.

The PIAMS also become a prime attack vector for the Evil Inc.'s and malicious states of the planet. It's effectively our digital brains. Thus, it requires:

- LOTS of security thought and use cases in the initial design and POC's
- Extensive red security team attacking the PIAM
- Continuous threat analysis by the new, global, independent, well-funded, non-profit

Further, there's the major issue of how all people on the planet will communicate with their PIAM regardless of how they learn, communicate and any disabilities. Thus, co-design becomes critical in design, implementation and maintenance as rapid technical change occurs.

Smart Digital Identities PIAM Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Smart Digital Identity API Subcomponent Cost Centre:

Background:

The API Cost Centre section states the following:

> "Beyond the challenges associated with writing legal identification information to the source code, there's another challenge i.e., how to uniformly access the legal identification within an AI system or bot? I have an idea on how to solve this…
>
> Create a standard AI system/bot legal identity API which can also be inserted into the source code. It addresses the problems of how to query trillions of AI systems and bots, and billions of human legal physical and AI leveraged, smart digital identities, for their legal identities/credentials for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed."

The API is the "electronic front door" to our legal identities and credential information. It becomes a prime attack vector for the Evil Inc.'s and malicious states of the planet. Thus, it requires:

- **LOTS of security thought and use cases in the initial design and POC's**
- **Extensive red security team attacking the PIAM**
- **Continuous threat analysis by the new, global, independent, well-funded, non-profit**

Whatever the final architectural solution agreed to for AI systems/bots will likely be used for smart digital identities of us. Thus, the costs associated with developing this can be amortized over the two cost centres.

Smart Digital Identities API Subcomponent Costs:

The costs will be borne by the Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Costs section of this document.

CRVS Artificial Intelligence and Bots Legal Framework Cost Centre

Background:

Skim these three articles:

- **"The Challenge with AI & Bots - Determining Friend From Foe"**
- **"A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings"**
- **Slides 7-9 in "Underpinnings of a Global, Decentralized ONDC (Open Network for Digital Commerce)" https://hvl.net/pdf/GlobalDecentralizedONDCFinal.pdf or PowerPoint version https://hvl.net/pdf/GlobalDecentralizedONDCFinal.pptx**
- **Page 9 in "Guesstimate Cost Notes: Rethinking Legal Identity & Learning"**
- "AI Can Legally Own a Company!"

They challenges/problems expressed above are crying out for a new legal identity architecture for AI systems and bots. How will this be done down in the coding weeds? The honest answer is I don't know.

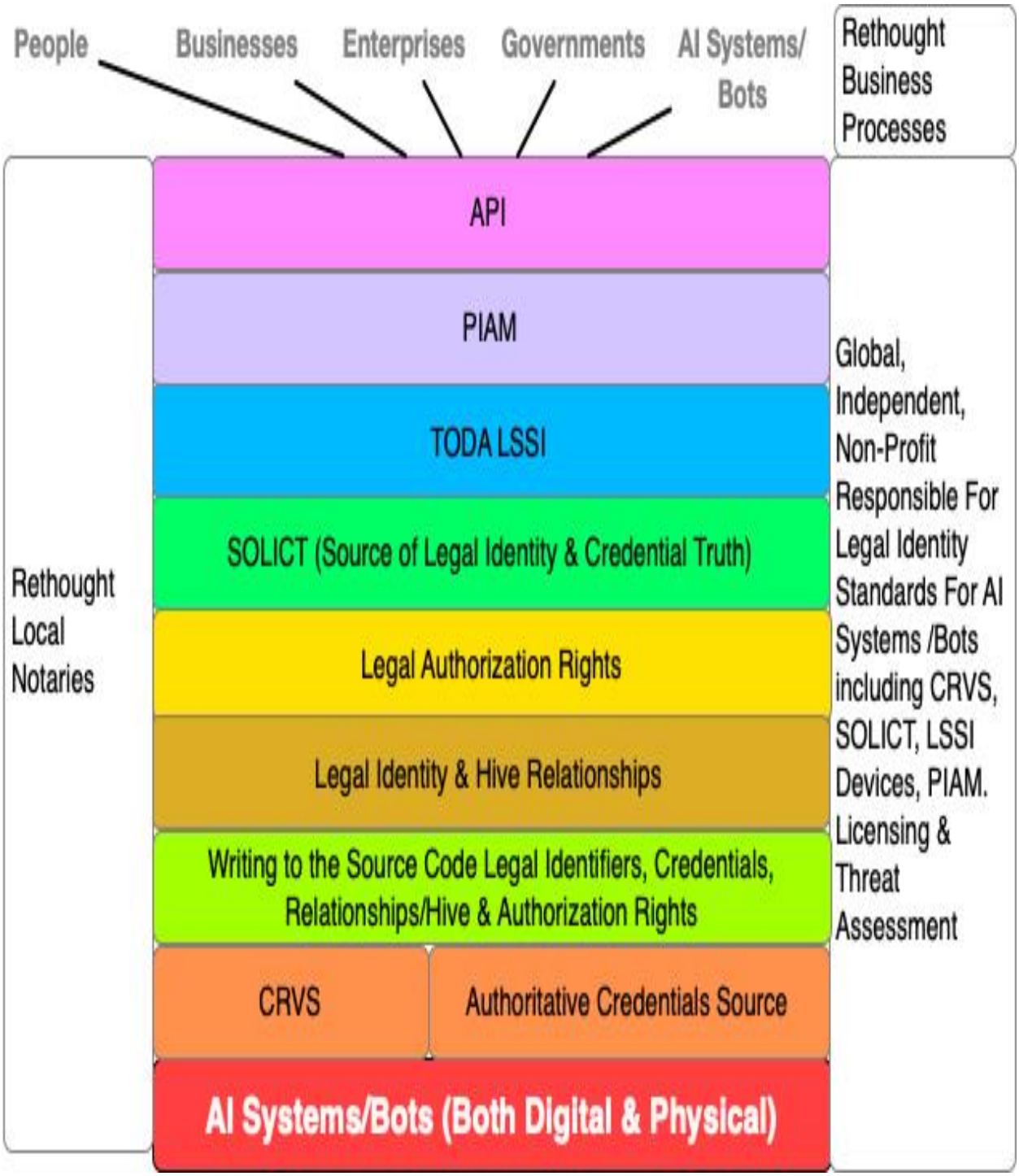
Years ago, I had the idea of creating an identification unit within the source code. Here's the challenge with doing this:

- Can the identification unit code be securely inserted into an AI system or bot source code such that it can't be easily manipulated?
- How will the identification unit data be queried by a person, entity or system wanting to know what it's legal ID is?
- How will any authorization rights assigned to the AI system or bot be attached to the actual legal identity?
- How can all of the above including compiling code be done in fractions of seconds with the CRVS or Credential Issuance Authority sure it's the entity's source code they're writing to?

It requires the brightest technical minds from around the planet to begin drilling into this. Yet, "AI technoids" are not the solution in and of themselves. It also requires some very, very smart, and clever lawyers, business process, security, law makers to get involved." **I suspect, but don't know, it requires creation of a new programming language.**

So, given the fact I'M NOT AN AI EXPERT, what follows in this cost section are simply my best guesses as to how the legal architecture could work and what potential cost centres are associated with it. I will likely be corrected by brighter minds than myself.

AI Systems/Bots High Level Architecture Subcomponent Cost Centres Diagram:



AI Systems/Bots Subcomponent Cost Centre

Background:

Skim this, "**AI, Bots & Us - Examples of Rapid Change**". It's examples at the 100,000-foot level of current AI system and bots. The strategy is to find a funding country then bear down on only 1-2 industry sectors to focus our efforts on. These sectors must include use of AI systems, physical and virtual bots.

I believe the education sector is perfect for this since all the above exists in it. To examples of this skim these articles:

- "**Vision: Learning Journey of Two Young Kids in a Remote Village**"
- "**Sir Ken Robinson - You Nailed It!**"
- "**The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom**"

Health is a highly probable sector to also focus on. To see an example skim this, "**Entity Management System'**.

AI Systems/Bots CRVS Subcomponent Cost Centre

Background:

Why use the human CRVS system to legally register AI systems and bots? Skim these three articles:

- "The Challenge with AI & Bots - Determining Friend From Foe"
- "A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings"
- "**Underpinnings of a Global, Decentralized ONDC (Open Network for Digital Commerce)" https://hvl.net/pdf/GlobalDecentralizedONDCFinal.pdf or PowerPoint version https://hvl.net/pdf/GlobalDecentralizedONDCFinal.pptx.**
- "AI Can Legally Own a Company!"

Then watch this 67-minute video, "The AI Dilemma". Then consider this tech change curve.

Bottom line? These entities, based on risk, require legal identities. Further over time, as these entities acquire more and more human like abilities, as well as also operating as smart digital identities of us, the lines blur between human and AI systems/bots. Thus, it makes cost effective sense to leverage a rethought CRVS system to also register AI systems and bots' legal identities.

If the decision is made to do so, then it makes sense to expand the teams and budgets used for human CRVS systems. That's the assumption the following costs are based on…

CRVS AI Systems/Bots Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a budget for the following team:
  - AI systems, physical and virtual bot experts and vendors in this space
  - Smart digital identities of us experts and vendor in this space
  - Legal AI systems/bots' experts
  - Possibly including university AI/law combined faculty
  - Red team/security experts in attacking AI systems/bots and smart digital identities of us
  - Coding experts
  - Network experts
  - CRVS experts
  - Business process experts
  - Lesson learnt experts
  - Notary experts

- Start with the following parallel sub-projects:
    - Determine legal requirements in laws and regulations within jurisdictions allowing for CRVS systems to function as the legal identity registration source for AI systems/bots
    - Determine use cases for AI systems/bots legal identity registration
    - Determine use cases for identity collisions
    - Determine use cases for exporting out to the entity's SOLICT
    - Determine API requirements for these entities
    - For all the above:
        - Determine potential identify potential attack vectors and determine risk mitigation measures
        - Determine deliverables, costs and create a design/implementation plan
- Do rapid POC's until it works well for all the use cases
- Then do a small, controlled pilot it in 1-3 jurisdictions
- Transition management of this to the global, independent, non-profit

Authoritative AI Systems Bots Credential Sources Subcomponent Cost Centre

Background:

The same assumption made above for leveraging the work of the human CRVS team, should also apply here for determining what authoritative credentials sources are required to certify these entities for different things e.g., teaching credentials, medical credentials, etc. Don't reinvent wheels.

Authoritative AI Systems Bots Credential Sources Subcomponent Cost Centre:

Cost will be borne by the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document.

AI/Bots Writing to Source Code Legal Identity/Credential Registration Subcomponent Costs:

Background:

As noted in **"The Challenge with AI & Bots - Determining Friend From Foe", "A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings** and Page 9 in **"Guesstimate Cost Notes: Rethinking Legal Identity & Learning"** determining exactly how a legal identification can be securely inserted into an AI system/bots source code is not trivial. Why?

- **Speed at which digital entities can be created**
  - Thousands to millions per second, which in the next instance can be operating in all other jurisdictions around the planet
- **Writing to the underlying source code at transactional speeds**
  - Requires the ability of the CRVS system to write to the underlying source code of the entity at whopper speeds, which is then rapidly compiled
- **Security**
  - The unique identifiers written to the source code MUST NOT BE EASILY OBTAINABLE BY THE EVIL INC.'S OF THE PLANET
- **Ability to rapidly query the entity for legal identity and credentials**
  - Requires standards including DNS, endpoint, etc. which the entity is forced to use

Out of all the cost centres within this long document, this one is the most technically challenging and critical. I suspect, but don't know, it requires a new programming language.

For many years, I've been wanting to work with the best and brightest programmers, legal, business processes, security, and governance folks on the planet on this. That's what this cost centre delivers.

1. The same team working on this must also work with the following other teams described in the cost centre document:
   a. CRVS Smart Digital Identity Source Code
   b. Cost Centre: Authoritative Gov't Credentials Source

By solving it for one, it applies to the other.

Cost Centres Dependent Upon This Cost Centre:

- Smart Digital Identities' Legal Identity & Credential Writing To Source Code Subcomponent Cost Centre
- Non-Profit LSSI Standards - Writing LSSI Information to an Entity's Source Code Subcomponent Costs

AI Systems/Bots Writing to the Source Code Legal identity & Credential Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a budget for the following team:
  - AI systems, physical and virtual bot experts and vendors in this space
  - Smart digital identities of us experts and vendor in this space
  - Legal AI systems/bots' experts
  - Possibly including university AI/law combined faculty
  - Red team/security experts in attacking AI systems/bots and smart digital identities of us
  - Coding experts
  - Network experts
  - CRVS experts
  - Business process experts
  - Lesson learnt experts
  - Notary experts
  - Note – this is the same team described in AI Systems/Bots CRVS Subcomponent Cost Centre
- Create ideas on how this can be done and then quickly POC them
- Once successful POC's are obtained for all use cases
  - Pilot it in an industry with 1-3 jurisdictions
  - When it works, then rapidly scale
  - Transfer management of this to the global, independent non-profit

Note: If the funding country already has access to the above, then the costs will plummet.

AI/Bots Legal Identity & Hive Relationships Subcomponent Cost Centre:

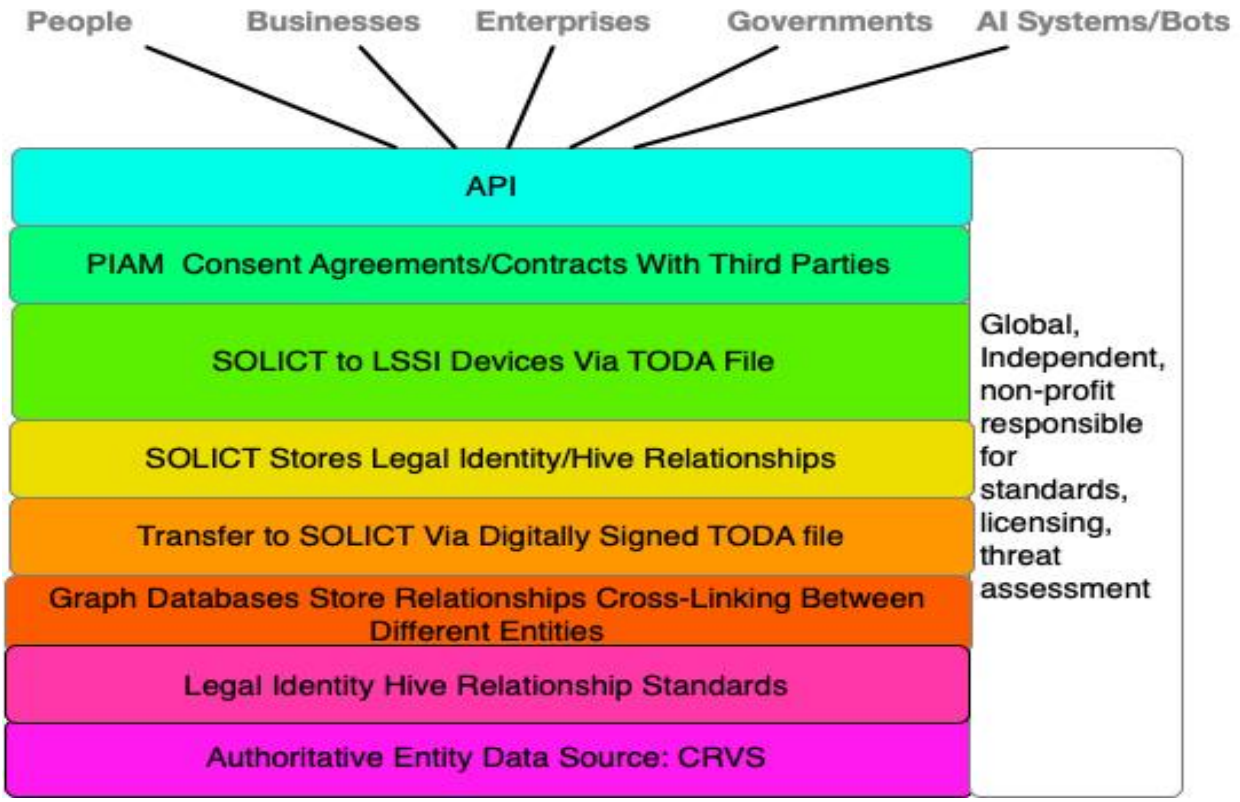
Background:

The Cost Centre – Legal Identity & Hive Relationships, describes the challenges with legal identity & hive relationships. Skim "**An Identity Day in the Life of Jane Doe**" to see how Nurse or Doctor Jane Doe's smart digital identity is in a medical hive relationship with AI systems and bots.

All of which requires out of the box thinking on creating legal identity relationships between AI systems, physical and digital bots, IoT devices and humans. Also note that these relationships might rapidly change. To achieve this requires new architectural toolkits including use of graphs and TODA.

That's what this cost centre addresses for AI systems and bots.

AI Systems/Bots Legal Identity & Hive Relationships Subcomponent Cost Centres Diagram:



AI/Bots Legal Identity & Hive Relationships Subcomponent Costs:

Costs will be borne by Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre section of this document.

AI/Bots Legal Authorization Rights Subcomponent Cost Centre:

Background:

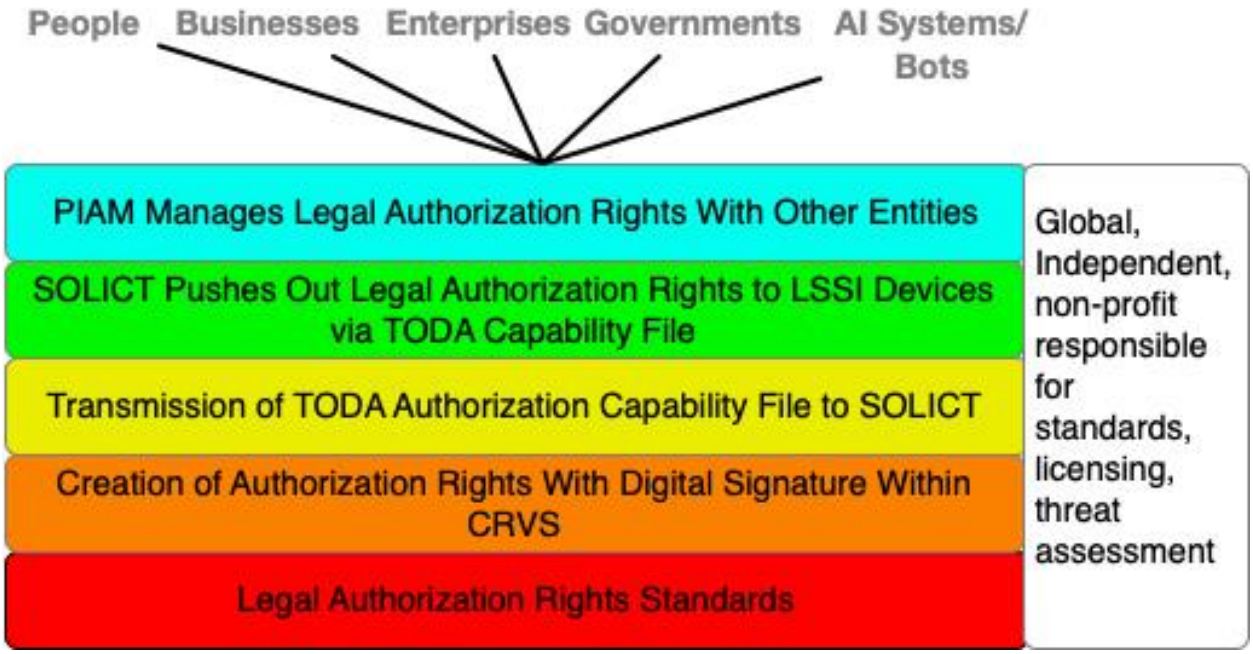
The Cost Centre – Legal Authorization Rights section of this document outlines the challenges with legal authorization. It states:

> "Skim these two articles on AI/AR/VR environments in a global classroom:
>
> - "**Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy**"
> - "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**"
> -
>
> It has a student, John Doe, who has his learning assistant bot "AssistBot", with a human teacher, Sally Goodteacher, and two teaching assistant bots, BobBot and PattyBot. Further, contracts need to be created on the fly between not only John's parent Jane Doe, for him and his AssistBot, his school district, other school districts, Sally Goodteacher, BobBot and PattyBot, that specifies what data can be used by whom, how it's used, stored, shared, archived, and terminated.
>
> So, an AI system, physical and/or digital bots will require authorization rights, which depending on risk, must be spelled out in contracts. My dumb question is how will this be done in a secure, scalable manner? Where will the contracts pertaining to a specific legal identity AI systems or bots be stored? **Yes, it's complicated. That's the world we're entering."**

It also discusses TODA capability files. All of which will be creating new laws and regulations for legal authorization for AI systems and bots.

All the above is what this cost section addresses.

AI Systems/Bots Legal Authorization Rights Subcomponent Cost Centres:



AI/Bots Legal Authorization Rights Subcomponent Costs:

Costs will be borne by Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre section of this document.

AI/Bots SOLICT (Source of Legal Identity & Credential Truth) Subcomponent Cost Centre:

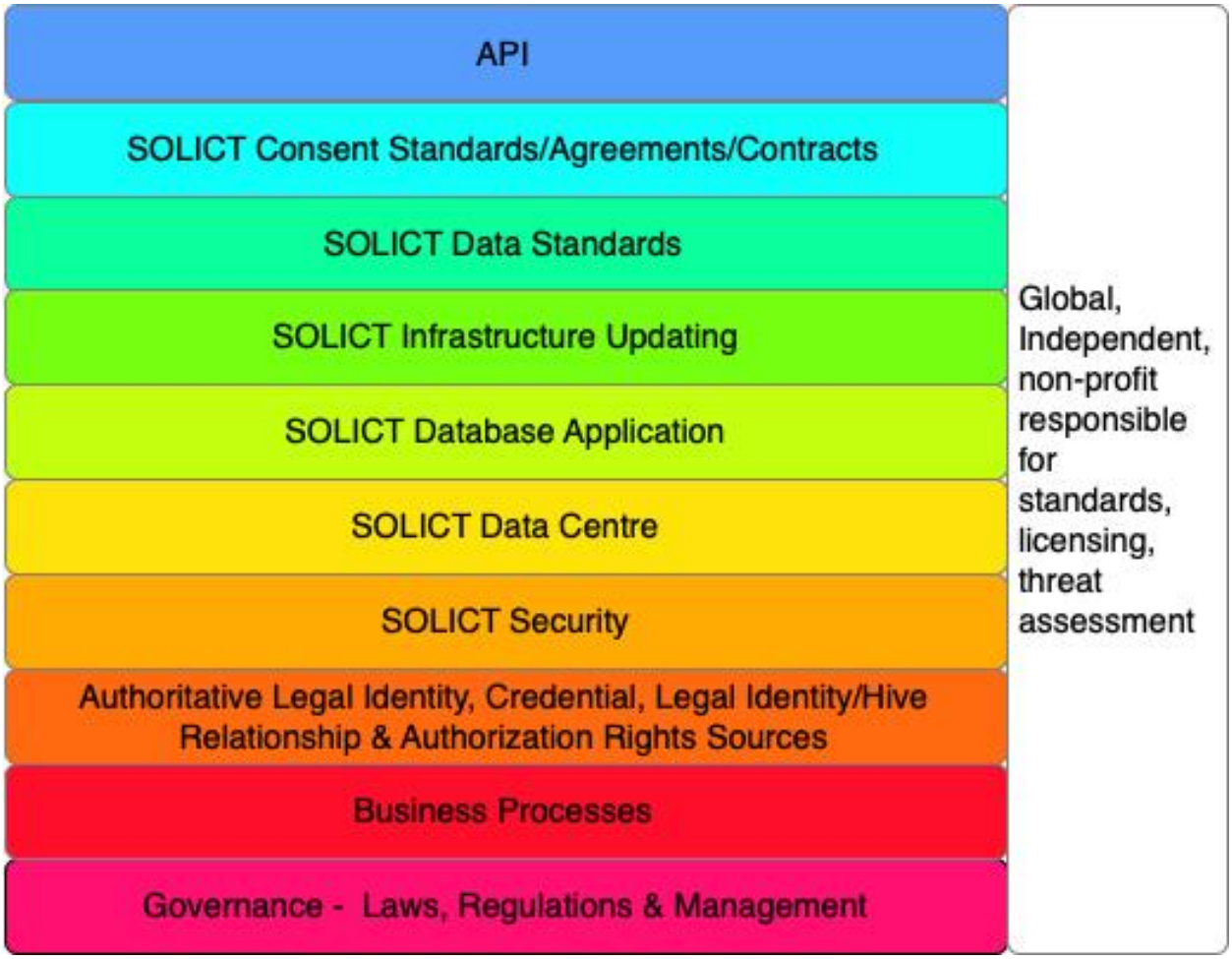
Background:

In the SOLICT section of "**Creating AI Systems/Bots Legal Identity Framework**" it states the following:

> **"Description:**
>
> When architecting for a new legal identity system for AI systems and bots, I wanted to build it from the ground up on privacy by design. Thus, as in the human legal identity architecture, I wanted to prevent a malicious jurisdiction from deleting all legal identity information from their databases about an AI system or bot. Thus, I wanted to leverage the SOLICT as in the human legal identity architecture.
>
> **YET, THERE'S SOME MAJOR WHOPPER SIZED PROBLEMS/CHALLENGES THAT COME WITH THIS. LIKE WHAT? PERFORMANCE AND SECURITY.**
>
> **Performance:**
>
> I could see in my mind the awesome speeds at which say digital bots can be created. Over time, it could easily be in the millions or billions per second/. Thus, I saw the CRVS local/global systems struggling not only with registration/validation performance, BUT ALSO CREATING A SOLICT FOR EACH NEW ENTITY. Thus, this must be addressed in design use cases.
>
> **Security:**
>
> I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks against the new age CRVS systems. They could effectively "drown the CRVS" with creations of new entities and sending out to the global, independent non-profit, who's managing the SOLICTS, LOTS of SOLICT creations. Thus, this must be addressed in design use cases.
>
> **Updating:**
>
> Finally, I could also see the business process problems of keeping track of billions or more AI system and bots legal identities. How would the CRVS be able to be notified an entity had changed, been adopted into another entity, terminated, etc. and then how would it notify the entity's SOLICT? Thus, this must be addressed in design use cases.
>
> **My message? All of the above problems/challenges are whopper sized. LOTS OF THOUGHT MUST BE APPLIED BEFORE LEADING TO DESIGN AND POC'S. Caveat emptor**."

THIS COST CENTRE MUST ADDRESS ALL THE ABOVE.

AI Systems/Bots SOLICT Subcomponent Cost Centres Diagram:



AI Systems/Bots SOLICT Subcomponent Costs:

The costs associated with this will be born in the SOLICT Cost Centre section of this document**".**

AI/Bots TODA LSSI (Legal Self-Sovereign Identity) Subcomponent Cost Centre:

Background:

In the TODA LSSI section of "**Creating AI Systems/Bots Legal Identity Framework**" it states the following:

Description:

As with the human legal identity architecture, I wanted to enable entities to manage their own legal identities. Thus, as in the human legal identity architecture, the AI systems/bots architecture leverages LSSI.

However, there are likely differences between the Ai system/bot architecture of LSSI vs humans:

- Unlikely to leverage paper based legal identification LSSI
- Won't use biometric wristbands to tie the entity to their wristband containing their LSSI

As noted in the SOLICT section, I also realized similar whopper sized challenges with creating LSSI for AI systems and bots:

Performance:

I could see in my mind the awesome speeds at which say digital bots can be created. Over time, it could easily be in the millions or billions per second/. Thus, I saw the new global, independent non-profit managing the SOLICT LSSI creations likely having performance challenges. Thus, this must be addressed in design use cases.

Security:

I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks against the new global, independent non-profit. They could effectively "drown the CRVS" with creations of new entities and sending out to the global, independent non-profit, who's managing the SOLICTS, LOTS of SOLICT/LSSI creations. Thus, this must be addressed in design use cases.

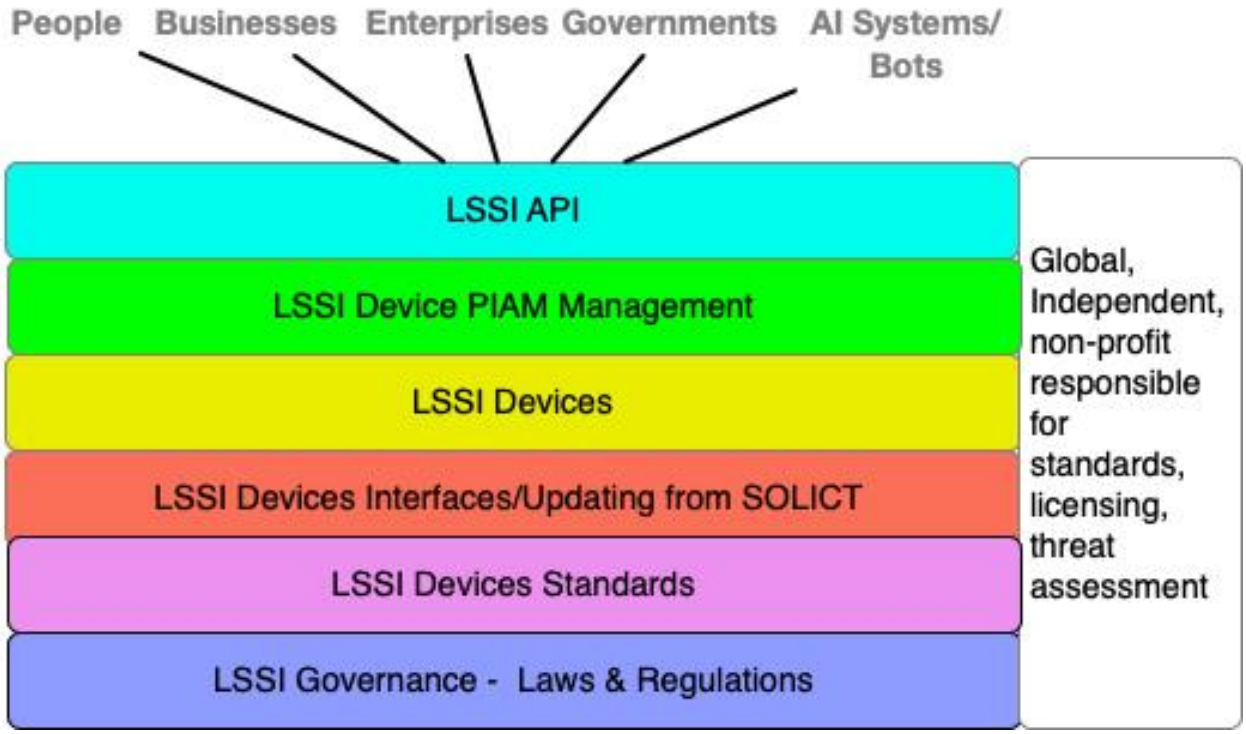
My message? All the above problems/challenges are whopper sized. LOTS OF THOUGHT MUST BE APPLIED BEFORE LEADING TO DESIGN AND POC'S. Caveat emptor.

THIS COST CENTRE MUST ADDRESS ALL THE ABOVE.

AI/Bots TODA LSSI (Legal Self-Sovereign Identity) Subcomponent Costs:

Costs will be borne in the LSSI Devices Cost Centre section of this document.

AI Systems/Bots LSSI Subcomponent Cost Centres Diagram:



AI Systems/Bots LSSI Subcomponent Costs:

The costs associated with this will be born in the LSSI Cost Centre section of this document**.**

AI/Bots PIAM (Personal Identity Access Management) Subcomponent Cost Centre:

Background:

In the PIAM section of "**Creating AI Systems/Bots Legal Identity Framework**" it states the following:

Description:

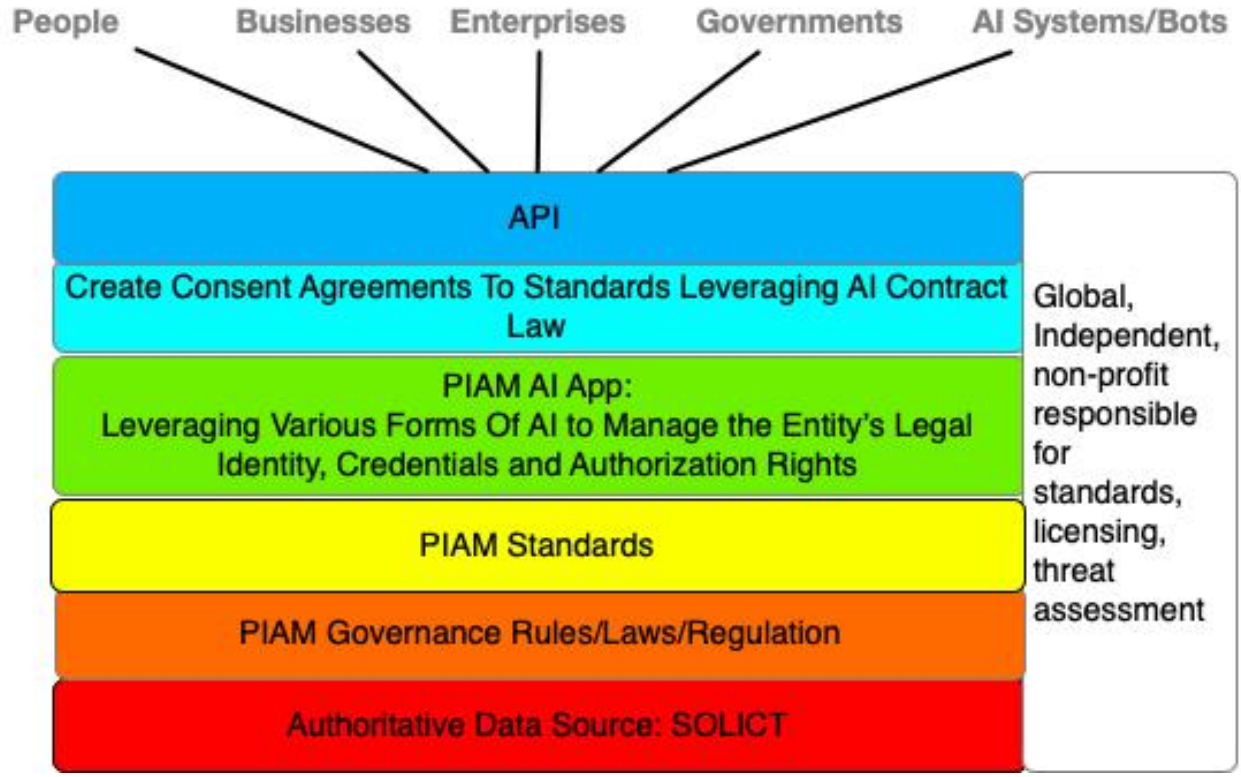
As with the human legal identity architecture, I wanted each entity to have the ability to be in control of their legal identity and consent information. My vision was to create an AI leveraged PIAM able to manage these activities.

Now making this vision become a reality requires security standards, since the PIAM will become a prime point of attack by criminals. Further, given this curve, it means today's best security standards can quickly become tomorrow's turd. Which is why the architecture calls out for PIAM standards to be managed by the global, independent non-profit, which also does 24x7x365 threat analysis against it. Thus, the architecture is designed to constantly keep the PIAM secure.

Finally, I can easily see where companies will want to produce PIAMS for not only humans but AI systems and bots. Why? It puts them closest to their customers be they human or AI systems/bots. My goal in creating the architecture is to adopt PIAM standards:

- Protecting an entity's PIAM regardless of who provides it
- Allowing companies to innovate, leveraging AI, and rapidly feeding this back into PIAM standard changes"

AI System/Bots PIAM Subcomponent Cost Centres Diagram:



AI Systems/Bots PIAM Subcomponent Costs:

The costs associated with this will be likely be born in the PIAM Cost Centre section of this document.

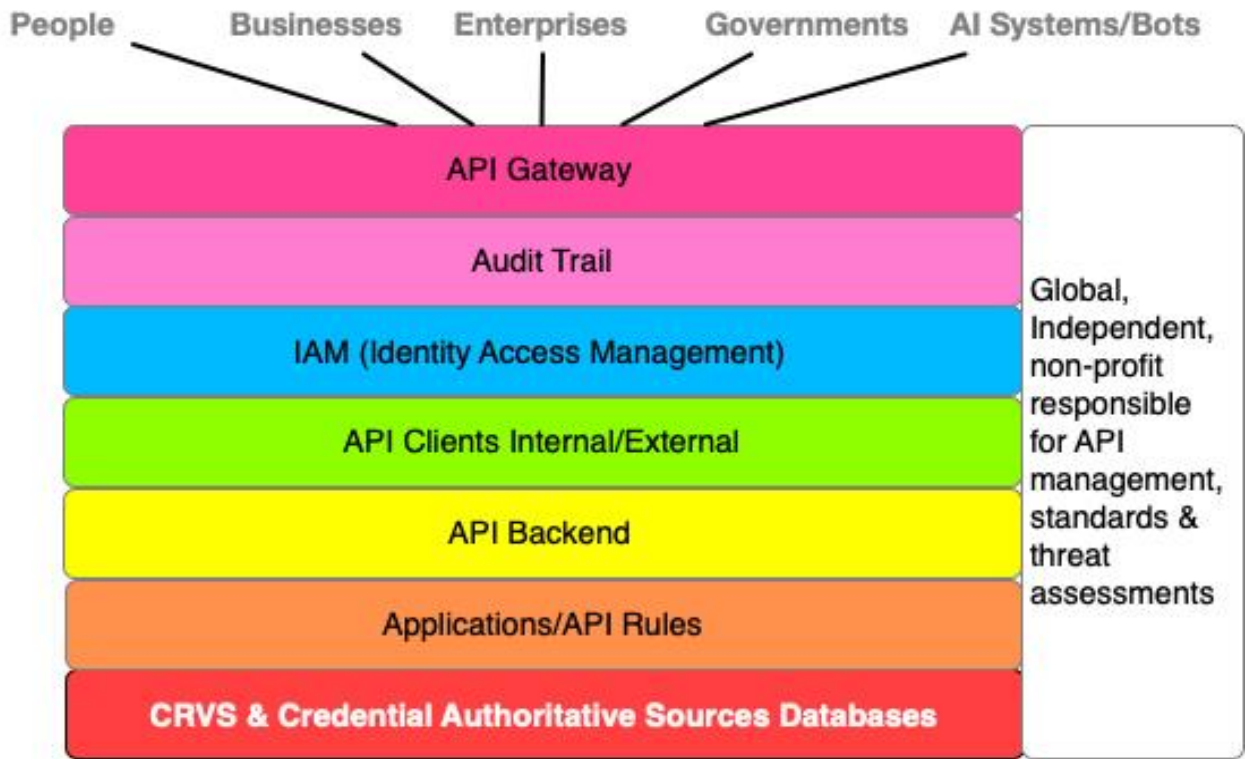
AI System/Bots API Subcomponent Cost Centre:

Background:

In the API section of "Creating AI Systems/Bots Legal Identity Framework" it states the following:

> **"Description:**
>
> Beyond the challenges associated with writing legal identification information to the source code, there's another challenge i.e., how to uniformly access the legal identification within an AI system or bot? **I have an idea on how to solve this…**
>
> Create a standard AI system/bot legal identity API which can also be inserted into the AI system/bot source code. Hypothetically, it can be designed to be very secure. It addresses the problems of how to query trillions of AI systems and bots for their legal identities and/or for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed."

AI System/Bots PIAM Subcomponent Cost Centres Diagram:



AI Systems/Bots Legal Identity API Subcomponent Costs:

The costs associated with this will borne by the API Cost Centre section of this document.

CRVS Legal Identity & Hive Relationships Framework Cost Centre

Background:

Skim this article, "**Legal Identity Relationships**". It describes the current planetary mess in proving one's legal identity relationship. It also describes the rapidly emerging world of "hive relationships". The article states:

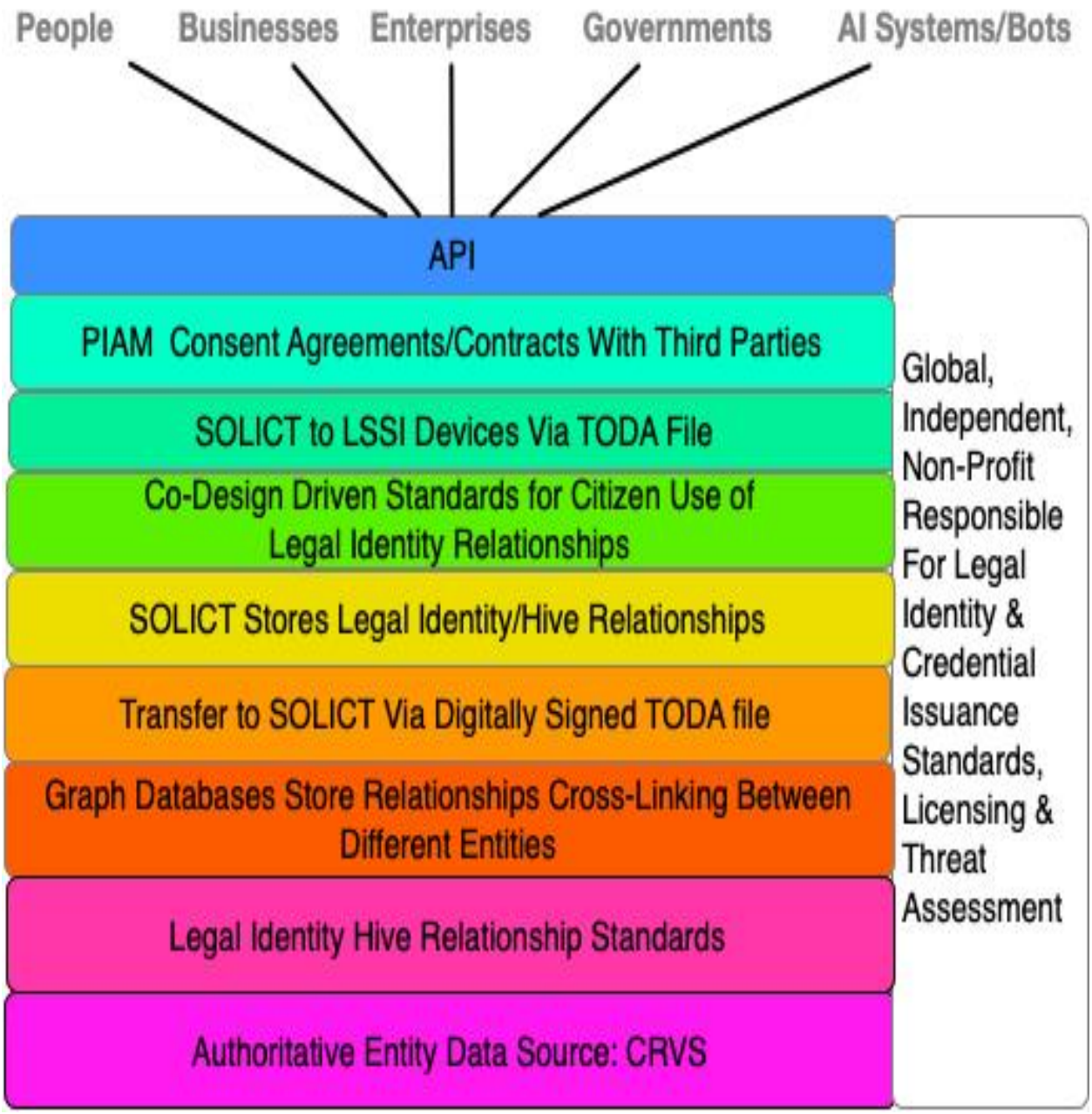
> "Watch this video about a bot hive. Then skim this article about AI leveraged smart digital identities of us. Now come with me on a short mental journey...
>
> - Jane or John Doe could have 1 or many different, AI leveraged, smart digital identities which
> - Belong to a hive with one or more AI systems which
> - Also includes one of more physical bots which
> - Also includes one or more digital bots which
> - Also includes one or more IoT devices
>
> Where legal risk warrants it, the legal identity relationship amongst each of the entities with the hive must be registered. Then consider this article, "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**". It means, in the not-so-distant future, hive entity relationships might only last seconds, minutes, hours, days, weeks, months or years. YIKES!!!!!
>
> Thus, it requires an extraordinary fast CRVS system with the ability to map one to one, one to many, and many to many legal identity relationships. Enter graphs as described above.
>
> Yes, it's darned complicated. New architectural tools are required by the new age CRVS."

New Toolkit Required:

Read "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**". It describes graph databases. Graphs are the tools to use in rapidly mapping and managing complex one to one, one to many, and many to many relationships. Thus, the proposed CRVS architecture leverages this.

Further, the CRVS MUST export the legal identity relationships out to each entity's SOLICT. This is done leveraging TODA files, which can perform at transactional speeds. The SOLICT in turn pushed the legal identity information out to the entity's LSSI devices using TODA files.

CRVS Legal Identity & Hive Relationships Subcomponent Cost Centres Diagram:



CRVS Legal Identity & Hive Relationships Authoritative Data Source CRVS Subcomponent Cost Centre

Background:

There are several challenges in creating the legal identity relationship within the CRVS system:

1. Creating business processes able to instantly verify entities' legal identities and their legal identity relationships between them
2. Securely creating interfaces into the CRVS system to input and register legal identity relationships
3. CRVS digitally signing each entity's legal identity relationship
4. Ability to perform the above functions at sub-second speeds under what I call "whopper loads" i.e., hundreds of thousands, millions to billions per second
5. Ability to export out the legal identity relationships for each entity to their SOLICTs leveraging TODA files
6. Ability to perform the SOLICT writing functions at sub-second speeds under what I call "whopper loads" i.e., hundreds of thousands, millions to billions per second
7. Ability to keep it all secure as this tech change curve hypothetically generates new attack vectors against the legal identity relationship framework each hour.

Skim "**Jane Leverages Her AI Leveraged, Medical Digital Identity Which Is Part of a Hive At Work**" in "**An Identity Day in the Life of Jane Doe**" –to see an example of how it will be used.

CRVS Legal Identity & Hive Relationships Authoritative Data Source CRVS Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre section of this document.

CRVS - Legal Identity Hive Relationship Standards Subcomponent Cost Centre:

Background:

Creating legal identity relationship/hive standards requires a new toolkit including Graphs and TODA. Hypothetically, legal identity relationships can be defined within the CRVS via graph relationships and encryption cross-linking to different entities. Then this can be exported out to the SOLICT via a TODA capability file. All of which requires standards. That's what this cost centre addresses.

CRVS - Legal Identity Hive Relationship Standards Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre section of this document.

CRVS Legal Identity & Hive Relationships - Graph Databases Store Relationships Cross-Linking Between Different Entities Subcomponent Cost Centre

Background:

In the 90's LDAP (lightweight Directory Access Protocol) was adopted by the emerging identity industry to act as a central enterprise hub for identities. Authoritative data sources like HRMS (Human Resource Management Systems), CRM (Customer Relationship Management), etc. fed the central LDAP. On top of the LDAP was built IAM (Identity Access Management) systems.

This is still the architecture used today. As discussed in "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" it's not going to work today. I have a friend, Derek Small, whose company, Nulli, for the past several years has been deploying graph databases together with IAM systems to handle fast changing relationships between entity identities and data.

I like graphs and have built them into the architecture, especially for legal identity relationships. **HOWEVER, I have some concerns:**

- Sheer speed at which an AI system can create digital bots requiring creation of legal identity hive relationships i.e., thousands to millions or more per second – can graphs work at this speed?
- Hypothetically high-volume identity relationship/hive validations in the CRVS system – can graph systems cope with this? What volume do they "crap out"?
- Danger of DNS (Denial of Service) type attacks on the CRVS system from the Evil Inc.'s and malicious states of the planet – graphs are part of the end-to end CRVS system. How will these attack be mitigated?

All the above must be addressed in the design and implementation of graphs within the CRVS system.

Other Cost Centres Dependent Upon This Cost Centre:

- Legal Identity & Hive Relationships - Graph Databases Store Relationships Cross-Linking Between Different Entities Subcomponent Cost Centre

CRVS Legal Identity & Hive Relationships - Graph Databases Store Relationships Cross-Linking Between Different Entities Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - AI systems, physical and virtual bot experts
  - Smart digital identities experts
  - Industry vendors in both the AI systems/bots as well as smart digital identities space
  - Coding experts
  - Legal AI systems/bots experts
  - Legal identity relationship experts
  - Identity graph database experts
  - Business process experts
  - Security/Red team experts
  - Standards experts
  - Network/connectivity experts
  - Notary experts
  - Co-design experts
  - Lesson learnt experts
  - DNS and encryption experts
- Create legal identity relationship and hive use cases
- Then do quick POC's to see what works and what doesn't work
- Adjust new legal identity/hive relationship standards based on what works and doesn't work in graphs
- Pilot it in 1-3 industries/jurisdictions
- When it works, then rapidly scale
- Transfer this to the global, independent non-profit

CRVS Legal Identity & Hive Relationships - Transfer to SOLICT Via Digitally Signed TODA file Subcomponent Cost Centre

Background:

While architecting for the legal identity relationship/hives, I knew in my head there was some problems/challenges to be overcome:

- What global/local legal identity/hive relationship standards would need to be created?
- How would these be securely exported out of the CRVS to the entity's SOLICT
- Since many of the new emerging hive entity relationships would be fast changing, how would this be done at fast transactional speeds?
- Security implications of all the above. As mentioned in other sections of this doc, I was wondering of how to mitigate of DNS type attacks (denial of service) on the new, global, independent non-profit who's managing the SOLICTS in the global cloud?

Enter TODA Files and New Local/Global Legal Identity Relationship & Hive Standards:

Read, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**". It describes how TODA:

- Can work at transactional speeds
- Containing a TODA file which could be anything

When I saw this, I knew it was a new foundational piece of the new legal identity architecture.

If new local/global standards are created for legal identity and hive relationships, then the TODA file can carry it from the CRVS endpoint to the entity's SOLICT endpoint. Thus, it can be proved on X date, at Y time, a TODA CRVS legal identity/hive file containing a hash of the file as well.

CRVS Legal Identity & Hive Relationships - Transfer to SOLICT Via Digitally Signed TODA file Subcomponent Graph Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - AI systems, physical and virtual bot experts
  - Smart digital identities experts
  - Industry experts in AI systems/bots, smart human digital identities
  - Coding experts
  - Legal AI systems/bots experts
  - Legal identity relationship experts
  - Identity graph database experts
  - Business process experts
  - Security/Red team experts
  - Standards experts
  - Network/connectivity experts
  - Notary experts
  - Lesson learnt experts
  - DNS and encryption experts
  - SOLICT experts
  - Co-design experts
- Create legal identity relationship and hive standards for TODA files
- Then do quick POC's leveraging TODA files to see what works and what doesn't work
- Pilot it in 1-3 industries/jurisdictions
- When it works, then rapidly scale
- Transfer this to the global, independent non-profit

CRVS Legal Identity & Hive Relationships - SOLICT Stores Legal Identity/Hive Relationship Subcomponent Cost Centre:

Background:

The design of the SOLICT MUST be able to:

- Handle complex one to one, one to many and many to many legal identity/hive relationships
- Be able to perform at high speeds
- Be secure from outside attacks

Enter Graphs:

As described above, graphs are the right tool to use for this within the CRVS, assuming they can work at very high transactional type speeds with writes and lookups (mostly from AI leveraged, smart digital identities of humans wanting to confirm hive relationships). It also requires the new, global, independent, well-funded, non-profit to continually perform attack vector threat analysis.

Co-Design and SOLICT:

Citizens, regardless of their abilities/disabilities, need to be able to understand what legal identity and hive relationships are stored within their SOLICT. That's who co-design brings to the table.

CRVS Legal Identity & Hive Relationships - SOICT Legal Identity/Graph Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

.

CRVS Legal Identity & Hive Relationships - Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Subcomponent Cost Centre:

Background:

Citizens, regardless of their abilities or disabilities, must be able to understand legal identity relationships. Then they can make their own decisions on who to share their legal identity relationships with, and their LSSI devices and/or PIAM can securely, instantly execute this. That's what co-design brings to the table.

CRVS Legal Identity & Hive Relationships - SOLICT to LSSI Devices Via TODA File Subcomponent Costs:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS Legal Identity & Hive Relationships - SOLICT to LSSI Devices Via TODA Files/LSSI Subcomponent Cost Centre:

Background:

As described in "TODA Files Containing Legal Identity Relationship Sent to SOLICT CRVS Subcomponent Cost Centre" the challenges are how to securely transmit legal identity relationships/hive data. TODA is a good fit. Thus, the SOLICT MUST transmit this data to the LSSI devices leveraging standardized TODA legal identity/hive files.

As mentioned in SOLICTs, the same problems occur for ensuring the transmission is secure:

- This is where the new, global, independent, non-profit comes into play doing 24x7x365 continual threat assessments

Then there's the challenge of how the legal identity/hive data is securely stored within the LSSI devices:

- The design teams must address this

A critical piece of LSSI devices is how many different citizens, with many different learning styles, communication abilities and disabilities will be able to manage their LSSI devices. This is where co-design is a critical component.

CRVS Legal Identity & Hive Relationships - SOLICT to LSSI Devices Via TODA File Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre, the Cost Centre: API (Application Programming Interface) and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS Legal Identity & Hive Relationships - PIAM Consent Agreements/Contracts with Third Parties (Personal Identity Access Management) Subcomponent Cost Centre

Background:

Skim "**An Identity Day in the Life of Jane Doe**". It describes how Jane leverages her PIAM to give consents as well as to add in a new digital bot to a medical hive she's legally part of.

Next, look at this diagram showing how Jane Doe leverages PIAM to prove to a school district her legal identity relationship with her son John Doe and his learning assistant bot, AssistBot.

Then look at this diagram showing hive relationships, PIAM's, SOLICTs, etc.

The PIAM is the entity's "electronic brain" deciding who to release and not release legal identity relationship/hive data to. It becomes a very attractive attack vector target by the Evil Inc.'s and malicious states of the planet. Thus, performance and security are vital. All of this is what this cost centre addresses.

A critical piece of PIAM's is how many different citizens, with many different learning styles, communication abilities and disabilities will be able to manage their PIAM. This is where co-design is a critical component.

CRVS Legal Identity & Hive Relationships - PIAM Consent Agreements/Contracts with Third Parties Subcomponent Costs:

These costs will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS Legal Identity & Hive Relationships - SOLICT/LSSI API (Application Programming Interface) Subcomponent Cost Centre:

Background:

The API is the electronic front door to the PIAM and LSSI. If it's not secure, then Evil Inc.'s and malicious states will leverage weaknesses to access data like legal identity and hive relationships.

CRVS Legal Identity & Hive Relationships – API Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – API Subcomponent Cost Centre and the Non-Profit – API Rule Sets Subcomponent Costs section of this document.

CRVS – Legal Authorization Rights Cost Centre:

Background:

As AI systems, bots, and AI leveraged, smart digital identities of us emerge in large numbers, there's a challenge few people are even thinking about – authorization rights and the ability for an entity to delegate sections of them. Consider this example…

Jane Doe's son, John Doe is attending school. John has a learning assistant bot, AssistBot. How can:

- Jane delegate some of her authority, as John's mother, to the school district agreeing what sections of John's legal identity, biometric and behavioral data can be used by the school?
- Jane assign authorization rights to the school, to take some of John's learning data from AssistBot into their LMS (Learning Management System)?
- How can Jane and John's teacher, Mary Goodteacher, assign some of John's learning data to a global, AI/VR learning environment Mary teaches in with John?

Today, there isn't any legal identity framework on the planet for this which works locally and globally.

Vision:

Skim these two articles:

- "**Entity Management System**"
- "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"

They show how TODA capability files can be used to be assigned and delegate sections of an entity's authorization rights. It's out of the box thinking for out of the box times.

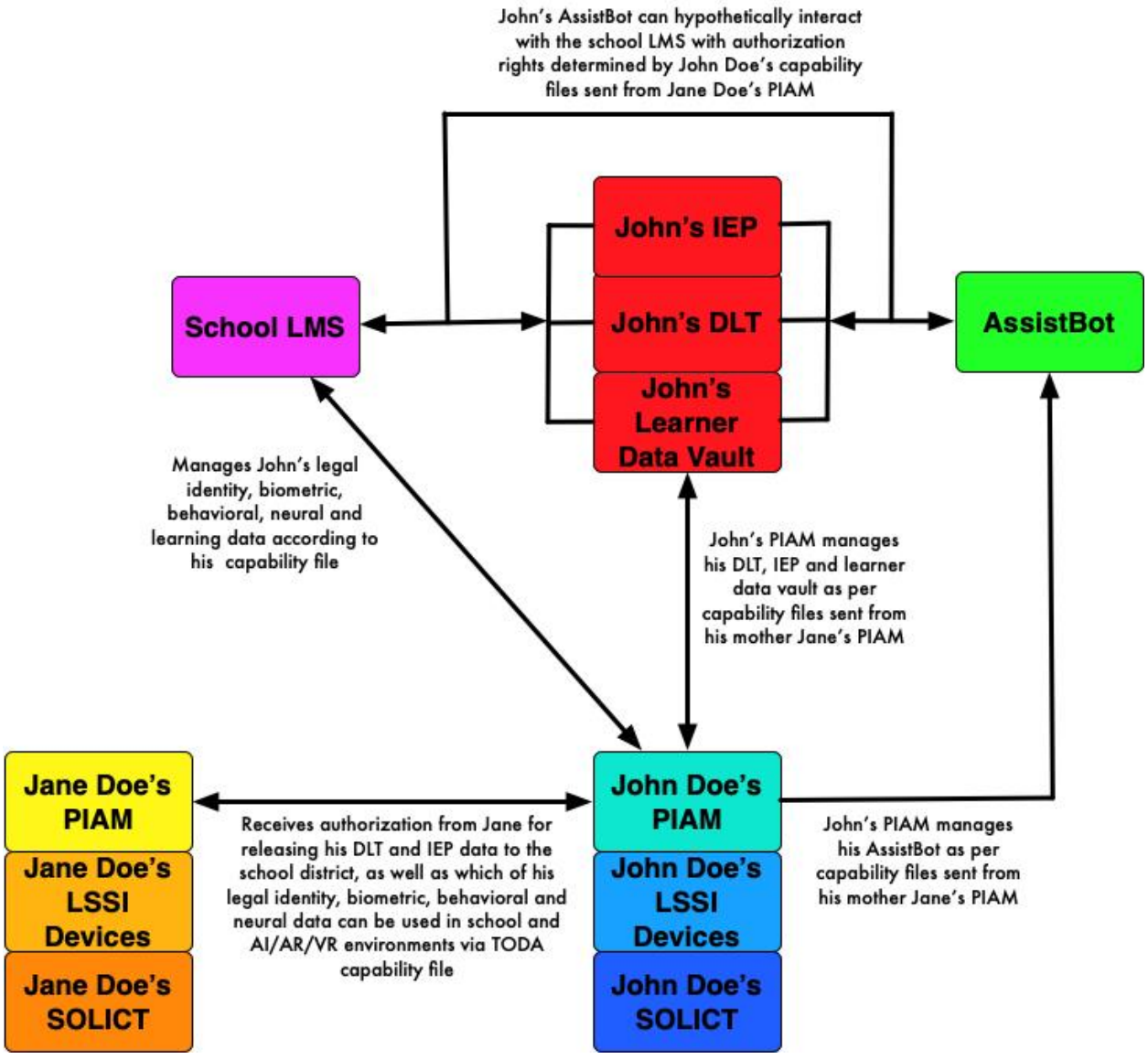
Note:

Within this cost centre doc there are two cost centres pertaining to legal authorization rights:

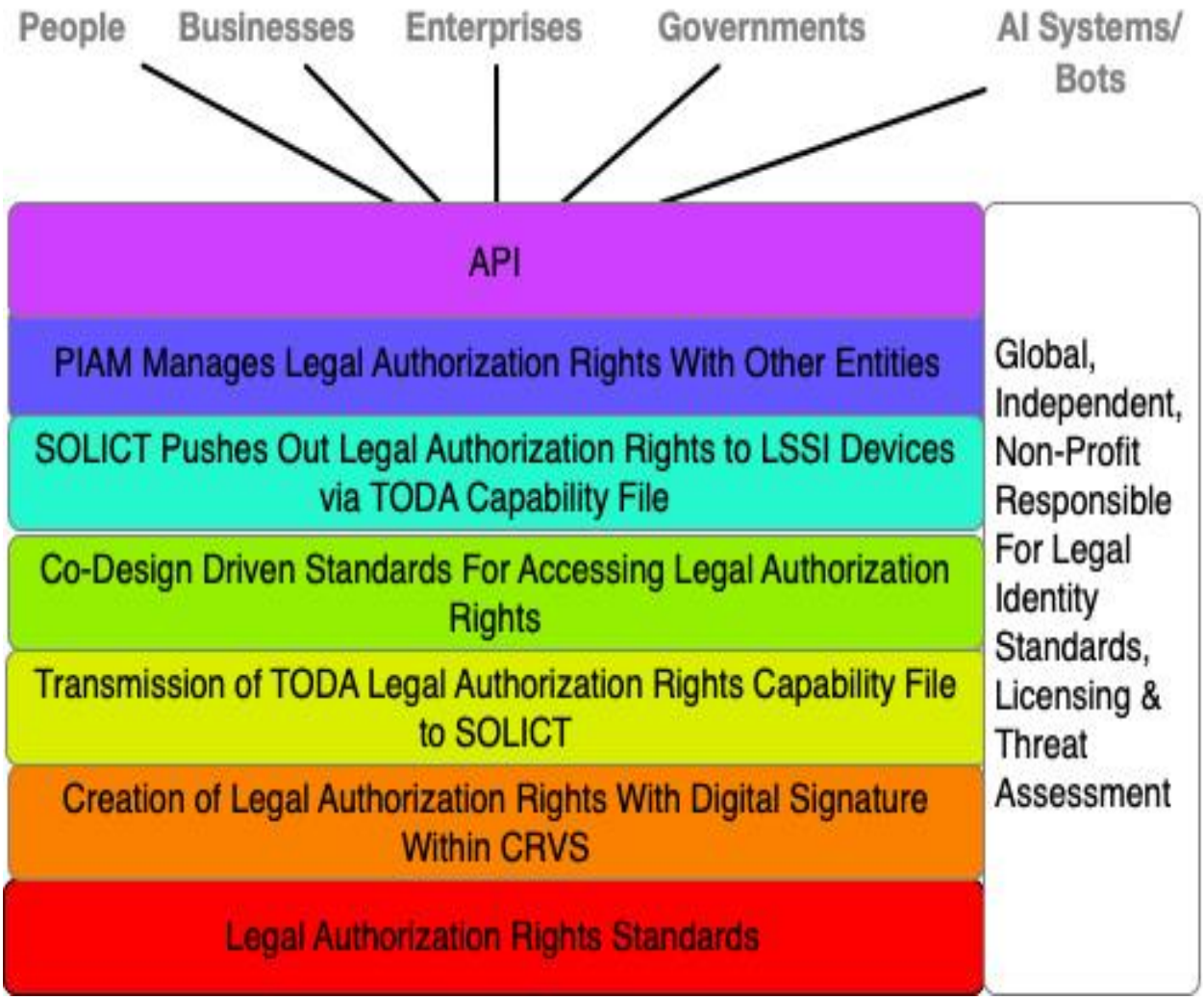
- **This CRVS cost centre**
- **Cost Centre – Legal Authorization Rights**

Why two cost centres? The CRVS is the authoritative source for legal identity and legal identity relationships only. Legal authorization might or might not use CRVS defined relationships. Thus, I've broken it out into two separate cost centres. The design and implementation teams might or might not want to merge the two cost centres.

Legal Authorization Rights Example:



CRVS - Legal Authorization Rights Subcomponent Cost Centres Diagram:



Other Cost Centres Dependent Upon This Cost Centre:

- Creation of Legal Authorization Rights With Digital Signature Within CRVS Subcomponent Cost Centre
- Legal Authorization Rights - Transmission of TODA Authorization Capability File to SOLICT Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

CRVS Legal Authorization Rights Standards Subcomponent Cost Centre:

Background:

Authorization is complicated. Examples include:

- Local jurisdiction assigning to Jane Doe full authorization privileges over her son John Doe until he comes of legal age or,
- Local jurisdiction assigning to Jane Doe full authorization privileges over her son John Doe's learning assistant bot, AssistBot or,
- As John ages, Jane might want to assign some of her authorization privileges over to John allowing him partial control over his legal identity or,
- Jane might have full authorization control over her AI leveraged, medical digital identity with the medical credential issuing organization granting to Jane Doe's medical digital identity the same, less or greater authorization rights than she has or,
- Jane's employer Acme Health Inc. might want to allow Jane's AI leveraged medical digital identity to have less authorization rights than Jane physically has

Authorization is complex due to the granularity of the authorization AND the literally millions of different types of authorizations on the planet today. It also has legal implications as risk rises. Therefore, laws and regulations might or might not apply to a wide variety of different authorization scenarios.

Therefore, what's required are:

- Local/global standards on authorization language allowing for creation of many different types of authorization
- Agreement on standards used for CRVS related authorization rights leveraging TODA capability files
- Changes to laws and regulations pertaining to use of CRVS related authorization rights
- Citizens of all types of abilities and disabilities able to manage their authorization rights through co-design
- Enforcement of these laws and regulations across different jurisdictions
- Flexible laws and regulations allowing for relatively quick upgrades to them as this technology curve occurs

That's what this cost centre MUST deliver.

CRVS Legal Authorization Rights Subcomponent Costs:

The costs for this will likely be born under the Legal Authorization Rights Cost Centre, the Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS Creation of Legal Authorization Rights By Authorized Entity With Their Digital Signature Subcomponent Cost Centre:

Background:

Part of the authorization rights verification process is ensuring the authorization party gave their authorization (i.e., proving it wasn't Malicious Molly or Evil Inc. masquerading as Jane Doe or the CRVS system). This requires the authorizing entity to digitally sign the TODA capability file containing the authorization right.

Let's use CRVS Jurisdiction A as an example granting to Jane Doe, legal identity authorization rights for her newborn son John Doe:

1. The CRVS first cross-indexes within the CRVS database both Jane and John's legal identities stating Jane Doe is the mother of John Doe
2. It then creates a TODA capability file stating the legal identity relationship AND AUTHORIZING JANE TO HAVE FULL AUTHORIZATION CONTROL OF JOHN DOE'S LEGAL IDENTITY
3. The CRVS digitally signs the TODA capability file
4. The CRVS then sends the digitally signed TODA capability file to both Jane and John's SOLICTs
    a. Note the TODA file sent from the CRVS to each of their SOLICTs also contains a hash of the file
    b. Thus, it can be proven on X date, at Y time, a TODA capability file with hash Z, was sent from CRVS endpoint to Jane and John's SOLICT endpoints
5. If a third party wants to verify Jane and John's legal identity relationship and authorization rights, with Jane's consent via her PIAM, they can obtain the CRVS digital signature and make a quick electronic trip to the CRVS to verify the digital signature.
    a. Thus, the third party has confidence it's really Jane and John's legal identity relationship and authorization rights issued by CRVS Jurisdiction A
6. **The entities, in this case Jane and John Doe, have control over their legal identity, with the ability to prove their legal identity relationship plus their authorization rights**

A critical component to make all the above occur, is having all citizens on the planet be able to manage their digital signature regardless of their learning style, communication abilities or their disabilities. Thus, co-design is critical.

CRVS Creation of Legal Authorization Rights By Authorized Entity With Their Digital Signature Subcomponent Costs:

The costs for this will likely be born under the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre section of this document.

CRVS - Transmission of TODA Legal Authorization Capability File to SOLICT Subcomponent Cost Centre:

Background:

The legal identity architecture is based on privacy by design. Thus, it includes creation of a SOLICT (Source of Legal identity & Credential Truth) for each entity. It's managed by the non-profit. The CRVS sends out to the SOLICT legal identity information via TODA.

Given this curve, it means the Evil Inc.'s and malicious states of the planet will leverage it to create new attack vectors against all the above. Thus, as new attack vectors are determined from the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs then technical as well as legal laws and regulations must be changed, updated, etc.

Transmission of TODA Authorization Capability File to SOLICT Subcomponent Costs:

Standards for the CRVS TODA capability file will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) section of this document.

CRVS - Co-Design Driven Standards For Accessing Legal Authorization Rights Subcomponent Cost Centre:

Background:

Authorization rights are complicated and their effects potentially limiting what a citizen can and can't do. Thus, regardless of a citizen's abilities or disabilities, they need to understand what their authorization rights are, make their own decisions, and then execute the authorization rights via their LSSI devices and/or their PIAM. That's what co-design brings to the table.

PIAM Manages Legal Authorization Rights With Other Entities Subcomponent Costs:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS - SOLICT Pushes Out Legal Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Cost Centre:

Background:

The SOLICT in turn pushes out the legal authorization information, via TODA capability files to the LSSI devices.

A citizen, regardless of their abilities or disabilities, MUST be able to:

- **Understand what their legal authorization rights are**
- **Be able to make a decision on who to share them with**
- **Then have the LSSI devices and/or PIAM instantly execute**

This is what co-design brings to the table.

SOLICT Pushes Out Legal Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Costs:

Costs will be borne by Non-Profit – Manages LSSI Standards Subcomponent Cost Centre, the Cost Centre: API (Application Programming Interface) and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS - PIAM Manages Legal Authorization Rights with Other Entities Subcomponent Cost Centre:

Background:

The AI leveraged PIAM manages release of legal authorization rights with third parties via the LSSI devices and consents via TODA/Kantara UMA (User Managed Access).

A critical component to make all the above occur, is having all citizens on the planet be able to manage their PIAM regardless of their learning style, communication abilities or their disabilities. Thus, co-design is critical.

PIAM Manages Legal Authorization Rights With Other Entities Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre section of this document and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS Legal Authorization Rights SOLICT/LSSI API (Application Programming Interface) Subcomponent Cost Centre:

Background:

The API is the electronic front door to the PIAM and LSSI. If it's not secure, then Evil Inc.'s and malicious states will leverage weaknesses to access data like legal identity and hive relationships.

CRVS Legal Identity & Hive Relationships – API Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – API Subcomponent Cost Centre and the Non-Profit – API Rule Sets Subcomponent Costs section of this document.

CRVS – API (Application Programming Interface) Cost Centre:

Background:

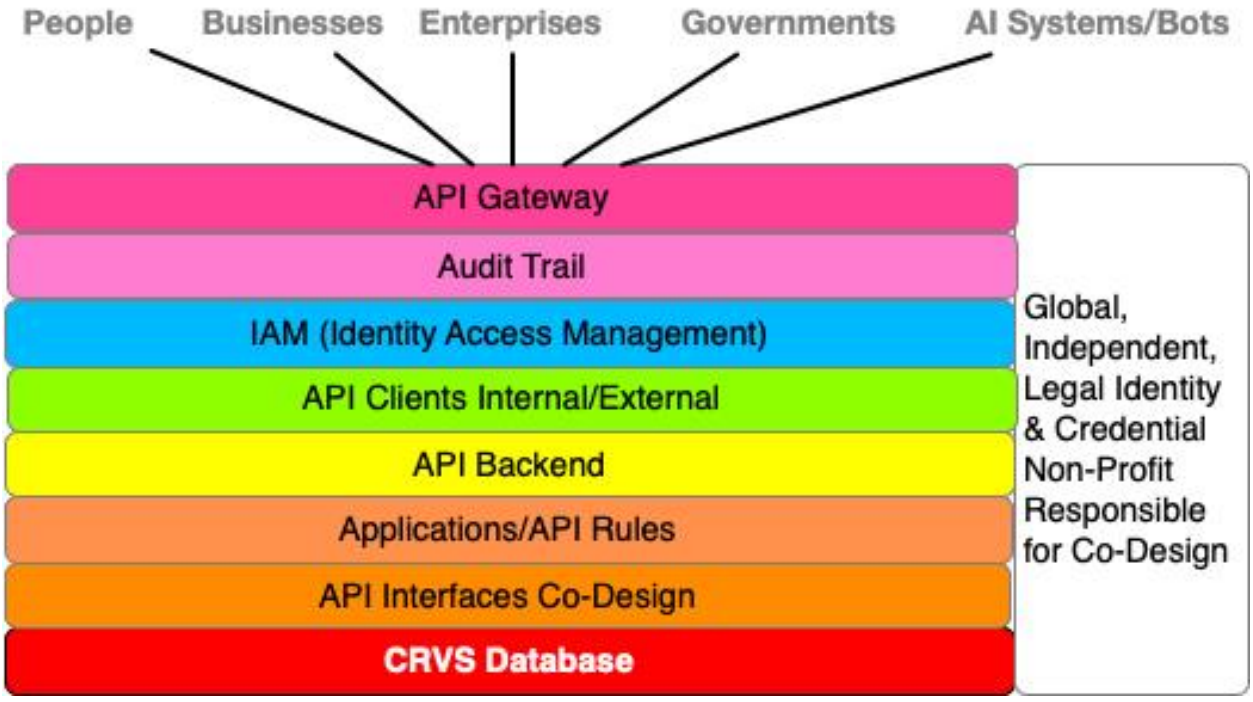
I have an underlying premise:

> "As the planet madly digitizes with AI systems, bots and AI leveraged, smart digital identities of us, the CRVS will become a prime attack target since it's the underlying legal repository for entities."

The API is the electronic front door to the CRVS. Thus, not only must it be able to function at sub-second speeds, under extreme loads, it also must be secure and kept secure as this curve occurs. That's what this cost centre addresses.

CRVS API Subcomponent Cost Centres Diagram:

Note: I'm NOT AN API EXPERT. Thus, the diagram below will likely be modified by those that are API experts!



CRVS API - CRVS Authoritative Sources Databases Subcomponent Cost Centre:

Background:

The CRVS system in this architecture will become standardized. Thus, from the perspective of creating standardized API's, it can be used with all CRVS systems. So, the API can begin with the underlying CRVS database (which may or may not be graph based).

It's possible to use a data API gateway to access CRVS data stored within the database. Hypothetically, it might enable application developers to focus on writing business services that access data via easy-to-use APIs instead of having to learn the intricacies of a database query language.

All of this must be measured against security and performance. The number of writes/per second to the database might be awe inspiring given the rate at which an AI system can create digital bots, if they require legal identity registration.

API - CRVS Authoritative Sources Databases Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre and the CRVS - Creating a New CRVS System With Data Standards for Legal Identities and Vital Statistics Subcomponent Cost Centre section of this document.

CRVS API – Co-Design Interfaces Subcomponent Cost Centre:

Background:

The legal identity, credential and notary architecture is built around ensuring all citizens, regardless of their abilities or disabilities can leverage their SOLICT, LSSI devices, PIAM, credentials and interact with a notary regarding these. Thus, any API interface pertaining to citizens, must be designed and tested allowing all citizens to interact with the above. That's what this cost centre delivers.

Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit – Co-Design API Interfaces Subcomponent Costs

CRVS API – Co-Design Interfaces Subcomponent Costs:

Costs will likely be borne by the **Non-Profit – Co-Design API Interfaces Subcomponent Costs** section of this document.

CRVS API – Applications/API Rules Subcomponent Cost Centre:

Background:

These CRVS requires an application API.

CRVS API – Applications/API Rule Subcomponent Costs:

Costs will borne by the Non-Profit – API Rule Sets Subcomponent Costs section of this document.

CRVS API - Backend Subcomponent Cost Centre:

Background:

The API calls will likely be translated into actions leveraging tech like Enterprise Service Bus (ESB), a database, another cloud service, a microservice, application, or web server. Thus, these must be specified, designed for, tested and kept up to date from a security perspective.

CRVS API - Backend Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Costs and the API - Backend Subcomponent Cost Centre section of this document.

CRVS API – Clients Internal/External Subcomponent Cost Centre:

Background:

The client is a set of development tools to test and debug API's. These need to be carefully selected and use for internal and external clients.

CRVS API – Clients Internal/External Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost and the API – Clients Internal/External Subcomponent Cost Centre section of this document.

CRVS API – IAM (Identity Access Management) Subcomponent Cost Centre:

Background:

When IAM came into being in the late 90's, it was built on authoritative identity sources feeding an LDAP (Lightweight Directory Access Protocol) on top of which the IAM system functioned. This model isn't going to work well anymore. Why?

Fast changing legal identity entity relationships. As explained throughout this document, hive relationships can be one to one, one to many, and many to many with fast changing relationships. LDAP is a poor choice for this, while graphs are likely much better.

Then there's the speed at which new entities can be created. An AI system, in one jurisdiction, can create digital bots at speeds of thousands to millions per second, which in the next second can be operating in all other jurisdictions on the planet. If these require registration showing hive relationships, then I'm not sure if graphs can work at such speeds.

Add to this the ability to confirm a CRVS legal identity entity data transfer occurred on X date, at Y time, containing a file Z, at transactional speeds. This requires use of TODA which isn't used today in IAM systems.

For information on graphs and TODA skim, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

Then there's the arrival of PIAM (Personal Identity Access Management) systems. This creates a very decentralized IM system. As noted in the PIAM Cost Centre section of this doc, it will likely become a very fast-moving standard, with lots of changes.

Finally, add to this the security effects of this curve. That's where the new, global, independent non-profit comes into play with 24x7x365 threat analysis against end-to-end legal identity framework.

My point? OUR OLD IAM ARCHITECTURE ISN'T GOING TO WORK. DESIGNERS TAKE NOTE.

CRVS API – IAM (Identity Access Management) Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost and the API – IAM (Identity Access Management) Subcomponent Cost Centre section of this document.

CRVS API – Audit Trail Subcomponent Cost Centre:

Background:

The audit trail is an essential component to the security and legal functioning of the CRVS.

TODA is a critical part of this because it can confirm on X date, at Y time, a file Z, was sent between two endpoints. Skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

A SECURE AUDIT API MUST BE DESIGNED AND IMPLEMENTED ALLOWING ADMINISTRATORS FAST ACCESS TO THE AUDIT LOGS/APPLICATIONS. AT THE SAME TIME ADMINISTRATORS MUST NOT BE ABLE TO EASILY CHANGE AUDIT/LOBS/APPLICATIONS.

CRVS API – Audit Trail Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost and the API – Audit Trail Subcomponent Cost Centre section of this document.

CRVS API – API Gateway Subcomponent Cost Centre:

Background:

The gateway provides the visible URL for an API, applies rules for use of the API, and then directs the API call to the back-end implementation. Rules can cover actions such as:

- Authentication and authorization
- Certificate management, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) termination and Mutual TLS
- Rate limiting and throttling
- Payload inspection (including payload size and the means to validate that the payload is structurally correct)
- Intelligent routing (routing based on the header or payload content)
- As importantly, from a security perspective, is the endpoint configuration, DNS standards, encryption, etc. to which API rules must be designed for

CRVS API Gateway Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost and then API – API Gateway Subcomponent Cost Centre section of this document.

CRVS – Data Centres:

Overview

While many people immediately leap to putting data into the cloud, assuming it is lower cost and always available, it doesn't easily apply to CRVS systems. Why?

They're jurisdictional, often with laws and regulations prohibiting storage of the data outside the jurisdiction. In countries like Canada, where I live, each province and territories having their own CRVS systems, each with requirements to store the data within the jurisdiction. Having said this however, there are certain cross-province data sharing agreements.

As the planet madly digitizes, accessing the data from any jurisdiction on the planet becomes required 24x7x365. Thus, the world of underlying legal identity data storage is complicated from assuring a highly available operating environment available to at least 99.999% availability or more.

I've led teams deploying such available systems. Several years ago, I was pondering the fact as legal identity becomes digitized, I was wondering what could bring the entire digital legal identity system down? Answer – a sun GMD (geomagnetic disturbance) creating EMP (electromagnetic pulse) events.

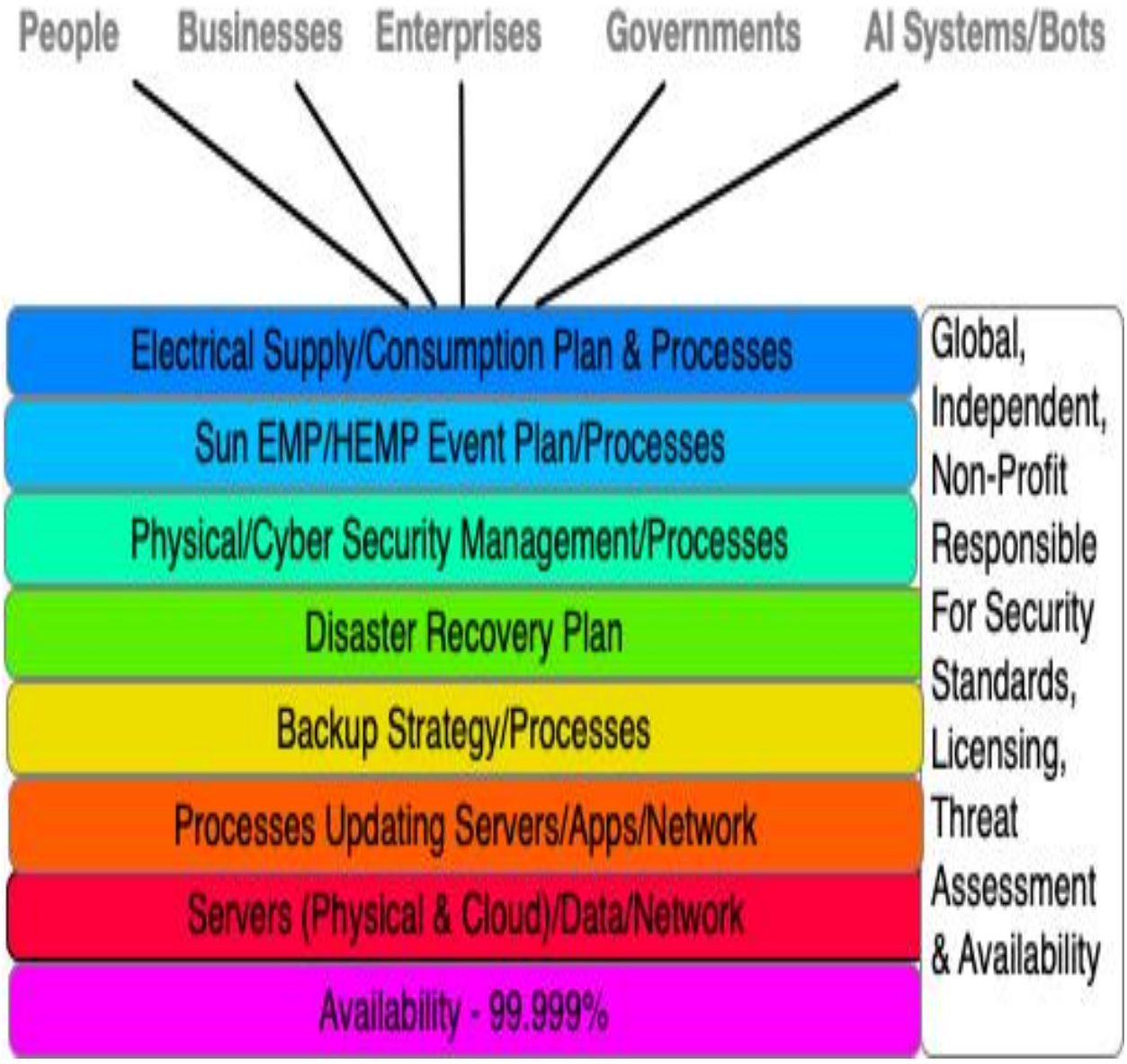
The US government estimates the effect of this would cause up to 90% deaths of the population post event. Why? The EMP event would likely bring down many transformers in the electrical grid. There are only a limited number of transformer manufacturers on the planet with long production times. Thus, it's highly likely the EMP event would bring the electrical grid to its knees, for a long period of time, resulting in no electrical power to our water, sewage, internet et al. Thus, the resulting high death rates.

What's the chance of an EMP event happening? 1 in 8 this decade! When I learnt this, I sat up on the edge of my seat, realizing this wasn't a low probability event.

Good news – tech exists to mitigate this risk. Bad news – no governments around the planet are implementing it to fully protect their electrical grids. I strongly suggest readers skim this article, "**When Our Digital Legal Identity Trust Goes Poof!**" -.

CRVS Data Centres Subcomponent Cost Centres Diagram:

Note: I'm NOT a data centre expert. Thus, I expect such experts, based on their expertise, to amend the cost centres below:



CRVS Data Centres 99.999% Availability Subcomponent Cost Centre:

Background:

Here's the challenge with today's digitizing world. Legal identity lookups and registration will occur 24x7x365 both locally and globally. **ALL SORTS OF BUSINESS AND CONTRACTUAL PROCESSES WILL RELY ON THE DATA. THUS, IT REQUIRES HIGH AVAILABILITY.**

As I see it, at a minimum, 5 9's availability (99.999% uptime is required) i.e., 5.26 minutes downtime per year. It would be desirable if it was 6 9's (99.9999%) i.e., 31.56 seconds downtime per year.

Thus, the foundational architectural piece for the new CRVS data centres is 5 9's at a minimum. This is what this cost centre must deliver.

CRVS Data Centres Availability Subcomponent Cost Centres:

Costs will be borne by Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Servers (Physical & Cloud)/Data/Network Subcomponent Cost Centre:

Background:

There's a challenge with putting a local CRVS's data up into the cloud – the data storage might by law, be required to be stored within the jurisdiction. In some countries with local state/provincial CRVS systems, there's agreements across the jurisdictions allowing for storage of data, but not outside the country. **THUS, THIS REQUIREMENT MUST BE TAKEN INTO CONSIDERATION IN LEVERGING CLOUD BASED SERVICES**.

CRVS Servers (Physical & Cloud)/Data/Network Subcomponent Cost Centres:

Costs will be borne by the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Processes Updating Servers/Apps/Network Subcomponent Cost Centre:

Background:

A 5-9 or 6-9 availability means servers, apps and network upgrades must occur without any downtime in the system. Thus, very careful planning and ongoing management of servers, apps and networks must occur. That's what this cost centre delivers.

CRVS Processes Updating Servers/Apps/Network Subcomponent Cost Centres:

Costs will be borne by the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Backup Strategy/Processes Subcomponent Cost Centre:

Background:

Back-ups of the underlying CRVS data is mission critical, not only operationally, but also legally. **Thus, this cost centre MUST deliver operational backup processes which are constantly being tested to ensure effectiveness.**

CRVS Backup Strategy/Processes Subcomponent Cost Centres:

Costs will be borne by the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Disaster Recovery Subcomponent Cost Centre:

Background:

Bluntly speaking, shit happens. IF SOMETHING CATASTROPHIC HAPPENS TO A CRVS SYSTEM, THEN A WELL-TESTED DISASTER RECOVERY PLAN MUST BE ENACTED. That's what this cost centre delivers.

CRVS Disaster Recovery Subcomponent Cost Centres:

Costs will be borne by the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Physical/Cyber Security Management/Processes Subcomponent Cost Centre:

Background:

The number of potential attack vectors against a CRVS are numerous. This includes:

- Wide assortment of cyber-attacks from DNA, endpoint through to network, databases, data, etc.
- Management attack vectors
- Business process attack vectors
- Physical security of the data centres
- Physical security of servers, networks, etc.

This tech change curve, hypothetically means, each hour, new attack vectors are being created against the end-to-end CRVS system, including data centres, management, etc. **THE NEW AGE CRVS SYSTEM BECOMES A PRIME ATTACK TARGET BTY THE EVIL INC.'S AND THE MALICIOUS STATES OF THE PLANET. THUS, A CONTINUAL STATE OF THE ART SECURTIY PROGRAM IS REQUIRED.**

One of the main jobs of the new, global, independent, well-funded non-profit is to ensure continual security standards are in place guaranteeing security and operational ability. **THAT'S WHAT THIS COST CENTRE DELIVERS.**

CRVS Physical/Cyber Security Management/Processes Subcomponent Cost Centres:

Costs will be borne by the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

CRVS EMP/HEMP Protection/Power Supply Subcomponent Cost Centre:

Background:

Read "**When Our Digital Legal Identity Trust Goes Poof!**". It lays out the 1 in 8 chance this decade of a sun geomagnetic disturbance electromagnetic pulse (GMD EMP) event. It also discusses high altitude magnetic pulse risks. If a major GMD EMP event occurs today, billions of people would die, post event.

Bottom Line:

1. Design of each CRVs/cloud data centres must address this type of event ensuring the underlying legal identity data survives the event.
2. Countries must take action to fund and legislate changes to their electrical grid to withstand pulse events

CRVS Sun EMP/HEMP Event Plan/Processes Subcomponent Costs:

Costs will be borne by the Non-Profit – EMP/HEMP Protection/Power Supply Subcomponent Cost Centre and the Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre sections of this document.

CRVS Data Centre Electrical Supply/Consumption Plan & Processes Subcomponent Cost Centre:

Background:

Look at figure 1 diagram "**Energy consumption of ML. Source: AMD**" in "**AI Power Consumption Exploding**". **It shows by 2040 AI consuming most electrical power on the planet. The electrical consumption isn't sustainable. Thus, this cost centre is politically very important**.

It requires jurisdictional leaders, power suppliers and AI industry to come together to create a viable electrical supply. In turn, this then ripples into electrical requirements to run each jurisdiction's CRVS system. **Very careful electrical consumption planning MUST occur with deployment of new age CRVS systems, used to register potentially millions, billions, and trillions of AI system/bots' identities.**

Finally, as global warming occurs, power supplies might become limited and/or more expensive. Thus, this cost centre focuses on creating CRVS low power consumption.

CRVS Data Centre Electrical Supply Plan/Processes Subcomponent Costs:

Costs will be borne by the Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre section of this document.

CRVS - Governance Laws and Regulations Cost Centre:

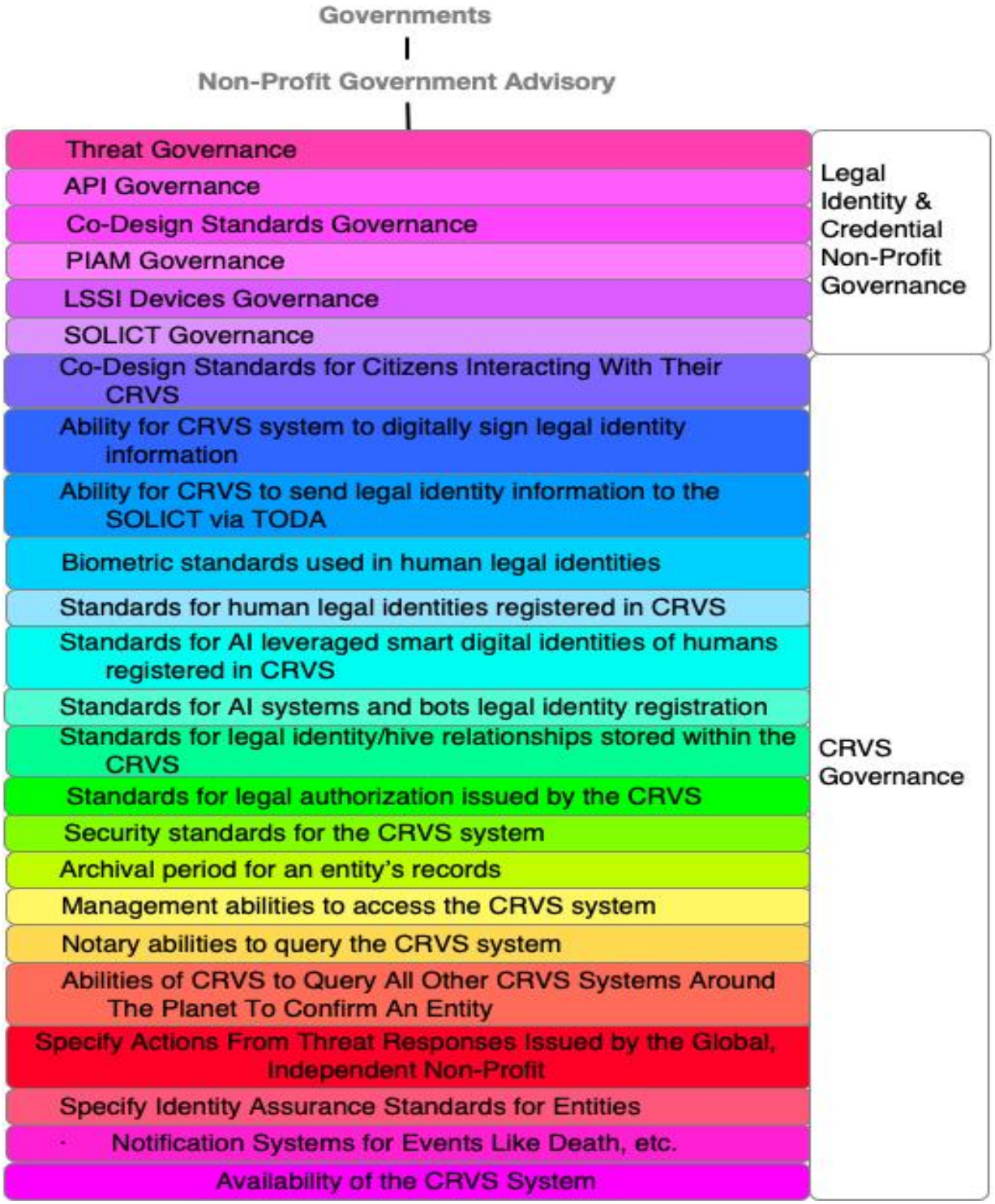
Background:

Each jurisdiction adopting the new age CRVS system, will have to change their underlying CRVS laws and regulations. They'll need to spell out the following:

- Use of forensic biometrics to legally identify a person from cradle to grave
- Use of biometrics
- Ability for CRVS system to digitally sign legal identity information
- Ability for CRVS to send legal identity information to the SOLICT via TODA
- Biometric registration processes for infants out in the field as well as in urban centres
- Standards for human legal identities registered in CRVS
- Standards for AI leveraged smart digital identities of humans registered in CRVS
- Standards for AI systems and bots legal identity registration
- Standards for legal identify relationships stored within the CRVS
- Standards for authorization issued by the CRVS
- Security standards for the CRVS system
- Archival period for an entity's records
- Management abilities to access the CRVS system
- Notary abilities to query the CRVS system
- Abilities of CRVS to query all other CRVS systems around the planet to confirm an entity
- Specify actions from threat responses issued by the global, independent non-profit
- Specify identity assurance standards for entities
- Notification systems for events like death, etc.
- Availability of the CRVS system
- Co-design standards for citizens regardless of their abilities or disabilities to interact with their local jurisdiction's CRVS department
- Etc.

CRVS Governance Laws & Regulations Subcomponent Cost Centres Diagram:

Note: For reference, I've included the entire legal identity governance framework below. This section only deals with CRVS governance.



CRVS Governance – Availability of the CRVS System Subcomponent Cost Centre:

Background:

The CRVS MUST BE HIGHLY AVAILABLE. Skim CRVS Data Centres Availability Subcomponent Cost Centre section of this document. Thus, the laws and regulations pertaining to the CRVS MUST STATE AVAILABILITY REQUIREMENTS.

CRVS Governance – Availability of the CRVS System Subcomponent Costs:

Costs will be borne by the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

CRVS Governance - Notification Systems for Events Like Death, etc. Subcomponent Cost Centre:

Background:

There are two types of CRVS event notifications:

- Personal notification services where the entity initiates the notification themselves, likely through a private notification service
- CRVS initiated notifications

This cost centre only address CRVS initiated notifications.

When an entity is born/created, dies/terminated, etc., as governments digitize their internal systems, then it becomes likely different areas of a jurisdiction will want to be notified by the authoritative CRVS system of the event. It comes with LOTS of governance requirements because the information might be restricted on notification due to existing laws and regulations.

As AI systems and bots legal identities are registered, it creates all sorts of new governance requirements within not only a jurisdiction, but also between jurisdictions. An AI system in one jurisdiction can created digital bots at speeds of thousands to hundreds of thousands per second which, in the next instance, can be operating in all other jurisdictions on the planet. This likely means inter-jurisdictional notifications will be required.

CRVS initiated notifications must also work for all citizens on the planet regardless of their abilities or disabilities. Thus, co-design should be applied to this.

CRVS Governance – Notification Systems for Events Like Death, etc. Subcomponent Cost:

Costs will be borne by the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre , Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

CRVS Governance - Specify Actions From Threat Responses Issued by the Global, Independent Non-Profit Subcomponent Cost Centre:

Background:

The non-profit operates a threat advisory service for the legal identity framework. This includes notification to the CRVS. The CRVS must be legally responsible for complying with the threats based on pre-determined response times and actions. Thus, it requires changes to existing CRVS laws and regulations as and when required to require the CRVS to comply. That's what this cost centre addresses.

CRVS Governance - Specify Actions From Threat Responses Issued by the Global, Independent Non-Profit Subcomponent Costs:

Costs will be borne by Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

CRVS Governance - Abilities of CRVS to Query All Other CRVS Systems Around The Planet To Confirm An Entity Subcomponent Cost Centre:

Background:

The sheer speed at which AI systems can create digital bot entities is awe-inspiring i.e., thousands to hundreds of thousands per second. In the next instance, they can be operating in all other jurisdictions around the planet. Couple this with fast emerging AI leveraged smart digital identities of humans. These too can operate in all other jurisdictions around the planet.

Add it all up and it requires the ability of a CRVS in one jurisdiction to be able to query all other CRVS systems around the planet to confirm an entity. Pushing aside the technical challenges, IT MUST INCLUDE JURISDICTIONAL LAWS AND REGULATIONS PERMITTING THIS, AS WELL AS REGULATING IT. That's what this cost centre delivers.

CRVS Governance - Abilities of CRVS to Query All Other CRVS Systems Around The Planet To Confirm An Entity Subcomponent Costs:

Costs will be borne by Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Governance - Notary Abilities to Query the CRVS System Subcomponent Cost Centre:

Background:

The Cost Centre: Rethought Notaries section of this document describes rethinking notaries. It allows the notary to be able to query a CRVS system to confirm an entity's legal identity. However, it comes with new challenges. Like what?

In "Notary- Legal Identity & Credential Verification Certification Process Subcomponent Costs" it states the following:

> **"While this function of the notary is very desirable from a human rights perspective, it potentially opens the doors to a notary being able to troll all CRVS systems around the planet for an identity. I can easily see criminals leveraging a corrupt notary to do this.**
>
> **THUS, MY VIEW IT TO NOT ALLOW A NOTARY TO BE ABLE TO TROLL CRVS SYSTEMS PLANET WIDE.** Instead, limit them to being only able to do a search on a single legal identity, in one CRVS system at a time. Let's use Jane Doe as an example…
>
> Jane has fled a country where they've deleted her CRVS and other jurisdictional legal identity databases. She goes to a local notary, claiming to be Jane Doe, from jurisdiction X, born on Y date at a certain location. She also claims she doesn't have any LSSI devices.
>
> The local notary could then, with Jane's consent, take her forensic biometrics and do a search/comparison for the date and location within Jurisdiction X. If they match, the notary could then create a physical/digital attestation it's Jane Doe. Jane Doe could then take this and use it to prove her legal identity.
>
> If Jane shows up at a local notary unable to recall which jurisdiction, she's from, date of birth, etc., the local notary would be unable to assist her. It would instead direct her to the local jurisdiction's CRVS office, where they would then use a special governance/business process to be able to obtain Jane's forensic biometrics, and search planet wide for her legal identity.
>
> On a side note: In the paper "**Human Migration, Physical & Digital Legal Identity**", it discusses the fact that up to 50% of migrants are children. Some of these will have no parents, etc. They will fall under the above category, where the government CRVS system will have to prove their legal identities.

If the Notary is requited to do a hive legal relationship certification, then they'd have to do each entity, one at a time, with the CRVS where they were registered.

A very important security function will then be vetting new age notaries, and then granting them privileges as described above. The business processes in this case are very important. Why?

The Evil Inc's. and malicious states of the planet, will leverage weak business processes to put into place notaries who can search the planet's CRVS systems for identities. Thus, the design process is full of not only political challenges, but also security ones."

Thus, it requires new CRVS jurisdictional laws and regulations directing what a notary can and can't do. That's what this cost centre addresses.

CRVS Governance - Notary Abilities to Query the CRVS System Subcomponent Costs:

Costs will be borne by Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Governance - Management Abilities to Access the CRVS System Subcomponent Cost Centre:

Background:

Who can access the very, very sensitive CRVS data? Who can make changes to it? What's the governance and business processes for this?

Very careful thought must be given by a jurisdiction, re their CRVS laws and regulations, about:

- CRVS database administrators
- CRVS system administrators
- Senior CRVS management
- Network administrators
- Etc.

That's what this cost centre addresses.

CRVS Governance - Management Abilities to Access the CRVS System Subcomponent Costs:

Costs will be borne by Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Governance - Archival Period for an Entity's Records Subcomponent Cost Centre:

Background:

Consider an AI system producing registered digital bots at speeds of thousands or more per second, which in the next instance can be operating in all other jurisdictions around the planet. How long will the entity's legal identity record be stored in the CRVS archival system?

Then to see what's coming skim, "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**". Jane Doe might have legally registered nanobots which have very short lifespans within her body. What is the archival process for these types of identities?

That's what this cost centre addresses.

CRVS Governance - Archival Period for an Entity's Records Subcomponent Costs:

Costs will be borne by Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre section of this document.

CRVS Governance - Security Standards for the CRVS System Subcomponent Cost Centre:

Background:

The architecture creating the new age CRVS comes with all sorts of new risks including:

- New attack vectors being created each hour and day by this curve
- Physical and digital attacks against CRVS data centres
- Masquerading both physically and digitally as CRVS administrators, etc.

My point? It requires continuous updating of security standards. Thus, in each CRVS jurisdiction they're going to have to get their heads around the fact that regulations pertaining to CRVS security might require daily, weekly or monthly updates. This is something they're not familiar with.

That's what this cost centre addresses. It continually addresses CRVS governance from a security perspective.

CRVS Governance - Security Standards for the CRVS System Subcomponent Costs:

Costs will be borne by Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre and the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs Centre section of this document.

CRVS Governance - Standards for Legal Authorization Issued by the CRVS Subcomponent Cost Centre:

Background:

The "Cost Centre – Legal Authorization Rights" section of this document lays out why legal authorization is becoming very important. I can easily see complexities growing as AI systems, physical and digital bots explode into our lives around the planet.

While the cost centre lays out use of TODA to assist in solving this, it doesn't address the CRVS, and jurisdictional laws and regulations required to create this. As importantly, as the legal authorization rights become more complex, it will also require updates to jurisdictional and CRVS laws and regulations. That's what this cost centre addresses.

CRVS Governance - Standards for Legal Authorization Issued by the CRVS Subcomponent Costs:

Costs will be borne by Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre and Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

CRVS Governance - Standards for Legal Identity/Hive Relationships Stored Within the CRVS Subcomponent Cost Centre:

Background:

Skim "Cost Centre – Legal Identity & Hive Relationships" section of this document. Hives are just coming into being. To see an example of this skim, "**An Identity Day in the Life of Jane Doe**" and read the section titled "**Jane Leverages Her AI Leveraged, Medical Digital Identity Which Is Part of a Hive At Work**".

Because of this curve, all I can coming at lawmakers is continual rapid changes in legal authorization requirements. That's what this cost centre addresses re legal standards for legal identity relationships/hive rights stored within the CRVS.

CRVS Governance - Standards for Legal Identity/Hive Relationships Stored Within the CRVS Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre and Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre sections of this document.

CRVS Governance - Standards for AI Systems and Bots Legal Identity Registration Subcomponent Cost Centre:

Background:

The CRVS Artificial Intelligence and Bots Legal Framework Cost Centre section of this document, lays out why it's necessary to create legal identities for AI systems and bots. What the section doesn't lay out are the CRVS governance standards required for the legal identities of the AI systems and bots. That's what this cost centre addresses.

Given this curve, it's highly likely that change will occur to the unique identifiers used to write to the underlying entity's source code, as well as how it's written. The Evil Inc.'s and malicious states will leverage the curve to create new attack vectors against the legal identities. Thus, any laws and regulations pertaining to AI systems and bots' legal identity standards created must be built with rapid changes in mind.

CRVS Governance - Standards for AI Systems and Bots Legal Identity Registration Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Standards Subcomponent Cost Centre and the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

CRVS Governance - Standards for AI Leveraged Smart Digital Identities of Humans Registered in CRVS Subcomponent Cost Centre:

Background:

Skim "**AI Leveraged Smart Digital Identities of Us**" to see what's coming. It will radically reshape how we live, work and play. Within this document, this is covered in "CRVS – Smart Digital Identities of Us Subcomponent Cost Centres".

What's not covered is actual standards, laws and regulations required to support this. That's what this cost centre delivers.

CRVS Governance- Standards for AI Leveraged Smart Digital Identities of Humans Registered in CRVS Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Standards Subcomponent Cost Centre and the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

Note: I broke this out as a separate governance subcomponent rather than bundling it in, as it should be, in the section, CRVS Governance - Standards for Human Legal Identities Registered in CRVS Subcomponent Cost Centre. Why? It's one of the main political drivers for this architecture, since there isn't any existing legal identity framework addressing it. Thus, I wanted to draw their attention to it. The funders and program teams might merge these two together.

CRVS Governance - Standards for Human Legal Identities Registered in CRVS Subcomponent Cost Centre:

Background:

Legally identifying humans is complex. The CRVS Biometric Technology Subcomponent Cost Centres section of this document lays out the numerous challenges with leveraging biometrics to create a legal identity for a human from cradle to grave. Further, as laid out in problem #1 in "**Legal Identity Problem Statements**", there are no CRVS legal identity data standards today for legal identities.

This curve, means that any standards created for the unique legal identity will come under increasing attack from the Evil Inc.'s and the malicious states of the planet. Thus, the jurisdictional CRVS laws and regulations must be built with the ability to rapidly change them as new attack vectors are determined from the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

All the above is what this cost centre addresses.

CRVS Governance- Standards for Human Legal Identities Registered in CRVS Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Standards Subcomponent Cost Centre and the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

CRVS Governance - Biometric Standards Used in Human Legal Identities Subcomponent Cost Centre:

Background:

The CRVS Biometric Technology Subcomponent Cost Centres section of this document lays out the numerous biometric standards required for creating a human legal identity system including:

- Biometric Standards for Infant Fingerprints
- Biometric Standards/Operating Procedures for People Who Don't Have Fingerprints or Iris's
- Biometric Standards for Legally Determining Physical Identity of a Deceased Person
- Research & Standards for Anonymous Biometric Identifiers
- Standardized, Secure Methods for Obtaining Biometrics Out in the Field/Urban Location
- Age Determination of When Children's Iris Registration Can Safely Occur
- Automation of Forensic Biometric Collection
- Research Confirming Fingerprints/Iris Are Enough to Legally Differentiate Human Clones

Given this curve, it means the Evil Inc.'s and malicious states of the planet will leverage it to create new attack vectors against all the above. Thus, the jurisdictional CRVS laws and regulations must be built with the ability to rapidly change them as new attack vectors are determined from the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

All the above is what this cost centre addresses.

CRVS Governance- Biometric Standards Used in Human Legal Identities Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Standards Subcomponent Cost Centre and the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

Note: I broke this out as a separate governance subcomponent rather than bundling it in, as it should be, in the section, CRVS Governance - Standards for Human Legal Identities Registered in CRVS Subcomponent Cost Centre. Why? Biometrics are also important politically in creating a new age CRVS system. It MUST BE VERY CAREFULLY POLITICALLY MANAGED SINCE THERE CAN BE LOTS OF POTENTIAL RESITSTANCE. I'M HOPING RUD BOLLE'S WORK PANS OUT IN REAL LIFE ALLOWING ANONYMIZATION OF BIOMETRICS. Thus, I wanted to draw their attention to it. The funders and program teams might merge these two together.

CRVS Governance - Ability for CRVS to Send Legal Identity Information to the SOLICT via TODA Subcomponent Cost Centre:

Background:

The legal identity architecture is based on privacy by design. Thus, it includes creation of a SOLICT (Source of Legal identity & Credential Truth) for each entity. It's managed by the non-profit. The CRVS sends out to the SOLICT legal identity information via TODA.

Given this curve, it means the Evil Inc.'s and malicious states of the planet will leverage it to create new attack vectors against all the above. Thus, the jurisdictional CRVS laws and regulations must be built with the ability to rapidly change them as new attack vectors are determined from the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

All the above is what this cost centre addresses.

CRVS Governance- Ability for CRVS to Send Legal Identity Information to the SOLICT via TODA Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

CRVS Governance - Ability for CRVS System to Digitally Sign Legal Identity Information Subcomponent Cost Centre:

Background:

THE CRVS MUST HAVE THE ABILITY TO DIGITALLY SIGN LEGAL IDENTITY ATTESTATIONS. It's at the heart of creating a trusted digital legal identity framework. As well, it must issue digital signatures for entities it registers.

Given this curve, it means the Evil Inc.'s and malicious states of the planet will leverage it to create new attack vectors against digital signatures. Thus, the jurisdictional CRVS laws and regulations must be built with the ability to rapidly change them as new attack vectors are determined from the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

All the above is what this cost centre addresses.

CRVS Governance- Ability for CRVS System to Digitally Sign Legal Identity Information Subcomponent Costs:

Costs will be borne by the Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

CRVS Governance – Co-Design Standards For Citizens Interacting With Their CRVS Subcomponent Cost Centre:

Background:

As stated throughout this document, co-design in mission critical in enabling citizens of all abilities and disabilities to interact with their CRVS and the resulting SOLICT, LSSI devices and PIAM. Additionally, all this new architectural CRVS and citizen legal identity and credential tools will become prime attack targets by the Evil Inc.'s and malicious states leveraging this rapid tech change curve. Thus, the governance framework must be able to quickly respond when warranted. That's what this cost centre addresses.

CRVS Governance – Co-Design Standards For Citizens Interacting With Their CRVS Subcomponent Costs:

The costs for this section will be borne by the "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre" section of this document.

CRVS - Global, Independent, Non-Profit Cost Centres:

Note:

As noted throughout this document, it contains creation of a new, global, independent, well-funded, legal identity & credential non-profit. It has these main tasks:

- Manages API standards
- 24x7x365 threat assessments
- Manages PIAM standards
- Manages LSSI devices standards
- Managed SOLICT databases
- Manages SOLICT standards
- Manages credential issuance standards
- Manages legal authorization standards
- Manages legal identity hive relationships standards
- Licenses CRVS system to jurisdictions & credential Issuance to credential bodies
- EMP/HEMP Protection/Power Supply
- Manages CRVS software/system
- Manages legal identity standards for humans/AI systems/bots
- Governance
- Manages notary design and security interactions with the CRVS
- Manages a central co-design team responsible for citizen interfaces to the above

Refer:

To Cost Centre - Global, Independent Legal Identity & Credential Non-Profit section of this document.

Cost Centre: Authoritative Credentials Source

Background:

Life has a multitude of different credentials issued by many different types of enterprises. Add to this the arrival of the following types of entities hypothetically requiring credentials:

- AI leveraged smart digital identities of humans
  - Skim "**AI Leveraged Smart Digital Identities of Us**"
- AI systems and bots
  - Skim "**Entity Management System**" and "**Verifiable Credentials For Humans and AI Systems/Bots**"

The architecture's strategy is to allow credential bodies to still act as the issuing authorities but adopt them for new types of entities. However, there's a condition attached to this. The credential standards body MUST ensure the actual credential is issued securely, without the ability of criminals and malicious states to tamper with it.

Thus, the architecture is built on a global, independent non-profit responsible for credential issuance standards, which the credential standards bodies can adopt. Over time, as the non-profit detects new attack vectors against the credential issuing standards, it can automatically notify the standards body, with the body taking appropriate action based on the threat risk level.

This approach leaves the credential standards body still in control over their management of the credential, but ensures as it's issued, both physically and digitally, it will be secure. Thus, it's politically acceptable.

Further, how citizens with different abilities and disabilities use credentials can now be standardized. Leveraging co-design, the new global, independent, legal identity and credential non-profit can create a wide variety of citizen interfaces to their credentials via their LSSI devices and/or PIAM. As security conditions change due to this curve, the citizen interfaces to the credentials can be updated based on threats.

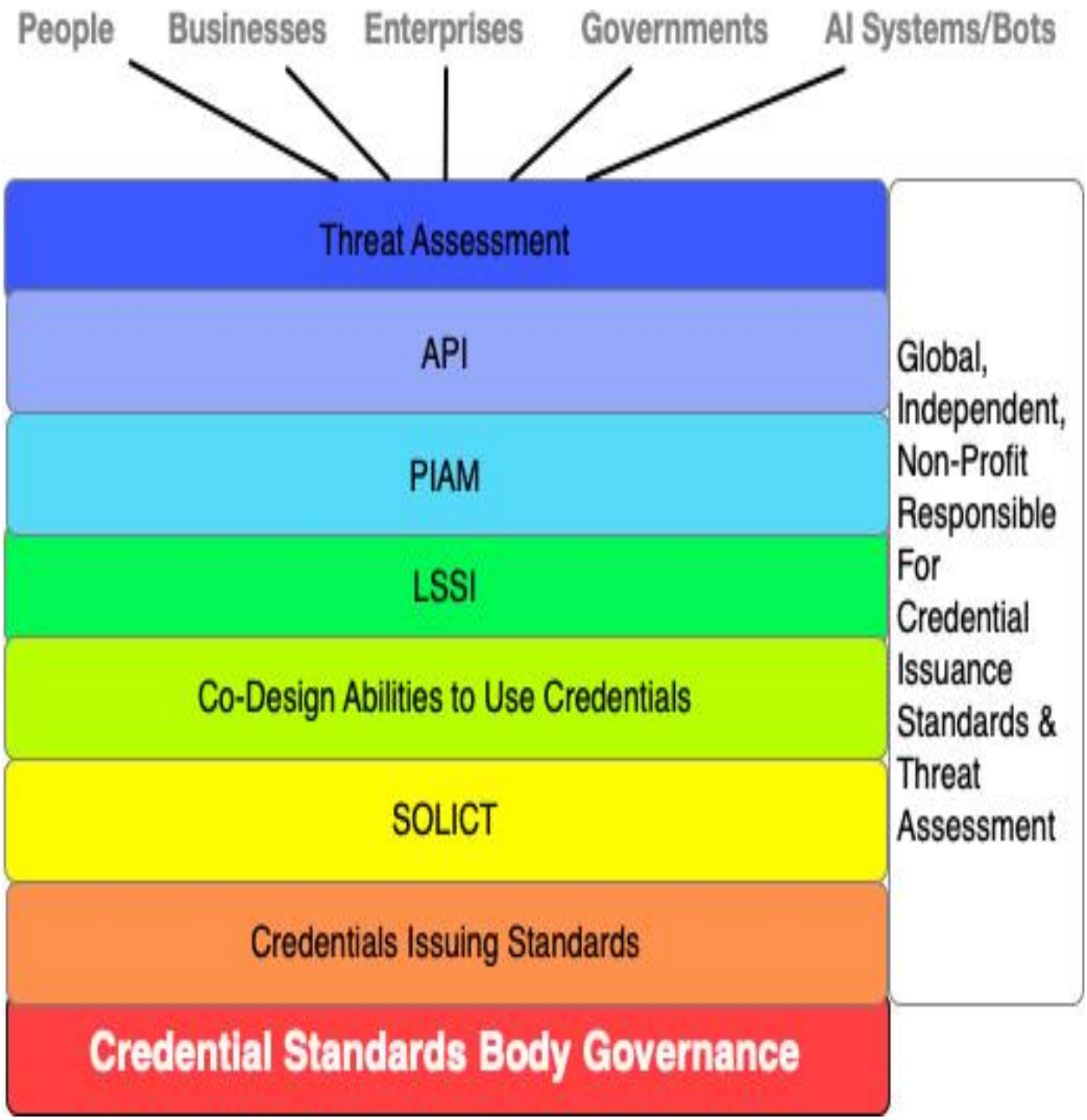
The cost centres associated with this, call out for rapid POC (proof of concept), learning what doesn't work and what works. When ready, do small, tightly controlled pilots in real life. When ready, rapidly scale around the planet.

The benefits of tying the legal identity LSSI devices to credential standards bodies are huge. For example:

- It could work with a person's AI leveraged smart digital identity having credentials. Skim "**Entity Management System**" to see Nurse or Doctor Jane Doe leveraging her AI leveraged, smart medical digital identity to simultaneously manage several patients while she works with another patient. Her medical credentials must be attached to her smart medical digital identity
- It also works with a person's AI leveraged smart digital identity having credentials. Skim "**Entity Management System**" to see Nurse or Doctor Jane Doe leveraging her AI leveraged, smart medical digital identity to simultaneously manage several patients while she works with another patient. Her medical credentials must be attached to her smart medical digital identity
- It could verify AI MedBot1 has X credentials used in medical diagnosis
- It also will work for students as they acquire course credential, degrees and/or professional certification

This is out of the box thinking, for out of the box times.

Credentials Issuing Source Subcomponent Cost Centres Diagram:



Credential Standards Body Governance Subcomponent Cost Centre:

Background:

The credential standards bodies already exist around the planet. My strategy is to not rock their boats i.e., simply adopt their credential standards, leaving the governance processes to them.

The only caveat to this, is when they want to be able to export their credentials to an entity's SOLICT, they'll be required to sign an agreement with the global, independent non-profit, agreeing to use the standards set forth by the non-profit regarding credential issuance standards. Further, they'll also agree to reacting in an approved manner to threat assessment levels issued by the global, independent, non-profit. Thus, they'll be adopting global best practices to protect the credentials they issue to people and, in the not-so-distant future, AI systems and bots.

I can see over time, not overnight, credentials bodies around the planet standardizing their credential issuances for issuance, active, inactive, etc.

What will change is how citizens prove they have the credential. Regardless of their abilities/disabilities all citizens will leverage a co-designed SOLICT, LSSI devices and PIAM to prove their credentials.

Credential Standards Body Governance Subcomponent Costs:

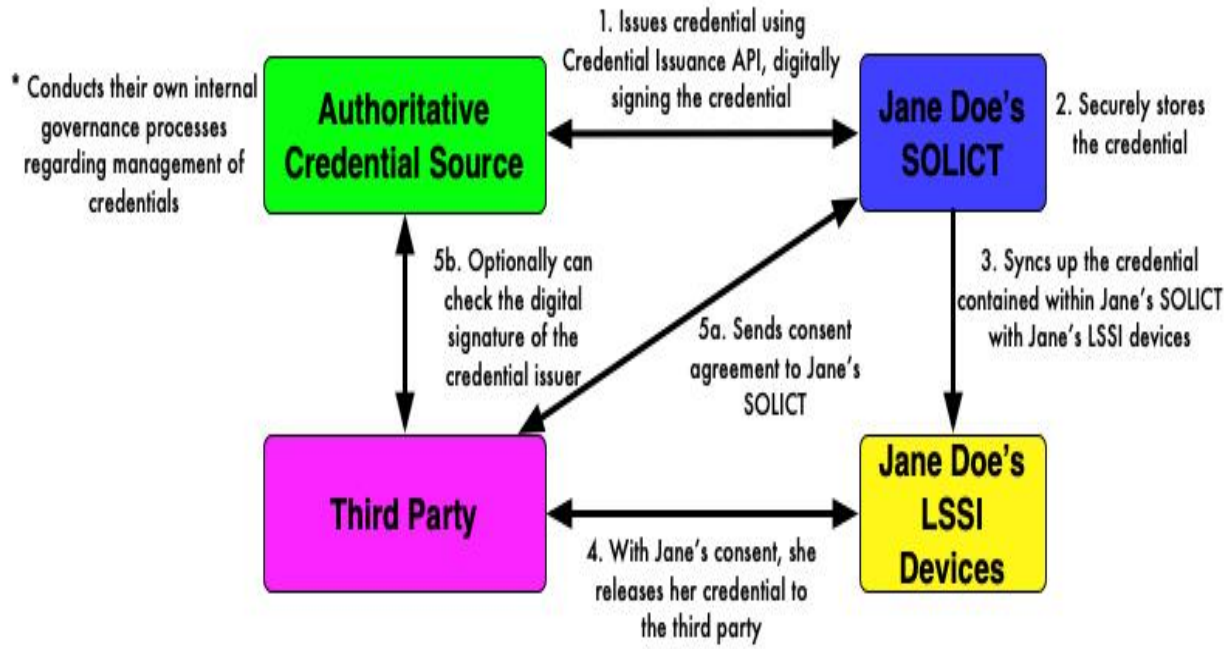
Note: The costs for this will be borne by the Non-Profit – CRVS/Government Coordination/Advisory Subcomponent Cost Centre section of this document.

Credentials Issuing Standards Subcomponent Cost Centre:

Background:

As previously described, the credential standards body will adopt credential issuance standards, which the global, independent, non-profit maintains. Included in this is a secure, credential issuance API. This in turn sends data to the person's SOLICT, leveraging TODA. Thus, the credentials standards body can prove on X date, at Y time, credential Z was securely sent from the credentials standard body to the entity's SOLICT. The entity is now in control of their credential. They can use it as and when they decide to, with their consent.

Credential Issuance Standards Example:



Credential Standards Issuance Subcomponent Costs:

The costs will be borne by the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document.

Credential Standards SOLICT (Source of Legal Identity & Credential Truth) Subcomponent Cost Centre:

Background:

All credentials issued to an entity:

- Flow from the credential issuing body
- Via the API running to new, global standards set forth by the new global, independent non-profit
- To an entity's SOLICT
- Which is now in control of the entity

Note: Each citizen needs to be educated on what the SOLICT stores re credentials applicable to them. This is where the co-design team comes into play re SOLICT.

This cost centre addresses issues with storing the credentials within the SOLICT.

Credential Standards SOLICT Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre , Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Credential Co-Design Abilities to Use Credentials Subcomponent Cost Centre:

Background:

As stated earlier, what will change is how citizens prove they have the credential. Regardless of their abilities/disabilities all citizens will leverage a co-designed SOLICT, LSSI devices and PIAM to prove their credentials.

Citizens need to understand what credentials they have, once they're entered their SOLICT, and how they can use them via their LSSI devices and/or PIAM. However, note that the co-design process must not tell the citizen when and where to use their credentials. This is up to each citizen. However, once a citizen decides they want to prove they have a credential, then the co-designed process must allow this to be done via their LSSI devices and/or PIAM rapidly and securely.

Credential Standards SOLICT Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Credential Standards LSSI (Legal Self-Sovereign Identity) Subcomponent Cost Centre:

Background:

An entity, be they human (including smart AI leveraged digital identity), Ai system or bot, needs to be able to prove they have Credential X. That's where the LSSI devices come into play.

There are five types fed legal identity and credential data from entity's SOLICT:

- Physical smart identity card
- Digital legal identity application
- Wristband containing legal identity/credentials biometrically tied to the person
- Chip implanted into an entity
- Code written to the underlying source code of the entity

For citizens, they need to understand what the LSSI device can do for them re their credentials. Let the citizen decide what, when, where and with whom to release their credentials. Then have the LSSI device securely do this. This is where co-design comes into play.

Credential Standards LSSI Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre, the LSSI Devices Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Credential Standards PIAM (Personal Identity Access Management) Subcomponent Cost Centre:

Background:

The architecture leverages AI (artificial intelligence) to create a PIAM (Personal Identity Access Management System). It manages our consents in real time, releasing sections of an entity's legal identity and credential information from their LSSI devices. Skim "**An Identity Day in the Life of Jane Doe**" to see examples of this.

Citizens must be educated on how their PIAM works with respect to releasing credentials. Then, they can make the decision of what credentials to release to whom and when this will occur. The PIAM then can execute this on behalf of the citizen. This is where co-design comes into play.

Credential Standards PIAM Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre, the Cost Centre - PIAM (Personal Identity Access Management) System and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Credential Standards API (Application Programming Interface) Subcomponent Cost Centre:

Background:

A critical security component of the architecture is leveraging:

- Common credential issuance API
- Which is constantly under 24x7x365 threat analysis by the new, global, independent non-profit
- That in turn issues rate risk threat assessments
- Which the credential issuing body responds to based on threat risk
- Thus, continually keeping the API credential interface secure

The API is the electronic front door to:

- Credential issuing body
- Entities who the credential issuing body sends their credentials to via their SOLICT

Thus, it's very, very critical to keep the API state of the art, across literally tens of thousands of credential issuing bodies around the planet. That's what this cost centre addresses.

Credential Standards API Subcomponent Costs:

The costs associated with this will be borne by the Non-Profit – API Rule Sets Subcomponent Costs and the API Cost Centre section of this document.

Credential Standards Threat Assessment Subcomponent Cost Centre:

Background:

As previously stated at the beginning of this section, the intent is to leave credential bodies in control of their systems i.e., don't rock the political boat. HOWEVER, the goal of this section is to drive into place standards for when the credential issuing body is issuing credentials to a person or entity.

There are several attack vectors that come with this:

- API interface
- SOLICT
- LSSI devices
- PIAM

Thus, this cost centre only focusses on them.

Credential Standards Threat Assessment Subcomponent Costs:

The costs associated with this will be borne by the "Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs Centre" section of this document.

Cost Centre – Legal Identity & Hive Relationships

Bakground:

Today, on the planet, we use pieces of paper, issued by government authorities, to prove our legal identity relationships. Examples include but aren't limited to:

- Parent/child
- Legal guardian/child
- Power of Attorney/person
- Etc.

This no longer works in today's age. Why?

- Paper is easily frauded.
- Doesn't work digitally locally and globally

Then there's the age of "hives" rapidly emerging. To see an example of a "bot hive" watch this video - https://www.youtube.com/watch?v=ssZ_8cqfBlE. Then read "**Hives, AI, Bots & Humans - Another Whopper Sized Problem**".

Here's what's rapidly coming at us:

- Jane Doe could have one or more AI leveraged, smart digital identities, registered in a CRVS system
- Her digital identities might belong to a "hive" which hypothetically could involve…
- One or more AI systems
- One of more digital bots
- One or more physical bots
- One of more IoT devices
- Where the risk warrants it, they're all legally registered as belonging to the "hive"

Here's the challenges in creating this:

- Speed at which hive legal identity relationships can hypothetically change i.e., seconds or minutes – so the CRVS system MUST BE FAST.
- Complex relationships i.e., it can be one to many and many to many – so the CRVS needs the architecture to allow for this.
- How to cross-link between all the different entities legal identities such that they can prove on their own the hive legal identity relationship.

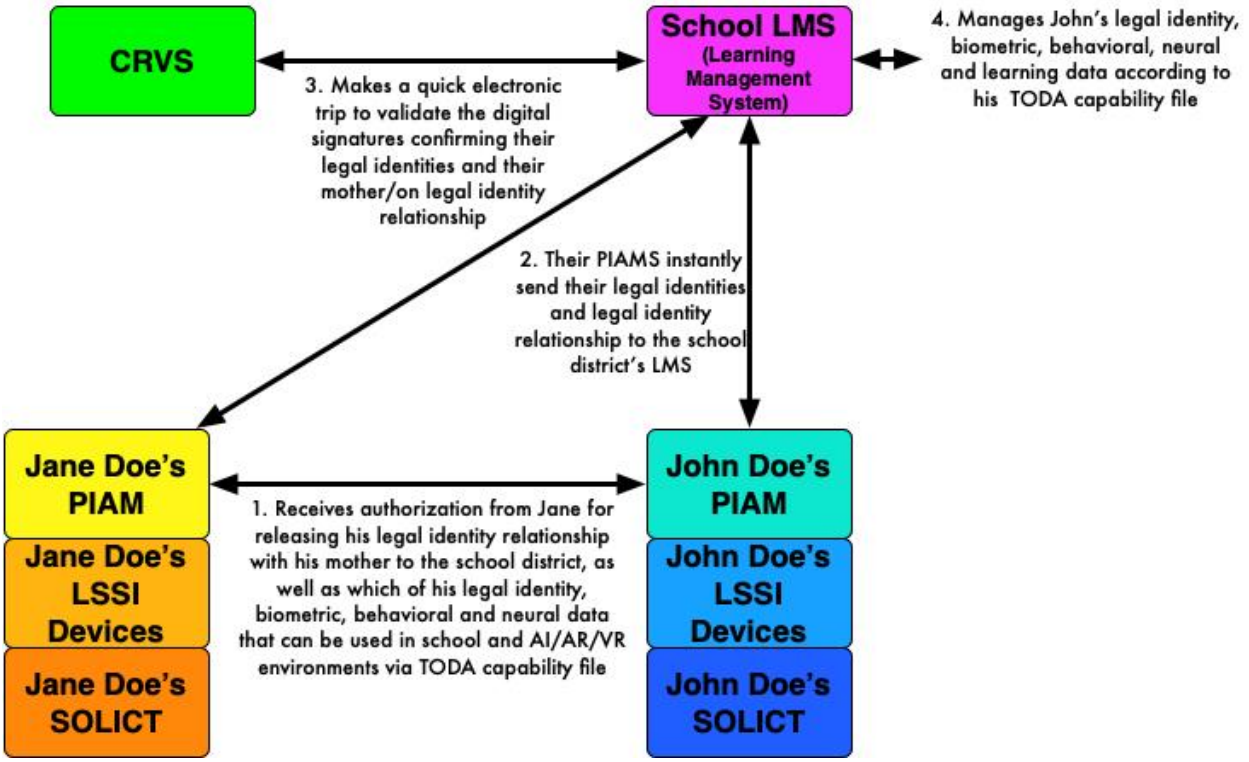
Enter TODA and Graphs

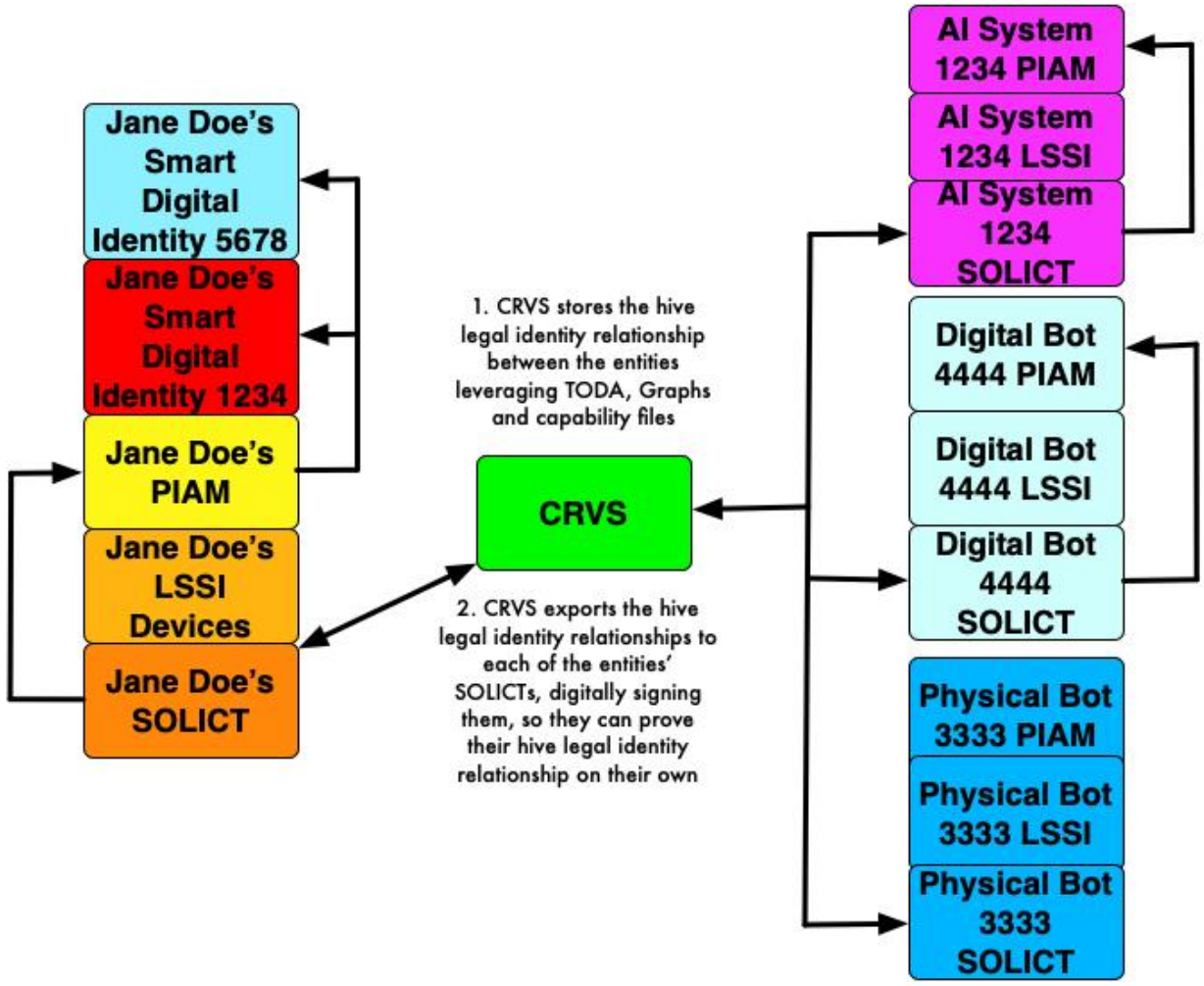
I strongly recommend readers read this, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" - https://www.linkedin.com/pulse/enterprise-change-guy-huntington-1c/

Thus:

- The CRVS will leverage graph databases to establish and manage rapidly changing legal identity relationships.
- It will also leverage TODA to send to each entity a digitally signed TODA file containing the legal identity relationships.

Legal Identity & Hive Relationship Examples:



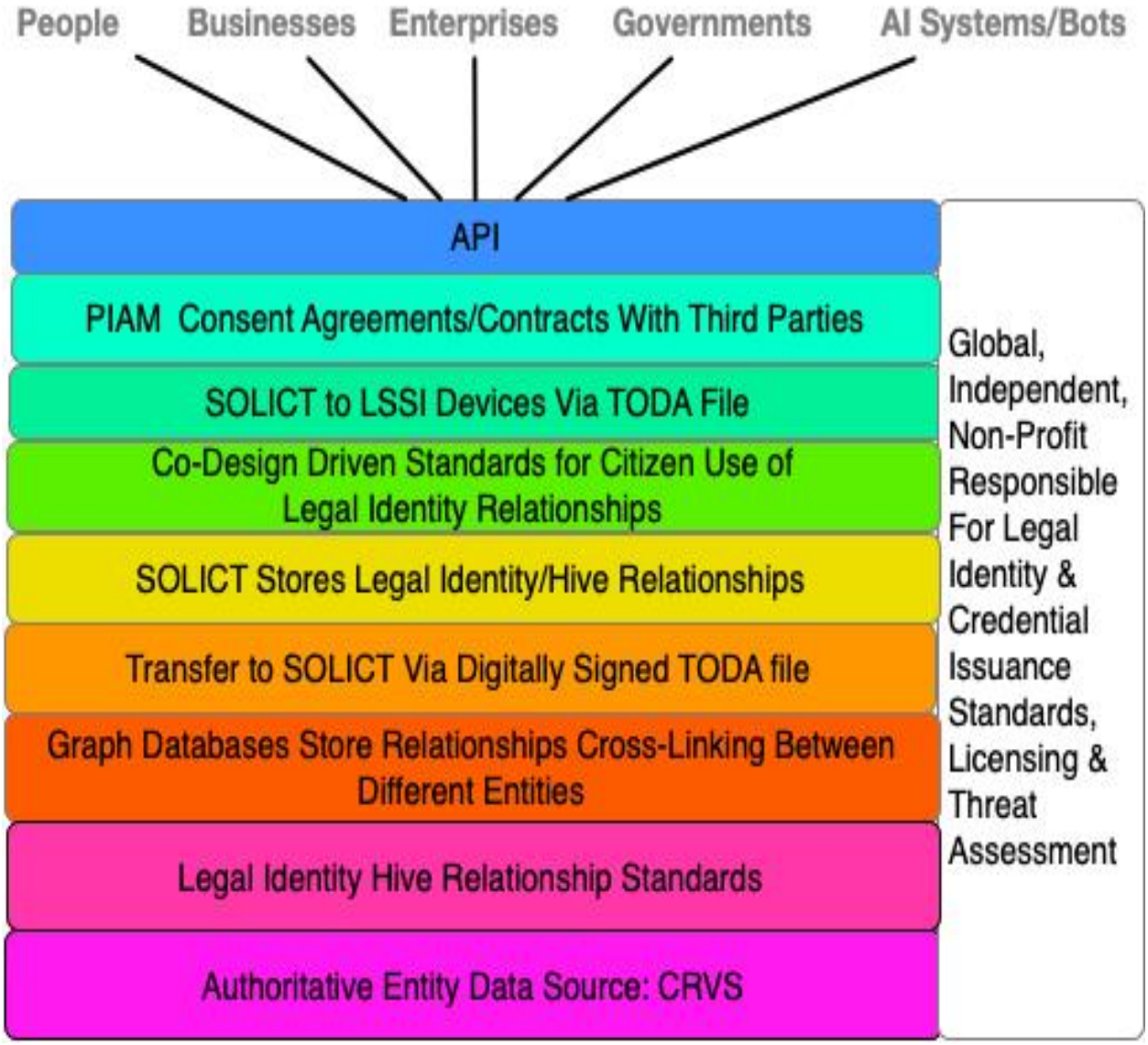


As importantly as the architecture, is all citizens, regardless of abilities or disabilities being able to:

- **Understand what a legal identity relationship is**
- **Understand what legal identity relationships they have stored in their SOLICT**
- **Understand how to use them via their LSSI devices or PIAM**
- **Allowing the citizen to make their own choice as to whom to release portions of their legal identity**
- **And then, instantly, and securely execute it**

This is what co-design brings to the table.

Legal Identity& Hive Subcomponent Cost Centres Diagram:



Other Cost Centres Dependent Upon This Cost Centre:

- AI/Bots Legal Identity & Hive Relationships Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

Legal Identity & Hive Relationships - Authoritative Entity Data Source – CRVS Subcomponent Cost Centre:

Background:

The authoritative source for legal identities of entities is the CRVS. Skim "**Legal Identity Relationships**". Then skim the CRVS Vision section of this document.

Authoritative Entity Data Source Subcomponent Costs:

The costs associated with this cost centre will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots and the CRVS Cost Centre section of this document.

Legal Identity Hive Relationship Standards Subcomponent Cost Centre:

Background:

Creating legal identity relationship/hive standards requires a new toolkit including Graphs and TODA. Hypothetically, legal identity relationships can be defined within the CRVS via graph relationships and encryption cross-linking to different entities. Then this can be exported out to the SOLICT via a TODA capability file and on to the LSSI devices. All of which requires standards. That's what this cost centre addresses.

Legal Identity Hive Relationship Standards Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre section of this document.

Legal Identity & Hive Relationships - Graph Databases Store Relationships Cross-Linking Between Different Entities Subcomponent Cost Centre:

Background:

In the 90's LDAP (lightweight Directory Access Protocol) was adopted by the emerging identity industry to act as a central enterprise hub for identities. Authoritative data sources like HRMS (Human Resource Management Systems), CRM (Customer Relationship Management), etc. fed the central LDAP. On top of the LDAP was built IAM (Identity Access Management) systems.

This is still the architecture used today. As discussed in "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" it's not going to work today. I have a friend, Derek Small, whose company, Nulli, for the past several years has been deploying graph databases together with IAM systems to handle fast changing relationships between entity identities and data.

I like graphs and have built them into the architecture, especially for legal identity relationships.

HOWEVER, I Have Some Concerns:

- Sheer speed at which an AI system can create digital bots requiring creation of legal identity hive relationships i.e., thousands to millions or more per second – can graphs work at this speed?
- Hypothetically high-volume identity relationship/hive validations in the CRVS system – can graph systems cope with this? What volume do they "crap out"?
- Danger of DNS (Denial of Service) type attacks on the CRVS system from the Evil Inc.'s and malicious states of the planet – graphs are part of the end-to end CRVS system. How will these attack be mitigated?

All the above must be addressed in the design and implementation of graphs within the CRVS system.

Authoritative Entity Data Source Subcomponent Costs:

The costs associated with this cost centre will be borne by the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre section of this document.

Legal Identity & Hive Relationships - Transfer to SOLICT (Source of Legal Identity & Credential Truth) Via Digitally Signed TODA File Subcomponent Cost Centre:

Background:

While architecting for the legal identity relationship/hives, I knew in my head there was some problems/challenges to be overcome:

- What global/local legal identity/hive relationship standards would need to be created?
- How would these be securely exported out of the CRVS to the entity's SOLICT
- Since many of the new emerging hive entity relationships would be fast changing, how would this be done at fast transactional speeds?
- Security implications of all the above. As mentioned in other sections of this doc, I was wondering of how to mitigate of DNS type attacks (denial of service) on the new, global, independent non-profit who's managing the SOLICTS in the global cloud?

Enter TODA Files and New Local/Global Legal Identity Relationship & Hive Standards:

Read, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**". It describes how TODA:

- Can work at transactional speeds
- Containing a TODA file which could be anything

When I saw this, I knew it was a new foundational piece of the new legal identity architecture.

If new local/global standards are created for legal identity and hive relationships, then the TODA file can carry it from the CRVS endpoint to the entity's SOLICT endpoint. Thus, it can be proved on X date, at Y time, a TODA CRVS legal identity/hive file containing a hash of the file as well.

Transfer to SOLICT Via Digitally Signed TODA File Subcomponent Costs:

The costs associated with this will be born in the Non-Profit – Manages SOLICT Standards, the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) and the CRVS Cost Centre section of this document.

SOLICT (Source of Legal Identity & Credential Truth) Store Legal Identity/Hive Relationships Subcomponent Cost Centre:

Background:

The CRVS is the authoritative source for an entity's legal identity/hive relationships. One challenge is how this information is transferred to the entity's SOLICT allowing it to legally prove legal identity/hive relationships.

As I see it, it will likely involve creating the following within the SOLICT from the CRVS:

- Graph file with entities digitally signed by the CRVS
- Showing their relationship with other entities (likely via TODA files)

As importantly, citizens, regardless of their abilities or disabilities, must be able to:

- **Understand what a legal identity relationship is**
- **Understand what legal identity relationships they have**
- **Understand they're stored in their SOLICT**

This is what co-design brings to the table.

SOLICT Store Legal Identity/Hive Relationships Subcomponent Costs:

The costs associated with this will be born in the Non-Profit – Manages SOLICT Standards and the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Cost Centre:

Background:

Each citizen on the planet, regardless of their abilities or disabilities, need to be educated about their legal identity relationships and how they can use them. Thus, this cost centre addresses this from the citizen's SOLICT to their LSSI devices to their PIAM.

C0-Design Driven Standards for Citizen Use of Legal Identity Relationship Subcomponent Costs:

The costs associated with this will be born in the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Legal Identity & Hive Relationships - SOLICT to LSSI (Legal Self Sovereign Identity) Devices Via TODA File Subcomponent Cost Centre:

Background:

The SOLICT will leverage an API to send a TODA file to the LSSI devices. With this, each citizen can now control, when, where and with whom to release portions of their legal identity relationships. As importantly, leveraging co-design, it enables all citizens, regardless of their abilities or disabilities to do this.

SOLICT to LSSI Devices Via TODA File Subcomponent Costs:

The costs associated with this will be born in the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre ,the LSSI Devices Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Legal Identity & Hive Relationships - PIAM (Personal Identity Access Management) Consent Agreements/Contracts With Third Parties Subcomponent Cost Centre:

Background:

Consider the current crappy consent laws around the planet. Skim this old paper "**Consent Principles in the Tsunami Age**". It suggests creating zones of consent. Here's the main point – the PIAM will be the manager of the consent agreements and prompt Jane or John Doe, when the consent agreements require it, to affirm their consent in clear terms. It thus becomes a prime conversation regarding privacy.

Good news - AI contract law is rapidly evolving. Thus, I can see the implementation of AI contact law within a PIAM app, along with standard consent contracts being developed. All consent agreements MUST be stored in the person's SOLICT.

As noted in prior sections, each citizen, regardless of their abilities or disabilities, must understand what their PIAM does re legal identity relationships. This is where co-design comes into play. However, the co-design must not tell the citizen what to do re-releasing their legal identity relationship information. This is outside the scope. It must allow each citizen to make their own choice. Then, the PIAM must be able to rapidly execute it.

PIAM Consent Agreements/Contracts With Third Parties Subcomponent Costs:

The costs associated with this will be borne in the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre, the Cost Centre - PIAM (Personal Identity Access Management) System and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Legal Identity & Hive Relationships API (Application Programming Interface) Subcomponent Cost Centre:

Background:

A major performance and security question is how to securely access:

- CRVS entity legal identification, identity/hive relationships and authorization data?
- Credential issuance data?
- Sending the above data to the SOLICT?
- SOLICT communicating with the LSSI devices?
- PIAM managing the LSSI devices?
- Third party consent agreements sent to the SOLICT?

Answer - Create standard API's (Application Programming Interface).

It addresses the problems of how to query billions of us with AI leveraged, smart digital identities and trillions of AI systems and bots for their legal identities and/or for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed.

Add to the above complexity the rapid attack new attack vectors being created against the legal identity framework from this curve. The API is the electronic front door. Which is why the architecture has the new, global, independent, well-funded, non-profit. One of its tasks is to do 24x7x365 threat analysis and produce rated threats and threat responses. Thus, the API's created will likely be very frequently updated.

Legal Identity & Hive Relationships API (Application Programming Interface) Subcomponent Costs:

The costs associated with this will be borne in the Non-Profit – API Rule Sets Subcomponent Costs and the Cost Centre: API (Application Programming Interface) section of this document.

Cost Centre – Legal Authorization Rights

Background:

Skim these two articles on AI/AR/VR environments in a global classroom:

- "**Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy**"
- "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**"

It has a student, John Doe, who has his learning assistant bot "AssistBot", with a human teacher, Sally Goodteacher, and two teaching assistant bots, BobBot and PattyBot. Further, authorization contracts need to be created:

- Between not only John's parent Jane Doe, for him and his AssistBot with the school district
- But also with school districts creating the AI/VR global learning environment
- All specifying what legal identity data can be used by Sally Goodteacher, BobBot, PattyBot and AssistBot
- Also specifying how the data is used, stored, shared, archived, and terminated

So, an AI system, physical and/or digital bots will require authorization rights, which depending on risk, must be spelled out in contracts. My dumb question is how will this be done in a secure, scalable manner? Where will the contracts pertaining to a specific legal identity AI systems or bots be stored? **Yes, it's complicated. That's the world we're entering.**

Which led me to a protocol called TODA, to rethink how not only contracts are sent from one party to another, but also to begin to create authorization rights standards, leveraging TODA capability files. Skim this article "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

.

I don't have a magic wand to wave that solves all AI systems and bots authorization rights and contracts. However, I can see the need to come together to agree on preliminary authorization rights, protecting a human and AI system/bots privacy. Which is why I've included capability files in my first guesstimate at an architecture.

Note:

Within this cost centre doc there are two cost centres pertaining to legal authorization rights:

- **This cost centre**
- **CRVS – Legal Authorization Rights Cost Centre**

Why two cost centres? The CRVS is the authoritative source for legal identity and legal identity relationships only. Legal authorization might or might not use CRVS defined relationships. Thus, I've broken it out into two separate cost centres. The design and implementation teams might or might not want to merge the two cost centres.

Legal Authorization Rights is Complicated!

There are literally likely tens of thousands or more authorization scenarios in real life. Many of them are agreed to by the entity and other parties. Some of them however require:

- Legal attestations of the underlying identities
- PLUS, legal agreement the entity can make authorization decisions on behalf of another (like Jane Doe making authorization decisions on behalf of her son John Doe and his AssistBot)

That's where the CRVS, legal identity relationships and authorization come together. It requires:

- CRVS to attest the entity is who they legally claim to be e.g., Jane Doe, John Doe and AssistBot
- CRVS to create legal identity relationships e.g., Parent/child relationship and owner of Assistbot
- **Authorization rights for the entities e.g., Jane can grant authorization for both John and AssistBot to the school district and their global learning environment**

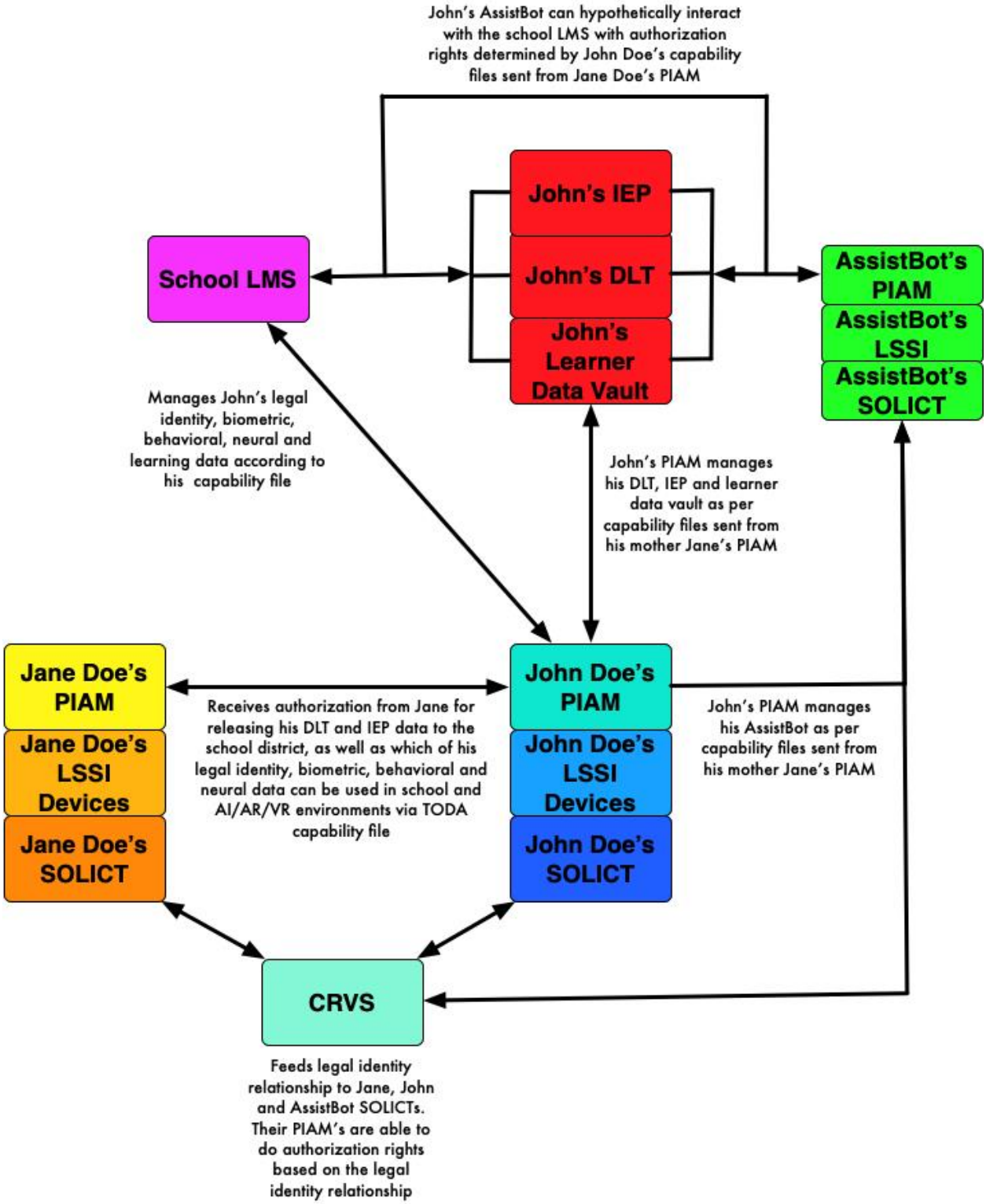
My suggestion is to:

1. First focus on use cases like above that require legal identity, relationship/hives legal relationships and authorization for only legal identity data
    a. DO NOT FOCUS BEYOND THIS BECAUSE IT'S A LARGE CAN OF LEGAL WORMS – KEEP IT TIGHTLY FOCUSSED
2. Focus on one to three industries i.e., keep it small and tightly focused with willing partners
3. Evolve some legal authorization standards for humans, AI systems and bots authorization rights
4. Assign the authorization rights using TODA capability files sent to each entity leveraging Kantara User Managed Access (UMA) to store it in a common, secure, location for each entity i.e., the SOLICT.

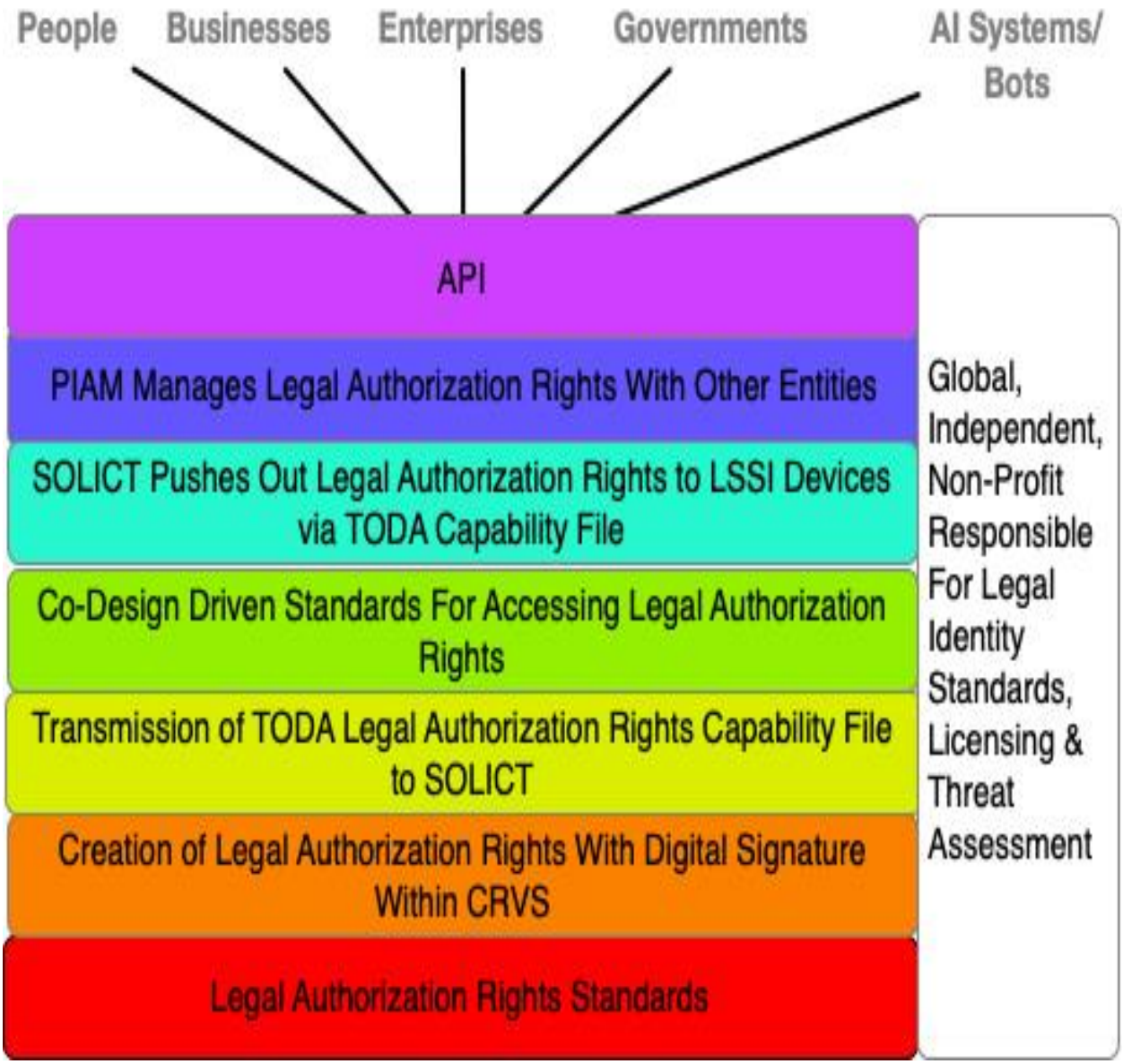
5. Address yet another challenge with legal authorization right i.e., security. In the SOLICT Cost Centre section of this document, it discusses performance and security considerations which MUST be addressed. It applies to TODA capability files as well.
6. Enable all citizens on the planet, regardless of their abilities or inabilities, to understand legal authorization rights and how to prove them. This is where co-design comes into play.

I can also see how the PIAM, and other databases will likely be leveraged by companies as they create abilities for entities to manage authorization rights. THIS MUST BE KEPT OUTSIDE THE SCOPE OF THE LEGAL IDENTITY ARCHITECTURE THIS DOCUMENT ADDRESSES.

Legal Authorization Rights Example:



Legal Authorization Rights Subcomponent Cost Centres Diagram:



Other Cost Centres Dependent Upon These Cost Centres:

- AI/Bots Legal Authorization Rights Subcomponent Cost Centre
- CRVS Creation of Legal Authorization Rights By Authorized Entity With Their Digital Signature Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

Legal Authorization Standards Subcomponent Cost Centre:

Background:

My suggestion is to only focus on use cases that require legal identity, relationship/hives legal relationships and authorization for only legal identity data. **DO NOT FOCUS BEYOND THIS BECAUSE IT'S A LARGE CAN OF LEGAL WORMS – KEEP IT TIGHTLY FOCUSSED.**

Legal Authorization Standards Costs:

Costs will be borne by the Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre section of this document.

Legal Authorization Rights - Creation of Legal Authorization Rights With Digital Signature Within CRVS Subcomponent Cost Centre:

Background:

This cost centre addresses these questions:

1. How will authorization rights be stored within the CRVS database?
2. How will it be proven that the CRVS created the authorization rights?

Creation of Legal Authorization Rights With Digital Signature Within CRVS Subcomponent Costs:

Costs will be borne by the CRVS – Legal Authorization Rights Cost Centre and the Non-Profit - Manages Digital Signature Entity Standards Subcomponent Cost Centre section of this document.

Legal Authorization Rights - Transmission of TODA Authorization Capability File to SOLICT Subcomponent Cost Centre:

Background:

The CRVS must securely send the authorization rights to the entity's SOLICT. This will be done via a TODA capability file. It also relies upon security standards for the API (Application Programming Interface).

Transmission of TODA Authorization Capability File to SOLICT Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) sections of this document.

Legal Authorization Rights - Co-Design Driven Standards For Accessing Legal Authorization Rights Cost Centre:

Background:

As earlier stated, all citizens on the planet, regardless of their abilities or disabilities, need to understand legal authorization rights and how to prove them. This is where co-design comes into play.

Co-design must be able to educate a citizen about their applicable legal authorization rights. IT MUST NOT TELL THE CITIZEN WHAT TO DO. INSTEAD, IT MUST LET THE CITIZEN MAKE THEIR OWN CHOICES RE DECIDING WHAT LEGAL AUTHORIZATION RIGHTS TO RELEASE TO WHOM AND WHEN. Then co-design should ensure that the citizen's choice is quickly, securely, executed.

That's what this cost centre addresses from the SOLICT to the LSSI device to the PIAM.

Legal Authorization Rights - Co-Design Driven Standards For Accessing Legal Authorization Rights Subcomponent Costs:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Legal Authorization Rights - SOLICT Pushes Out Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Cost Centre:

Background:

The SOLICT in turn pushes out legal authorization rights to the entity's LSSI devices. This will be done again using TODA capability files. The major question is how will each type of LSSI device store the authorization information?

Equally important, as noted in the prior section, is the use of co-design to educate the citizen about their legal authorization rights and then to assist them, once they've made a choice on who to release them to, to execute it securely and quickly.

SOLICT Pushes Out Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Costs:

The costs for this subcomponent will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre, the LSSI Devices Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Legal Authorization Rights - PIAM Manages Authorization Rights With Other Entities Subcomponent Cost Centre:

Background:

The AI leveraged PIAM (Personal Identity Access Management), manages authorization consents with other entities, governments, companies, enterprises, etc. The major question is how will it do this?

As note in prior sections, equally important, is the ability for each citizen, regardless of their abilities or disabilities, to understand what legal authorization rights they have. Each citizen must be able to configure their PIAM, at the citizen's discretion, to release portions of their legal authorization information to other parties. The PIAM then must be able to securely and instantly do this. All of this is where co-design comes into play.

PIAM Manages Authorization Rights With Other Entities Subcomponent Costs:

The costs for this subcomponent will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre, the Cost Centre - PIAM (Personal Identity Access Management) System and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

Legal Authorization Rights - PIAM API Subcomponent Cost Centre:

Background:

As noted throughout this document, a major performance and security question is how to securely access:

- CRVS entity legal identification, identity/hive relationships and authorization data?
- Credential issuance data?
- Sending the above data to the SOLICT?
- SOLICT communicating with the LSSI devices?
- PIAM managing the LSSI devices?
- Third party consent agreements sent to the SOLICT?

Answer - Create standard API's (Application Programming Interface).

It addresses the problems of how to query billions of us with AI leveraged, smart digital identities and trillions of AI systems and bots for their legal identities and/or for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed.

Add to the above complexity the rapid attack new attack vectors being created against the legal identity framework from this curve. The API is the electronic front door. Which is why the architecture has the new, global, independent, well-funded, non-profit. One of its tasks is to do 24x7x365 threat analysis and produce rated threats and threat responses. Thus, the API's created will likely be very frequently updated.

Legal Authorization Rights API (Application Programming Interface) Subcomponent Costs:

The costs associated with this will be borne in the Non-Profit – API Rule Sets Subcomponent Costs and the Cost Centre: API (Application Programming Interface) section of this document.

Cost Centre – SOLICT (Source of Legal Identity & Credential Truth)

Background:

When architecting for a new legal identity system for humans, AI systems and bots, I wanted to build it from the ground up on privacy by design. SOLICT was designed addressing this use case:

> "Jane Doe is targeted by a government, which deletes her CRVS record and all other government identity records. How can Jane Doe prove her legal identity?"

Scott David, University of Washington, gave me the idea of creating, for each person, a separate database, which they can control, that exists in the cloud, outside of a jurisdiction's reach. Thus, was born SOLICT. I've since applied it to AI systems and bots.

It reduces the potential impact when a large, legal identity database is breached, with all the records of many entities now hacked. By reducing the attack surface for each entity, it makes it more complex and costly for criminals to do their work across many different entity's legal identities i.e., it's highly decentralized.

Skim these two articles about SOLICT:

- "**Give Each Entity Their Own Source of Legal Identity & Credential Truth Database (SOLICT)**"
- "**A Database Per Entity on the Planet - A Deeper Dive on SOLICT**"
    - **Note – this is a long read BUT I STRONGLY URGE PEOPLE TO WADE THEIR WAY THROUGH IT. IT LAYS OUT LOTS OF RISK FACTORS**

SOLICT will contain all the consent agreements a person enters with third parties. It does this via leveraging an existing protocol, "**Kantara User Access Management (UMA)**" as well as TODA. Skim this, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

How will this be funded and managed? The SOLICT databases will be managed by the global, independent non-profit. **The scope of SOLICT is only legal identity, credentials, and consent agreements i.e., nothing more.**

Security Challenges – Performance, Security & Usability

SOLICT will become key to entities wanting to write to the SOLICT, interactions with an entity's LSSI (legal self-sovereign identity) devices and their PIAM (personal identity access management) system.

Performance:

I could see in my mind the awesome speeds at which say digital bots can be created. Over time, it could easily be in the millions or billions per second/. Thus, I saw the CRVS local/global systems struggling not only with registration/validation performance, BUT ALSO CREATING A SOLICT FOR EACH NEW ENTITY. Thus, this must be addressed in design use cases.

Security:

I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks against the new age CRVS systems. They could effectively "drown the CRVS" with creations of new entities and sending out to the global, independent non-profit, who's managing the SOLICTS, LOTS of SOLICT creations. Thus, this must be addressed in design use cases.

Updating:

I could also see the business process problems of keeping track of trillions or more AI system and bots legal identities. How would the CRVS be able to be notified an entity had changed, been adopted into another entity, terminated, etc. and then how would it notify the entity's SOLICT? Thus, this must be addressed in design use cases.

Citizens Understanding What Their SOLICT Is and Does:

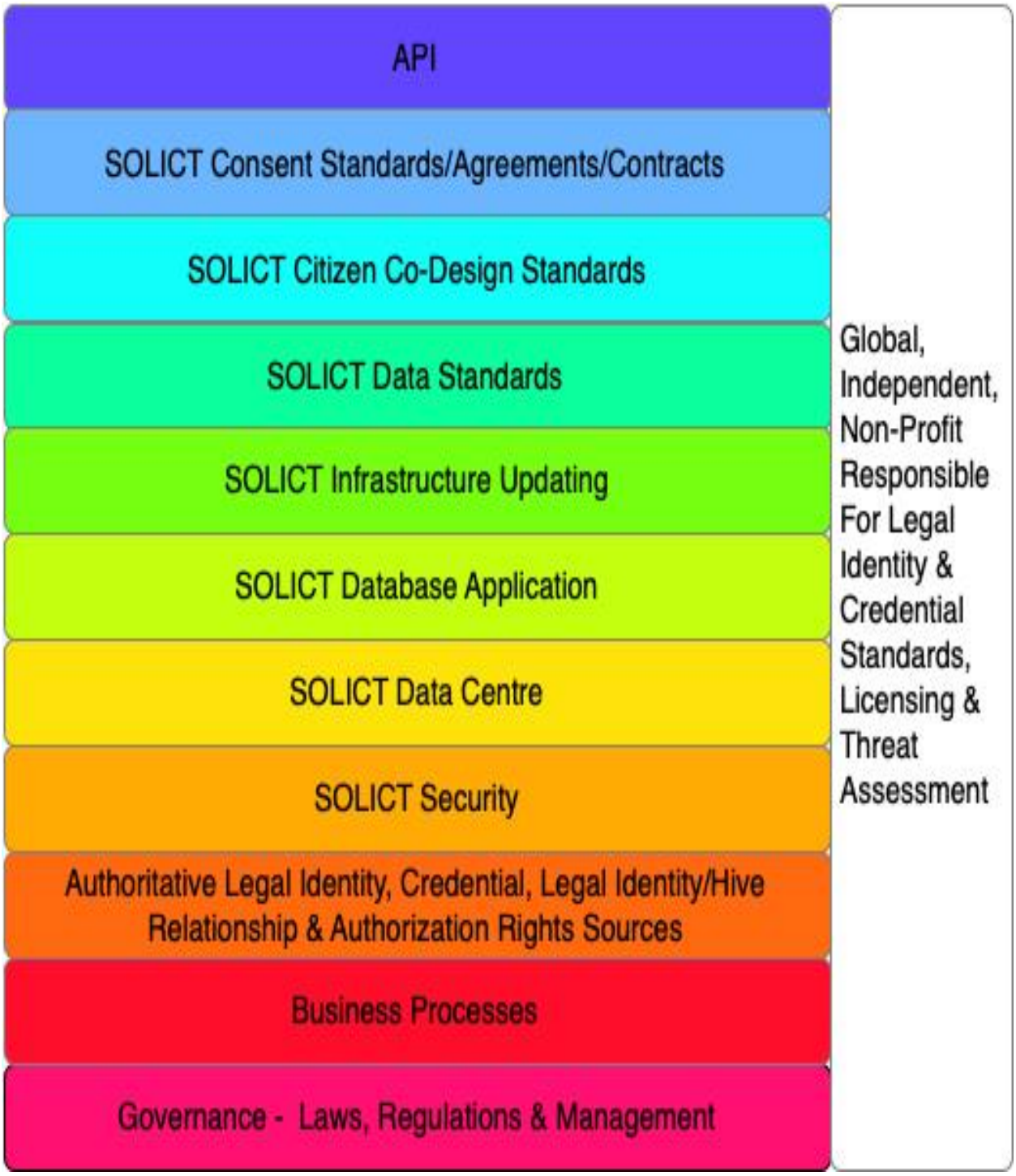
Literally billions of people around the planet will be leveraging their SOLICT to prove their legal identity and credentials. Regardless of their abilities or disabilities, they need to understand:

- What their SOLICT is
- How they can manage it via their LSSI devices and/or PIAM

This is where co-design comes into major play to deliver it to them around the planet and around the clock.

My message? All of the above problems/challenges are whopper sized. LOTS OF THOUGHT MUST BE APPLIED BEFORE DESIGNING AND IMPLMENTING

SOLICT Subcomponent Cost Centres Diagram:



Other Cost Centres Dependent Upon These Cost Centres:

- AI/Bots SOLICT (Source of Legal Identity & Credential Truth) Subcomponent Cost Centre
- CRVS - Transmission of TODA Legal Authorization Capability File to SOLICT Subcomponent Cost Centre
- Credential Standards SOLICT (Source of Legal Identity & Credential Truth) Subcomponent Cost Centre
- Legal Identity & Hive Relationships - Transfer to SOLICT (Source of Legal Identity & Credential Truth) Via Digitally Signed TODA File Subcomponent Cost Centre
- Legal Authorization Rights - Transmission of TODA Authorization Capability File to SOLICT Subcomponent Cost Centre
- LSSI Device Interfaces/Updating from SOLICT
- Rethinking Learning - SOLICT (Source of Legal Identity & Credential Truth) Cost Centre
- Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

SOLICT Governance – Laws, Regulations & Management Subcomponent Cost Centre:

Background:

SOLICT will be managed by the proposed global, independent non-profit. It will become the authoritative source for an entity's LSSI devices.

Authoritative sources feeding the SOLICT:

- Entity legal identities – CRVS
- Entity legal identity/hive relationships – CRVS
- Entity legal authorization – CRVS
- Credentials – credential issuing bodies
- Consents – any party, company, government to which the entity grant's their consent to release sections of their legal identity and/or credentials

ALL OF THIS MUST BE VERY SECURLEY DONE LEVERAGING API'S AND TODA.
Skim these:

- API Cost Centre section of this document
- "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"

SOLICT Governance Subcomponent Laws/Regulations:

Jurisdictional laws and regulations will need to be created and/or modified acknowledging the SOLICT as well as legally accepting it as the mostly authoritative source of an entity to manage on their own. Here's one of the challenges in doing this. Cross-border prosecution enforcing SOLICT laws and regulations.

Skim, "Fighting cybercrime – what happens to the law when the law cannot be enforced?" It shows the pathetic 0.05% success rate of prosecuting cybercrime. Thus, Jane Doe might be screwed in protecting her SOLICT from Evil Inc. who's operating out of a jurisdiction where they can't be prosecuted.

SOLICT Governance Subcomponent Management:

The new, global, independent non-profit will have management abilities over the billions and trillions of SOLICTS. This is both good and bad. It gives them potential abilities to misuse SOLICTs. I strongly suggest readers read "**A Database Per Entity on the Planet - A Deeper Dive on SOLICT**" to fully understand the management complexities SOLICT brings with it. It discusses things like death/termination, etc.

Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit – CRVS/Government Coordination/Advisory Subcomponent Cost Centre

SOLICT Governance Laws, Regulations & Management Subcomponent Requirements:

- Be legally recognized by the jurisdiction as a place the jurisdiction can write to with a person's legal identity and/or credential information
- The SOLICT will accept a jurisdiction's local authoritative source digital signature as part of the TODA information package being written
- Each SOLICT will have its own digital signature to digitally verify itself to local authoritative source
- Each SOLICT will have a governance contract determining which entities can manage a SOLICT on behalf of another person
    - Jane Doe, as mother of John Doe, would be assigned by the local jurisdiction as his mother at birth, with the jurisdiction cryptographically cross-linking both John and Jane's SOLICT files establishing the relationship
    - John Doe's SOLICT would issue a contract to his mother's SOLICT specifying what she can do to manage his legal identity, etc. as per the legal governance requirements, to new global standards, set forth and managed by the global, independent non-profit
    - If Jane dies, the local jurisdiction assigns a legal guardian, Sally Smith, for John. The jurisdiction writes the changes to both Sally and John's SOLICT files, as well as changing the status of Jane's SOLICT to deceased. The contract between Jane and John is now void. Sally would then receive a new contract from John's SOLICT, setting forth what she can do to manage his legal identity
- Have governance processes for changes to a person's SOLICT data
- Have governance processes for storage and archival of a person's SOLICT
- Have governance processes for notaries, with a person's consent, able to search on a SOLICT, doing a comparison of a person's forensic biometrics
- Have governance processes for managing consent contracts which are stored in SOLICT
- Have each jurisdiction adopting SOLICT/LSSI adopt a common identity assurance standard with the highest level of identity assurance being given to a person, at birth i.e., their forensic biometrics are obtained and stored not only in the CRVS system but also the person's SOLICT
- Transfer over administration of this to the non-profit governance cost centre

SOLICT Governance Laws, Regulations & Management Subcomponent Costs:

These costs will be borne by the Non-Profit – Governance Coordination/Advisory Subcomponent Cost Centre section of this document.

SOLICT Business Processes Subcomponent Cost Centre:

Background:

SOLICTs are an entity's consent storage repository. This requires some kind of legal agreement/contract agreed by the entity with another party.

Note that weak business processes are an attack vector against an entity's SOLICT. The same applies to the business processes used by the CRVS and credential issuing bodies.

Business process use cases must be prepared detailing the business process flow for entering, changing, storing, and archiving of data. I have an underlying premise that SOLICT data can never be deleted - to prevent malicious criminals from deleting data and then claiming it was never written to SOLICT. This presents a problem when perhaps data was erroneously written to a SOLICT, etc. Thus, these are just some of the use cases that will need to be developed and worked through by a team. In effect, the business processes drive how a SOLICT will be used.

SOLICT Business Process Subcomponent Costs:

These costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre section of this document.

SOLICT Authoritative Legal Identity, Credential, Legal Identity Relationships/Hive and Authorization Rights Sources Subcomponent Cost Centre:

Background:

Authoritative sources feeding the SOLICT:

- Entity legal identities – CRVS including:
  - Humans and AI leveraged, smart digital identities
  - AI systems and bots
- Entity legal identity/hive relationships – CRVS
- Entity legal authorization – CRVS
- Credentials – credential issuing bodies
- Consents – any party, company, government to which the entity grant's their consent to release sections of their legal identity and/or credentials

SOLICT Authoritative Legal Identity/Credential Sources Subcomponent Costs:

- CRVS entity legal identity related costs are borne in the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre section of this document
- Credential related costs are borne in the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document.
- Entity legal identity/hive relationships standards are borne in the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre section of this document
- Entity legal authorization rights and consent standards are borne in the Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre section of this document

SOLICT Security Subcomponent Cost Centre:

Background:

Performance:

I see in my mind the awesome speeds at which say digital bots can be created. Over time, it could easily be in the millions or billions per second/. Thus, I saw the CRVS local/global systems struggling not only with registration/validation performance, BUT ALSO CREATING A SOLICT FOR EACH NEW ENTITY. Thus, this must be addressed in design use cases.

Security:

I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks against the new age CRVS systems. They could effectively "drown the CRVS" with creations of new entities and sending out to the global, independent non-profit, who's managing the SOLICTS, LOTS of SOLICT creations. Thus, this must be addressed in design use cases.

Updating:

Finally, I could also see the business process problems of keeping track of trillions or more AI system and bots legal identities. How would the CRVS be able to be notified an entity had changed, been adopted into another entity, terminated, etc. and then how would it notify the entity's SOLICT? Thus, this must be addressed in design use cases.

There's LOTS of Security Attack Vectors to Consider:

Examples include but aren't limited to:

- API's (including DNS, port security, encryption, etc.)
- Network
- Databases
- Digital signatures
- Business processes
- Non-profit governance and management
- Cloud/servers
- Etc.

Rapid Rate of Change Creating New Attack Vectors:

The rate of change depicted by this curve hypothetically means, EACH HOUR, new attack vectors are being created. To address this, that's why on the right-hand side of the SOLICT cost component diagram is a global, independent non-profit who does 24x7x365 threat analysis against all the SOLICT attack vectors noted above.

It will constantly produce attach threat risk assessments. Thus, a very high threat risk MUST be responded to in a SOLICT, authoritative source writing to the SOLICT, SOLICT API, etc., within hours. This is bringing industry best security practices to the world of legal identity and SOLICTs.

SOLICT Security Subcomponent Costs:

Costs associated with this are borne in the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document.

SOLICT Data Centre Subcomponent Cost Centre:

Background:

SOLICT was created to protect an entity's n legal identity and credential data, mitigating risk of a jurisdiction deleting the entity from their CRVS and other national identity systems. It does this by having the jurisdictional CRVS/authoritative sources write to a SOLICT for each person, which exists in the cloud, outside the jurisdiction's control. All of this sounds good on paper, but how will it be deployed, such that it's always available 24x7x365, year after year, and can withstand events like sun GMD EMP/HEMP events noted in "**When Our Digital Legal Identity Trust Goes Poof!**"?

Then there's the sheer volume of the number of databases i.e., billions to trillions. How will the data centre/cloud strategy address this? What is the associated design, implementation and maintenance costs associated with this?

Next is the power consumption that billions or trillions of SOLICTS will place upon the data centres. It requires low power consumption per SOLICT.

My thinking when creating the idea of SOLICT was the operational cost would be borne by the global independent non-profit. I saw in my mind the non-profit collecting revenue from each local jurisdiction by licensing to them the new age CRVS system on an annual basis, up to a fixed amount. Taking this vision and making it a reality are two different things.

All the above is the design and cost challenge of the data centre/cloud strategy SOLICT will use.

SOLICT Data Centre/Cloud Subcomponent Costs:

Cost will be borne in the Non-Profit – Manages SOLICT Databases Subcomponent Cost Centre and the Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre section of this document.

SOLICT Database Application Subcomponent Cost Centre:

Background:

SOLICT is an out of the box idea for out of the box times. My thinking is to explore out of the box database applications as well for SOLICT rather than simply deferring to use of existing database types.

I'M NOT A DATABASE EXPERT. However, I have a friend, Derek Small, CEO of Nulli, who for the past several years has his company pioneering use of graph databases with IAM (Identity Access Management) systems. I strongly suggest readers read "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

A consideration will be the mapping of legal identity/hive relationships between entities. This will range from:

- One to one
- One to many
- Many to many

The future is telling us many of these relationships might only last seconds to minutes. Skim "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**". Thus, the type of database used must be low cost, efficient, secure, easily upgradeable and function well in a cloud, at very, very fast speeds.

Authorization Rights:

The CRVS is going to send to the SOLICT a TODA capability file containing the authorization rights. Which leads to the dumb question, "How will this be stored within the SOLICT database?" This must be addressed in this cost centre.

Note:

The actual identity, credential, legal relationship/hives and authorization rights data stored in the database will likely be small in terms of data quantity. HOWEVER, the consent contracts stored in the database will likely be very large over the lifespan of a person, and potentially become large in terms of data quantity.

SOLICT Database Application Subcomponent Costs:

Costs associated with this will be borne in the Non-Profit – Manages SOLICT Databases Subcomponent Cost Centre section of this document.

SOLICT Infrastructure Updating Subcomponent Cost Centre:

Background:

SOLICT will likely have billions to trillions of user's databases, which resides in the cloud. This also includes the associated infrastructure from the firewalls, load balancers, API's, network to the actual servers. The entire end-to-end infrastructure must be able to be upgraded on either a regular basis or, in an emergency fix.

EACH SOLICT must always be available. Finally, as this tech curve unfolds, it means that new tech will rapidly evolve, which hypothetically could mean replacing or rapidly updating the SOLICT database. All this means, right from the beginning, a secure infrastructure updating model needs to be well thought through, allowing for these possibilities.

SOLICT Infrastructure Updating Subcomponent Costs:

Costs will be borne in the Non-Profit – Manages SOLICT Databases Subcomponent Cost Centre section of this document.

SOLICT Data Standards Subcomponent Cost Centre:

Background:

The driving force behind having a legal self-sovereign identity (LSSI) is it's interoperable around the planet both physically and digitally. THUS, AS I SEE IT, ALL OF THE DATA STORD WITHIN EACH ENTITY'S SOLICT MUST BE TO GLOBAL STANDARDS. This includes:

- CRVS issued entity legal identity data
- CRVS issue legal identity/hive relationship data
- CRVS issued legal authorization rights data
- Credential bodies issuing credentials to the entities
- Consent agreements agreed to by an entity with a third party

This is easier said than done. It requires global coordination on:

- Entity legal identification standards
- Entity legal identity/hive relationships standards
- Entity legal authorization rights standards
- Credential bodies credential issuance standards
- Entity digital signature standards
- Consent agreement standards

SOLICT Data Standards Subcomponent Costs:

Overall SOLICT standards will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre section of this document.

SOLICT Citizen Co-Design Standards Subcomponent Cost Centre:

Background:

Citizens, regardless of their abilities or disabilities, should understand:

- What their SOLICT is
- What legal identity and credential information data is stored in it
- How they can manage the information be determining who to release portions of the data to via their LSSI devices and/or PIAM's

That's what this cost centre addresses via co-design.

SOLICT Citizen Co-Design Standards Subcomponent Costs:

Overall SOLICT codesign standards will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

SOLICT Consent Standards/Agreements/Contracts Subcomponent Cost Centre:

Background:

Our consent legal framework around the planet is badly broke. The "2017 Deloitte Global Mobile Consumer Survey; US Edition" states "**For ages 18 to 34, the rate of acceptance of terms and conditions, without reading them, reaches 97 percent**." Once a person's given their consent, the data can easily flow out of apps, each second, into colossal predictive behavior companies databases like Google, Facebook, Oracle, Acxiom, Alibaba, etc. This data can then be used to predict their behavior and sold to others.

In Principle 14 of "**Revised Principles of Identity**" – it states:

> "Depending on risk, different levels of informed consent for releasing sections of a person's legal identity, biometric, behavioral and neuro-data should be used."

Today, this is a daydream. Thus, down at the practical level of implementing SOLICT/LSSI into this world, I have architected SOLICT to do a small baby step towards rethinking consent around the planet. SOLICT will record all consents relating to release of a person's legal identity and credential information, from cradle to grave.

I can see, over time, not overnight, consent contract agreements will become standardized. This will help reduce the identity friction and costs, especially as AI (artificial intelligence) leveraged PIAM (personal identity access management) come into being.

It requires a new toolkit. Skim these:

- "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"
- Kantara UMA (User Managed Access)

For example, as Jane Doe walks down a shopping mall, leveraging her LSSI devices and her PIAM, she'll be able to automatically create consent agreements on the fly between herself and third parties, which make their way into her SOLICT (skim "**An Identity Day in the Life of Jane Doe**" to see an example of this.

Finally, it becomes imperative that all citizens, regardless of their abilities or disabilities understand consent agreements releasing their legal identity and/or credential information. Co-design is critical in ensuring this is possible.

Consent Standards/Agreements/Contracts Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre section and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

SOLICT API (Application Programming Interface) Subcomponent Cost Centre:

Background:

The API is the front door to an entity's SOLICT. It will quickly become an attack target by the Evil Inc.'s and malicious states of the planet. Couple it with this curve. It hypothetically means, EACH HOUR, new attack vectors are being created against the legal identity framework, of which the SOLICT is a key part.

I have an underlying premise – only the largest countries and companies around the planet have the resources, expertise and budgets to continually defend against these new rapid attacks. The rest of us don't i.e., we'll be prone to repeatedly successful attacks against us, including our SOLICTS.

Which is why the new, global, independent, non-profit is part of the architecture. Its job is to do 24x7x365 threat analysis against the end-to-end legal identity architecture. It will produce rated threat assessments with jurisdictions, companies, enterprises, and entities being required to update in a pre-determined time. This is how to bring current industry best practices to the world of legal identity.

All of which comes to bear with the SOLICT, and APIs used to write, read and manage each entity's SOLICT.

SOLICT API Subcomponent Costs:

The costs will be borne by the Non-Profit Manages API Standards Cost Centre section of this document.

LSSI Devices Cost Centre

Background:

Today, on the planet, it's a legal identity mess proving an entity's identity. Skim "**Legal Identity Problem Statements**."

Today, we don't control our legal identities both physically and digitally. Instead, we rely on pieces of paper issued by a government (which are easily forged and frauded). There's no way for say Jane Doe to prove her smart, AI leveraged, digital identities which are legally registered against her physical legal identity.

Then there's people, like my 94-year-old mother, who no longer has mental faculties, or young or poor people with no access to tech or don't have the means to store pieces of paper. Then consider people with different communication abilities and/or disabilities? How can they easily prove their legal identities?

Add to this the legal identities of AI systems and bots. How can they prove their own legal identities?

Finally, how can an entity legally, anonymously prove they're a human or bot? Today, on the planet, this legal identity framework doesn't exist.

All the above was in my mind while creating the new legal self-sovereign identity (LSSI) architecture.

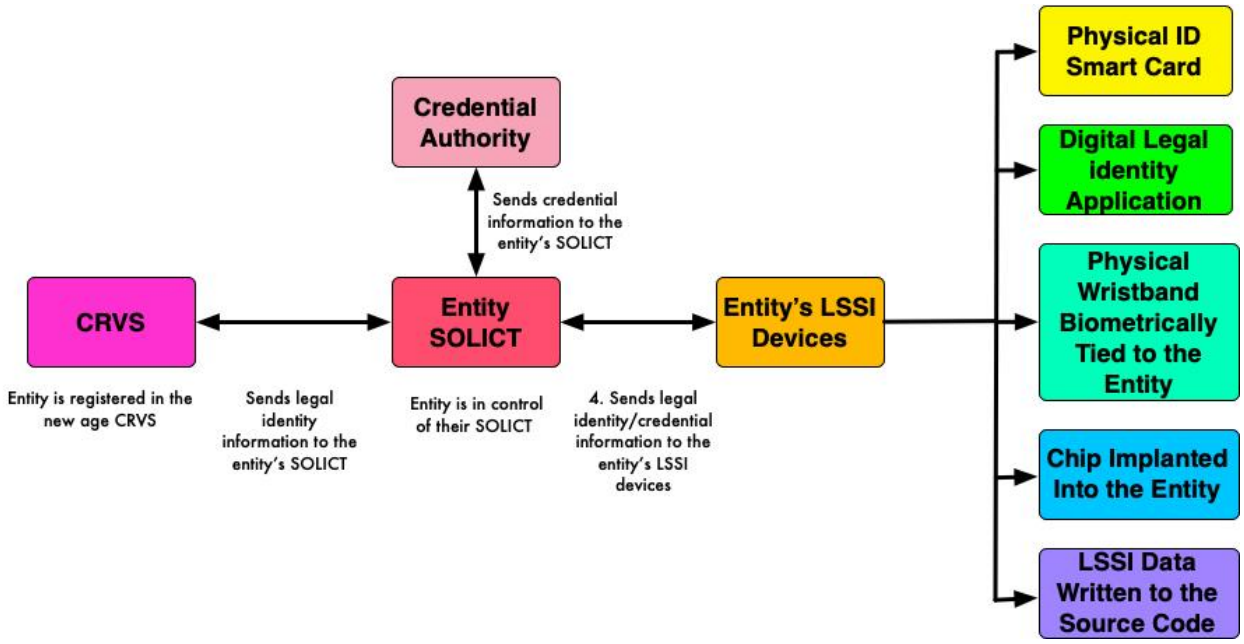
Vision:

There are five different types of LSSI devices:

- Physical, smart legal identity card
- Legal identity digital application
- Physical wristband, containing the legal identity/credential information, biometrically tied to the wearer
- A chip implanted into the entity
- Writing legal identity and credential information to the source code of an entity

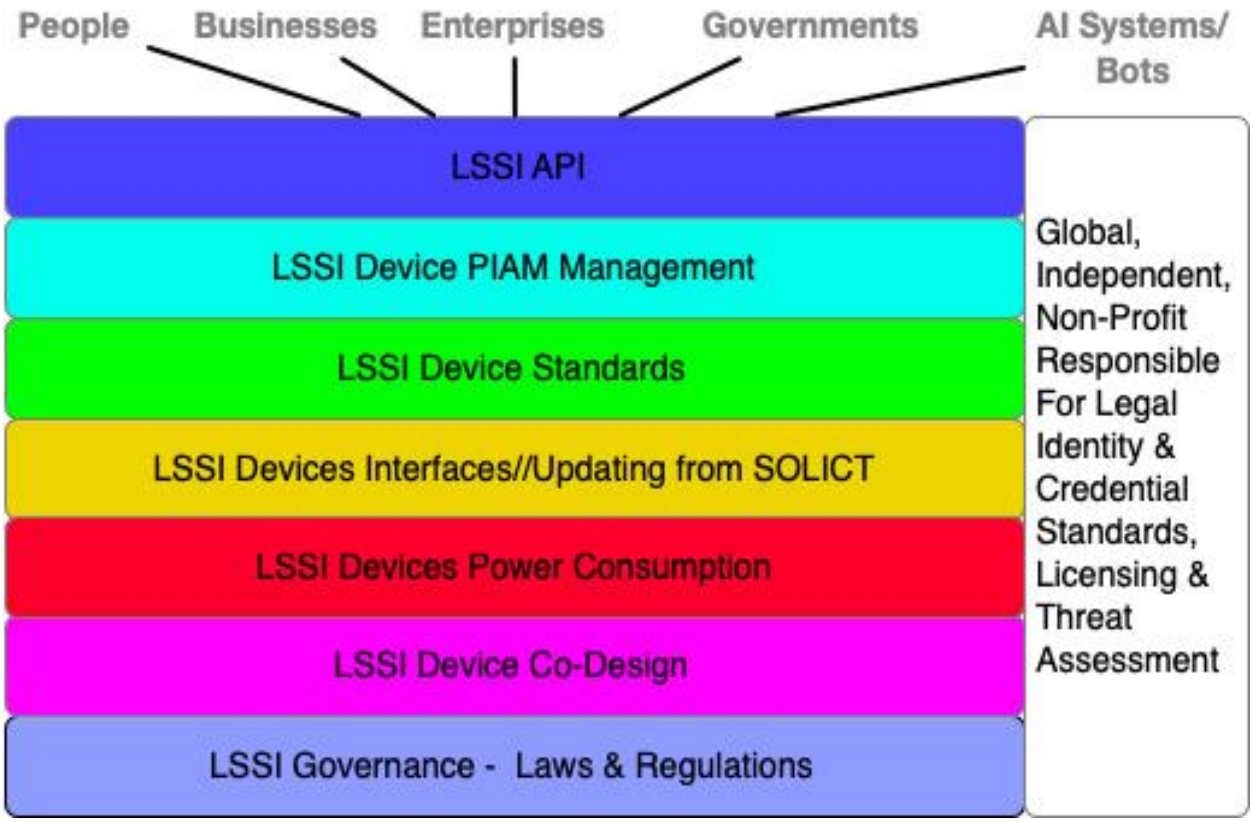
Thus, it meets the needs of all the above challenges. The source of truth for the LSSI device is the SOLICT. LSSI devices are fed their legal identity and credential data, from the SOLICT, via TODA files (skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" to understand TODA).

Here's a pic showing at the 100,000-foot level high level components:



To see a story about how a person leverages their LSSI/PIAM skim "**An Identity Day in the Life of Jane Doe**".

LSSI Cost Centre Subcomponents Diagram:



Other Cost Centres Dependent Upon These Cost Centres:

- AI/Bots TODA LSSI (Legal Self-Sovereign Identity) Subcomponent Cost Centre
- CRVS SOLICT Pushes Out Legal Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Cost Centre
- Credential Standards LSSI (Legal Self-Sovereign Identity) Subcomponent Cost Centre
- Legal Identity & Hive Relationships - SOLICT to LSSI (Legal Self Sovereign Identity) Devices Via TODA File Subcomponent Cost Centre
- SOLICT Pushes Out Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Cost Centre
- Rethinking Learning - LSSI (Legal Self-Sovereign Identity) Devices Cost Centre
- Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre
- Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Supply Subcomponent Cost Centre

LSSI Governance – Laws & Regulations Cost Subcomponent Cost Centre:

Background:

Each jurisdiction's identity assurance requirements, regulations and possibly acts will change with the introduction of SOLICT/LSSI. The same identity assurance requirements, regulations and possibly acts will also likely need to change addressing different levels of assurance for how a LSSI device is used to proof their identity.

The LSSI devices will also likely fall under several different regulatory bodies in each jurisdiction. This could be overwhelming at the start in addressing them.

As importantly is ensuring, by laws and regulations that all citizens, regardless of their abilities or disabilities, can understand and use their LSSI devices.

Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit – CRVS/Government Coordination/Advisory Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre

LSSI Governance – Laws & Regulations Subcomponent Costs:

Costs will be borne by the Non-Profit – CRVS/Government Coordination/Advisory Subcomponent Cost Centre

LSSI Device Co-Design Subcomponent Cost Centre:

Background:

As stated in the co-design vision section re criticality:

"As I see it, these architectures two most important, critical challenges are:

1. **Creating a continually secure architecture for registering digital entities at transactional speeds**
2. **Creating citizen interfaces, designed from the ground up, enabling them to understand and use their SOLICT, LSSI devices, PIAM, DLT, IEP and LDV easily and securely. Without this, the architectures won't work in the field.**

Thus, co-design is a mission critical component of the architecture.

LSSI devices are several interfaces a citizen can choose to use to release portions of their legal identity and credential information. Thus, it's where co-design hits the floor running. A citizen, regardless of their abilities or disabilities, needs to be able to:

- Understand what the LSSI devices are
- Determine what data they can choose to release
- Then make decisions on their own
- And have the LSSI devices, and/or their PIAM's, instantly, securely execute this

That's what this cost centre addresses.

LSSI Device Co-Design Subcomponent Costs:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

LSSI Devices Power Consumption Subcomponent Cost Centre:

Background:

The architecture gives each person on the planet their own LSSI devices to use i.e., there will be billions of them. Then all digital entities will also have their own LSSI devices i.e., potentially trillions of them. Many of these devices will be consuming power.

Thus, this is why I created this separate subcomponent power consumption cost centre to address it. Its goal is to stay on top of finding economical ways of creating low power consumption LSSI devices.

LSSI Device Interfaces/Updating from SOLICT Subcomponent Costs:

Costs will be borne by the Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre section of this document.

LSSI Device Interfaces/Updating from SOLICT

Background:

There are three main components of interfaces/updating LSSI devices from SOLICT:

- Business processes
- Technical processes
- SOLICT/LSSI interface

All of which create potential attack vectors.

The business processes must include but not be limited to:

- Consent from the user to update their LSSI devices (or via their PIAM)
- Consent records being created in the SOLICT
- Consent processes for each LSSI device to update from the SOLICT
- Delegated management of the above processes where another person is legally assigned to manage another's legal identity, and hence their SOLICT/LSSI e.g., parents, etc.
- Business processes when an update connection is lost mid-transmission
- Etc.

The technical processes must include but not be limited to:

- End-to-end security processes from the SOLICT to the LSSI device
- Digital signature type and encrypted secured connections from the SOLICT to the LSSI device
- Update processes from the database to the LSSI device
- Use of TODA capability files to transmit legal identity, hive relationships, legal authorization and credentials to ensure the SOLICT is only updating the LSSI device with X file on Y date at Z time
- Etc.

The SOLICT/LSSI interface must include but not be limited to:

- Creating a standard for the interface including:
    - Security standards
    - API interface standards
    - Etc.

LSSI Device Interfaces/Updating from SOLICT Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre and the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) section of this document.

LSSI Devices Standards Subcomponent Cost Centre :

Background:

There are five potential types of LSSI devices:

- Legal ID physical card
- Digital LSSI app
- Biometrically tied LSSI ID wristband
- Chips inserted into people containing their LSSI information
- LSSI information written to an entity's source code

On each of these devices will be stored TODA files or perhaps, the Toda file will be written to a small database on the device. THIS MUST BE DETERMINED IN THE DESIGN PROCESS.

This curve means that the Evil Inc.'s and malicious states will leverage it to create new attack vectors against the LSSI devices. Thus, the new, global, independent non-profit 24x7x365 threat analysis is required to constantly update the LSSI devices. All of which requires LSSI device standards with the ability to rapidly update/upgrade them.

This isn't a simple task, given the billions of people who will be using the LSSI devices. Thus, each LSSI device subcomponent cost centre must address this.

LSSI - Legal Physical ID Cards Subcomponent Costs:

Background:

In today's smart card world, there's a limit to the amount of data the card can hold. This might be limitations when wanting to write LSSI files to them. The challenge with LSSI, over time, not overnight, is the amount of data will likely increase as one has different credentials. Each LSSI entry will also likely require a digital signature issued by the local authority. Thus, consideration must be given to thinking of producing a very small, secure LSSI database on the card or, devising an alternate solution allowing for secure data scaling on the card, to common global LSSI standards.

The current legal ID cards typically have a face image and/or name type data on the front of them. It limits the ability of a person to prove they're a human legally, anonymously and/or above age of consent

There are limited abilities for a person to provide their consent. How will a person provide their consent? Can voice be used on physical cards? How will the card and third party know where to securely send the consent to the person's SOLICT URL address?

All of this applies to enabling people of all abilities and disabilities to understand:

- What their physical ID card is
- What personal legal identity and credential data they have
- Then make their own decision on what to release
- Having the LSSI physical ID card then be able to execute it instantly and securely

Then there's the issues of how legal identity delegation will occur for two people and their LSSI physical legal ID cards e.g., a parent and child. How will this work?

The rapid tech changes caused by this curve, mean that new attack vector is being rapidly created. Thus, the physical ID cards must be continually assessed by the global, non-profit with continuous threat assessments being issued.

Finally, practical things like a person acquiring a new credential, vaccination, changing them, etc. requires rapid update processes to the card.

All of these are design factors in implementing LSSI on to existing legal ID physical cards. It might require design teams to accept limitations in the short term to get rapid adoption or, to issue new legal ID cards to people having capabilities addressing the above. All these factors affect costs.

Legal Physical ID Cards Subcomponent Costs:

Costs will be borne in the Non-Profit LSSI Standards - Legal Physical ID Cards Subcomponent Costs and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

LSSI - Digital LSSI App Subcomponent Costs:

Background:

In today's world, there's some common standards for things like digital driver's licenses, passports et al. I can see a need for a Digital LSSI app, which applies to:

- Young children through to very old people i.e., cradle to grave
- Entity creation to termination

This app will allow for use of Toda LSSI file being written to it or, to a small LSSI database within the app, or connecting through to an entity's SOLICT.

Citizens, of all abilities and disabilities, MUST understand:

- What their digital LSSI app is
- What personal legal identity and credential data they have
- Then make their own decision on what to release
- Having the LSSI digital app then be able to execute it instantly and securely

Then there's the way the entity will grant consent to a third party to release their legal identity and credential data to. Hypothetically, in addition to typical consent buttons, for humans, different types of biometric and behavioral factors could be used to provide consent.

Then there's the issues of how legal identity delegation will occur for two people and their LSSI Digital LSSI apps e.g., a parent and child. How will this work? Each person's TODA capability LSSI files will need to be present on the devices with appropriate processes allowing say a parent to control their child's legal identity LSSI app.

The rapid tech changes caused by this curve - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf, mean that new attack vector are being rapidly created. Thus, the Digital LSSI app must be continually assessed by the global, non-profit with continuous threat assessments being issued.

Finally, practical things like a person acquiring a new credential, vaccination, changing them, etc. requires rapid update processes to the card. As well, changes caused by the curve might require digital LLSI app updating.

All of these are design factors in implementing LSSI on to existing digital legal identity apps. It might require design teams to accept limitations in the short term to get rapid adoption or, to issue new legal identity LSSI apps to people having capabilities addressing the above. All these factors affect costs.

Digital LSSI App Subcomponent Costs:

Costs will be borne by the Non-Profit LSSI Standards - Digital LSSI App Subcomponent Costs and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

LSSI - Biometrically Tied LSSI ID Wristband Subcomponent Costs:

Background:

Billions of people around the planet don't have access to tech or, are unable to use it. They all require LSSIT capabilities to use in their life. The requirements are it must be:

- Made of a durable material able to withstand lots of physical abuse
- Able to function after being dropped in dirt, mud, urine and feces
- Washable by hand or machine
- Able to function in hot, cold, dry, or wet environments
- Biometrically linked to the wearer
- Color differentiated allowing people to recognize which is their wristband
- Updateable via some form of wireless API
- Have enough memory to contain legal identity and credential data
- Low cost
- **And most importantly have each citizen, regardless of their abilities or disabilities, to understand:**
    - **What the biometrically tied LSSI bracelet is**
    - **How they can use it (taking into account their disabilities)**
    - **Allowing them to make their own choice on who to release portions of their legal identity and credential data to**
    - **With the bracelet able to execute it quickly and securely**

Biometrically Tied LSSI ID Wristband Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

LSSI - Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs:

Background:

The speed of this curve, means the technology is rapidly evolving resulting in creation of the hypothetical possibility of inserting chips into people containing their TODA LSSI file. This concept is typically met in older people with disdain, fear, and mistrust, while younger people are more open to it. Scientific, legal and privacy research is required for this. Additionally, all people, regardless of their abilities or disabilities MUST be involved in design and testing i.e., strong use of co-design.

Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

LSSI - Writing LSSI Information to an Entity's Source Code Subcomponent Costs:

Background:

The explosion of AI systems, bots and AI leveraged, smart digital identities of humans require the ability to write LSSI information to the source code. This is the same challenge facing CRVS design of writing legal identity information to the entity's source code.

LSSI - Writing LSSI Information to an Entity's Source Code Subcomponent Costs:

This cost centre will likely be borne by the AI/Bots Writing to Source Code Legal Identity/Credential Registration Subcomponent Costs section of this document.

LSSI Device PIAM Management Subcomponent Cost Centre:

Background:

The LSSI (legal self-sovereign identity) vision includes creation of an AI leveraged "Personal Identity Access Management" (PIAM), to manage a person's consents. Skim "**An Identity Day in the Life of Jane Doe**", to see an example of this.

Thus, the PIAM of an entity will be interacting with the entity's SOLICT/LSSI. It begs the question of how access rights of an entity to this will be done? It also begs another question about this becoming yet another attack vector and how we're going to mitigate risk?

Finally, all people, regardless of their abilities or disabilities, MUST be able to understand:

- **What their PIAM is**
- **How it interacts with their LSSI devices**
- **How they can use it**
- **Allowing them to make decisions on how to configure their PIAM**
- **With the PIAM able to execute on their behalf instantly and securely**

This is where co-design plays a mission critical role.

LSSI Device PIAM Management Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre, the Cost Centre - PIAM (Personal Identity Access Management) System and the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre section of this document.

LSSI Device API Subcomponent Cost Centre:

Background:

Similar to SOLICT API's, the LSSI API is effectively the "electronic front door" to accessing LSSI device-based data. The API must be to a global protocol, clearly explaining how entities, browsers, apps, PIAM's, smart digital identities of us, and people who have consent privileges to manage our legal identity, will be able to securely access SOLICT data with our consent.

There's this curve to consider. -It means it's highly likely, over time, LSSI API requirements will change, sometimes quite quickly, as it becomes a prime security attack point. In addition to designing a secure API interface, thought must also be given to addressing potential attack vectors like a denial-of-service attack on the LSSI endpoints if available online. This effectively shutting down an entity's ability to digitally function in today's digital world i.e. digital death (skim this article where I discuss digital death, "**Death & Digital Identity**").

Taking all the above into consideration, very careful thought needs to be given in the early days of design, ensuring the API is secure, and can perform well. So, what are the associated costs with getting the LSSI API up, going and maintained over time? That's what this cost centre must dive into.

LSSI Device API Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost Centre and the Cost Centre: API (Application Programming Interface) section of this document.

Cost Centre - PIAM (Personal Identity Access Management) System

Background:

Imagine Jane Doe walking down a street, wearing AI/AR glasses, where she's both in the online and offline world simultaneously. She'll likely be bombarded by requests for her to share her identity. She's not going to want to have to manually do this. That's why I created the concept of a PIAM.

It leverages AI for Jane to then pre-determine who she wants to share her legal identity and credential information to. If you skim, "**An Identity Day in the Life of Jane Doe**" you'll see how Jane's PIAM allows her to mostly live privately except with those third parties she wants to share her information with.

Now making this vision become a reality requires security standards, since the PIAM will become a prime point of attack by criminals. Further, given this curve, it means today's best security standards can quickly become tomorrow's turd. Which is why the architecture calls out for PIAM standards to be managed by the global, independent non-profit, which also does 24x7x365 threat analysis against it. Thus, the architecture is designed to constantly keep the PIAM secure.

A person will use their PIAM to control their smart digital identities as well as any AI systems/bots they have a contractual relationship with. Then there's the large challenge of enabling citizens of the planet, regardless of their abilities or disabilities, being able to:

- **Understand what their PIAM is**
- **Understand what portions of their legal identity & credentials to release**
- **Then make the choice on their own**
- **With the PIAM/LSSI devices able to instantly, securely execute it**

This is where co-design in mission critical.

Yes, it's complex, which is why the PIAM cost centres start out with a series of small, rapid POC's and pilots to work our way through the many challenges in designing, implementing and maintain PIAMs.

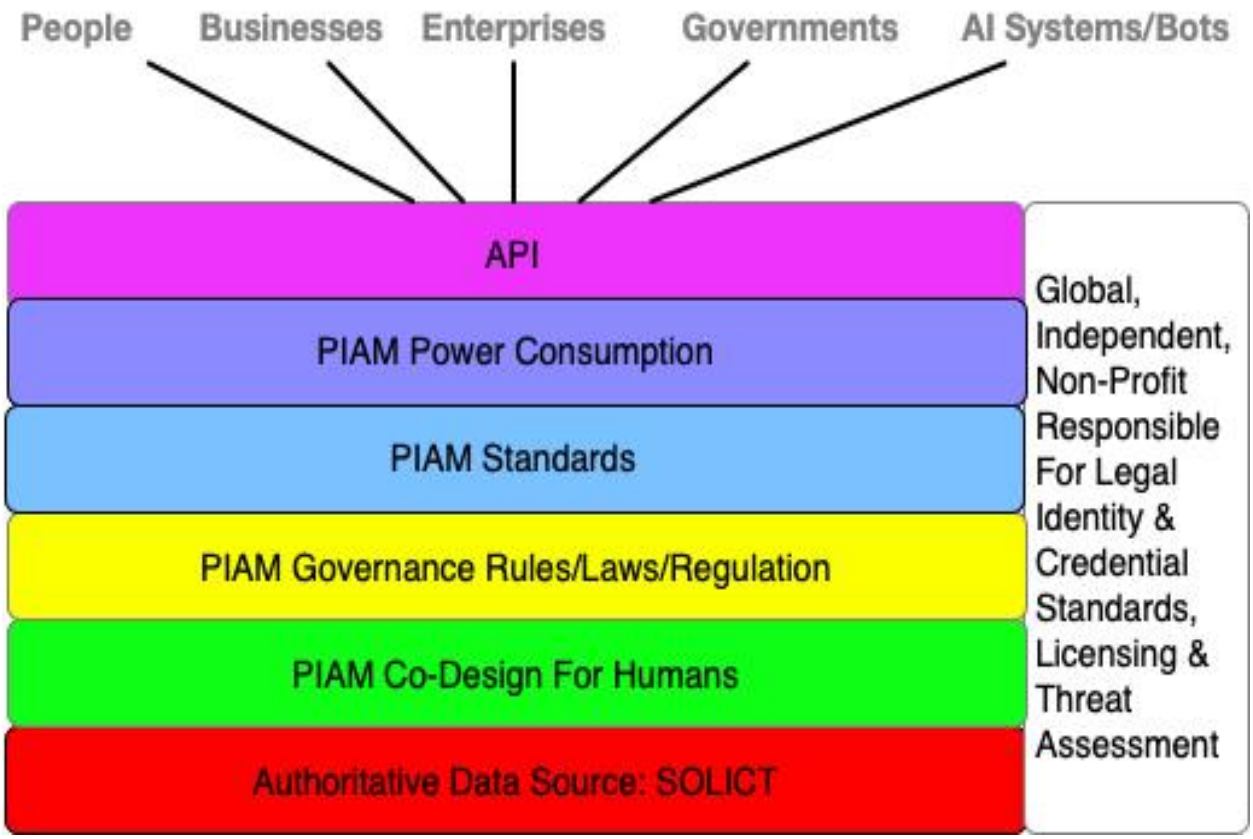
Finally, I can easily see where companies will want to produce PIAMS. Why? It puts them closest to their customer. My goal in creating the architecture is to create PIAM standards:

- Protecting a person's PIAM regardless of who provides it
- Allowing companies to innovate, leveraging AI, and rapidly feeding this back into PIAM standard changes

Note:

1. **I'M NOT AN AI EXPERT.** Thus, what follows are only my best guesses at architecture and potential cost components.
2. Readers should review the PIAM Vision section of this document see numerous examples of how the PIAM works.

PIAM Architecture Subcomponents Costs Diagram:



Other Cost Centres Dependent Upon These Cost Centres:

- AI/Bots PIAM (Personal Identity Access Management) Subcomponent Cost Centre
- CRVS - PIAM Manages Legal Authorization Rights With Other Entities Subcomponent Cost Centre
- Credential Standards PIAM (Personal Identity Access Management) Subcomponent Cost Centre
- Legal Identity & Hive Relationships - PIAM (Personal Identity Access Management) Consent Agreements/Contracts With Third Parties Subcomponent Cost Centre
- Legal Authorization Rights - PIAM Manages Authorization Rights With Other Entities Subcomponent Cost Centre
- LSSI Device PIAM Management Subcomponent Cost Centre
- Rethinking Learning - PIAM (Personal Identity Access Management) Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre
- Non-Profit – Manages PIAM Standards Subcomponent Cost Centre

PIAM –Authoritative Data Source SOLICT Subcomponent Cost Centre:

Background:

The SOLICT is the source of truth for the PIAM. The SOLICT gets its authoritative data from:

- CRVS
  - Entity legal identity data
  - Entity digital signature
  - Entity legal identity hive relationships
  - Entity authorization rights
- Credential Authorities
  - Credentials issued to the entity
- Consent agreements from third parties

PIAM Authoritative Source SOLICT Subcomponent Costs:

The costs associated with:

- Legal entities will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre section of this document
- Credential issuance standards will be borne by the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document
- Consent standards will be determined by the Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre section of this document

PIAM Co-Design For Humans Subcomponent Costs:

Background:

As stated in prior sections a citizen needs to be able to:

- Understand what their PIAM is
- Understand what portions of their legal identity & credentials to release
- Then make the choice on their own
- With the PIAM/LSSI devices able to instantly, securely execute it

This is where co-design in mission critical.

PIAM Co-Design For Human Subcomponent Costs:

Costs will be borne by the Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre.

PIAM Governance Rules/Laws/Regulation Subcomponent Costs:

Background:

An entity, be they human, AI system or bot, will have a bewildering number of interactions, each day, with all sorts of different entities. Thus, their PIAM will likely need to make hundreds of consent decision request to the entities, either reusing them or agreeing. This in turn will then require smart AI leveraged contracts to be created, stored in the entity's SOLICT, resulting in the entity releasing legal identity, relationships, authorization, or credential data to the entity.

Then consider delegation abilities. Look at this diagram to see the PIAM decisions for John Doe, son of Jane Doe as an example who uses his AssistBot at school. Even more complicated look at this diagram indicating legal hive entity relationships which the PIAM must manage on behalf of, and at the direction of, its entity.

I strongly suspect, when PIAM's appear, companies will want to leverage the heck out of it. Why? It's the decision front door to an entity. Thus, they'll want to do increasingly complex things with it.

All of which will increase, faster and faster, due to this curve. Skim "**Underpinnings of a Global, Decentralized ONDC (Open Network for Digital Commerce)" https://hvl.net/pdf/GlobalDecentralizedONDCFinal.pdf or PowerPoint version https://hvl.net/pdf/GlobalDecentralizedONDCFinal.pptx.** Thus, it requires not only standards, but ability to rapidly change them due to the curve.

Then factor in increasing rapid new attack vectors against the PIAM and the entity's API. This requires the new, global, independent, well-funded non-profit to do 24x7x365 threat analysis against the API, PIAM, LSSI, SOLICT and feeds from the authoritative sources.

I can also see Denial of Service type attacks against an entity via its PIAM by making thousands or more requests per second. This too must be addressed in the PIAM security design.

All of which comes down to governance of the PIAM with new laws and regulations. Here's the challenge with new laws and regulations. Today, they can't be enforced outside of jurisdiction (e.g., the pathetic cybercrime prosecution success rate of 0.05%). Thus, as mentioned throughout this document, it likely requires changes to trade agreements allowing cross-jurisdictional prosecution.

All I can in my head is this massive wall of change coming at us, with the PIAM at the front, making decisions on our behalf. It will become like the "wild west" with different groups wanting to do different things with it, very quickly.

PIAM Governance Rule/Laws/Regulations Subcomponent Costs:

Costs will be borne by the Non-Profit – CRVS/Government Coordination/Advisory Subcomponent Cost Centre section of this document.

PIAM Standards Subcomponent Cost Centre:

Background:

Skim "**An Identity Day in the Life of Jane Doe**". It shows Jane leveraging her PIAM and LSSI devices to do a wide variety of different tasks for her together with several AI leveraged, smart digital identities.

Then consider the rise of neural biometrics and use of our brains to control things. Skim "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**" to see what's coming at us re brainwaves. Watch minute 19:30 of the "The AI Dilemma" it shows how AI can read our brainwaves. Thus, in the not-so-distant future, the PIAM will likely be controlled by us thinking commands, via AI, with the PIAM automatically doing them regarding release of our data.

This is the world the PIAM will operate in i.e., fast changing, legal contracts and complex decision making, interacting with third parties.

All of which begs the question "How will this work?" Answer – use of different forms of AI, which will likely rapidly change due to the effects of this curve. That's what this subcomponent cost centre addresses.

Of all the components of the human, AI system and bots, learning architecture, I feel the PIAM will become the most publicly focussed one, always in the press, with lots of vendor and political pressure.

Down in the technical weeds, it will likely leverage natural language understanding, speech to text and neural interfaces, visual recognition, machine learning, etc. ALL OF WHICH I'M NOT AN EXPERT IN AND WHAT CO-DESIGN IS ALL ABOUT.

Consider the current crappy consent laws around the planet. Skim this old paper "**Consent Principles in the Tsunami Age**". It suggests creating zones of consent. Here's the main point – the PIAM will be the manager of the consent agreements and prompt Jane or John Doe, when the consent agreements require it, to affirm their consent in clear terms. It thus becomes a prime conversation regarding privacy.

Given the fast pace of change from this tech change curve, the PIAM requires a very flexible standards body, able to make changes in increasingly short-time frames.

All the above is what this cost centre delivers.

PIAM Standards Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre section of this document.

PIAM Power Consumption Subcomponent Cost Centre:

Background:

Look at Figure 1 in "**AI Power Consumption Exploding**". It shows, if current AI power consumption trends continue, by 2040-ish AI will be consuming most of the planet's power. Of course, this is untenable. Yet, sadly, it's not on most peoples' and policy makers radar screens.

It's on mine. Why? The architecture gives each person on the planet their own PIAM which is Ai leveraged. Thus, there will literally be billions of these on the planet. Thus, I've broken out this separate subcomponent cost centre to focus on this.

Its job is to innovate, coming up with low energy cost AI versions. A potential way might be decentralized AI. Skim "**Decentralized AI – Risks, Legal Identity, Consent & Privacy**".
.

PIAM Power Consumption Subcomponent Costs:

Costs will be borne by the Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre section of this document.

PIAM API Subcomponent Cost Centre:

Background:

The PIAM will leverage the SOLICT/LSSI API's. It might or might not require development of its own API.

PIAM API Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost Centre and the Cost Centre: API (Application Programming Interface) section of this document.

Cost Centre: API (Application Programming Interface)

Background:

A major performance and security question is how to securely access:

- CRVS entity legal identification, identity/hive relationships and authorization data?
- Credential issuance data?
- Sending the above data to the SOLICT?
- SOLICT communicating with the LSSI devices?
- PIAM managing the LSSI devices?
- Third party consent agreements sent to the SOLICT?

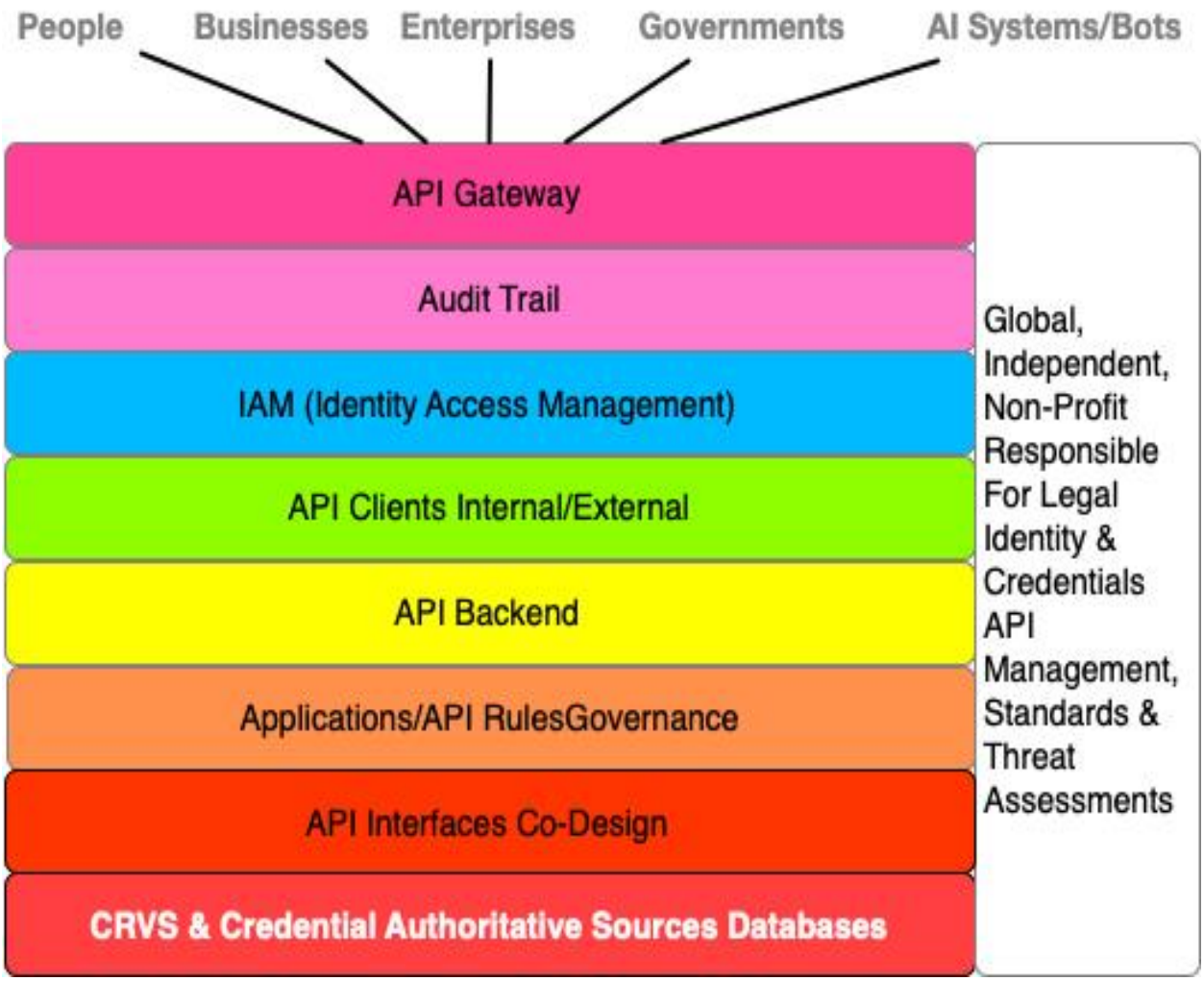
Answer - Create standard API's (Application Programming Interface).

It addresses the problems of how to query billions of us with AI leveraged, smart digital identities and trillions of AI systems and bots for their legal identities and/or for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed.

Add to the above complexity the rapid attack new attack vectors being created against the legal identity framework from this curve. The API is the electronic front door. Which is why the architecture has the new, global, independent, well-funded, non-profit. One of its tasks is to do 24x7x365 threat analysis and produce rated threats and threat responses. Thus, the API's created will likely be very frequently updated.

I'M NOT AN API EXPERT. Thus, what follows is only my best guess at the API cost centres. I'm sure API experts will likely change them.

API Subcomponent Cost Centres Diagram:



Other Cost Centres Dependent Upon These Cost Centres:

- AI System/Bots API Subcomponent Cost Centre
- Credential Standards API (Application Programming Interface) Subcomponent Cost Centre
- Legal Identity & Hive Relationships API (Application Programming Interface) Subcomponent Cost Centre
- LSSI Device API Subcomponent Cost Centre
- PIAM API Subcomponent Cost Centre
- Notary – API Subcomponent Cost Centre
- Rethinking Learning - Identity API (Application Programming Interface) Cost Centre
- Non-Profit – Co-Design API Interfaces Subcomponent Costs

API - CRVS & Credential Authoritative Sources Databases Subcomponent Cost Centre:

Background:

The CRVS system in this architecture will become standardized. Thus, from the perspective of creating standardized API's, it can be used with all CRVS systems. So, the API can begin with the underlying CRVS database (which may or may not be graph based).

THE SAME CANNOT BE SAID FOR AUTHORITATIVE CREDENTIAL SOURCES.
There are literally likely tens of thousands of such bodies on the planet today. Thus, the API architecture administered by the new, global, independent, well-funded non-profit will likely only apply to the credential issuance interface.

HOWEVER, having said this, the non-profit can issue best practices to the credential bodies, starting with the databases. This can be continually updated.

It's possible to use a data API gateway to access CRVS data stored within the database. Hypothetically, it might enable application developers to focus on writing business services that access data via easy-to-use APIs instead of having to learn the intricacies of a database query language.

All of this must be measured against security and performance. The number of writes/per second to the database might be awe inspiring given the rate at which an AI system can create digital bots, if they require legal identity registration.

API - CRVS & Credential Authoritative Sources Databases Subcomponent Costs:

Costs will be borne by the Non-Profit – API Subcomponent Cost Centre section of this document.

API- Interfaces Co-Design Subcomponent Cost Centre:

Background:

The legal identity, credential and notary architecture is built around ensuring all citizens, regardless of their abilities or disabilities can leverage their SOLICT, LSSI devices, PIAM, credentials and interact with a notary regarding these. Thus, any API interface pertaining to citizens, must be designed and tested allowing all citizens to interact with the above. That's what this cost centre delivers.

Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit – Co-Design API Interfaces Subcomponent Costs

API- Interfaces Co-Design Subcomponent Cost:

Costs will likely be borne by the **Non-Profit – Co-Design API Interfaces Subcomponent Costs** section of this document.

API – Applications/API Rules/Governance Subcomponent Cost Centre:

Background:

These are the following applications APIs should be designed for:

- CRVS
- SOLICT
- LSSI
- PIAM
- Credential authorities issuing interface
- Consent standards via:
    - TODA – skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"
    - Kantara UMA – skim Kantara UMA Working Group

API – Applications/API Rules/Governance Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Costs section of this document.

API - Backend Subcomponent Cost Centre:

Background:

The API calls will likely be translated into actions leveraging tech like Enterprise Service Bus (ESB), a database, another cloud service, a microservice, application, or web server. Thus, these must be specified, designed for, tested and kept up to date from a security perspective.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS API - Backend Subcomponent Cost Centre

API - Backend Subcomponent Costs:

Costs will be borne by the Non-Profit – API Subcomponent Cost Centre section of this document.

API – Clients Internal/External Subcomponent Cost Centre:

Background:

The client is a set of development tools to test and debug API's. These need to be carefully selected and use for internal and external clients.

Other Cost Centres Dependent Upon This Cost Centre:

Costs will be borne by the Non-Profit – API Subcomponent Cost Centre section of this document.

API – IAM (Identity Access Management) Subcomponent Cost Centre:

Background:

When IAM came into being in the late 90's, it was built on authoritative identity sources feeding an LDAP (Lightweight Directory Access Protocol) on top of which the IAM system functioned. This model isn't going to work well anymore. Why?

Fast changing legal identity entity relationships. As explained throughout this document, hive relationships can be one to one, one to many, and many to many with fast changing relationships. LDAP is a poor choice for this, while graphs are likely much better.

Then there's the speed at which new entities can be created. An AI system, in one jurisdiction, can create digital bots at speeds of thousands to millions per second, which in the next second can be operating in all other jurisdictions on the planet. If these require registration showing hive relationships, then I'm not sure if graphs can work at such speeds.

Add to this the ability to confirm a CRVS legal identity entity data transfer occurred on X date, at Y time, containing a file Z, at transactional speeds. This requires use of TODA which isn't used today in IAM systems.

For information on graphs and TODA skim, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

Then there's the arrival of PIAM (Personal Identity Access Management) systems. This creates a very decentralized IM system. As noted in the PIAM Cost Centre section of this doc, it will likely become a very fast-moving standard, with lots of changes.

Finally, add to this the security effects of this curve. That's where the new, global, independent non-profit comes into play with 24x7x365 threat analysis against end-to-end legal identity framework.

My point? OUR OLD IAM ARCHITECTURE ISN'T GOING TO WORK. DESIGNERS TAKE NOTE.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS API – IAM (Identity Access Management) Subcomponent Cost Centre

API – IAM (Identity Access Management) Subcomponent Costs:

Costs will be borne by the Non-Profit – API Subcomponent Cost Centre section of this document.

API – Audit Trail Subcomponent Cost Centre:

Background:

The audit trail is an essential component to the security and legal functioning of the:

- CRVS
- SOLICT, LSSI and PIAM
- Credential authority's issuance
- Consent agreements stored within the entity's SOLICT

TODA is a critical part of this because it can confirm on X date, at Y time, a file Z, was sent between two endpoints. Skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

A SECURE AUDIT API MUST BE DESIGNED AND IMPLEMENTED ALLOWING ADMINISTRATORS FAST ACCESS TO THE AUDIT LOGS/APPLICATIONS.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS API – Audit Trail Subcomponent Cost Centre

API – Audit Trail Subcomponent Costs:

Costs will be borne by the Non-Profit – API Subcomponent Cost Centre section of this document.

API – API Gateway Subcomponent Cost Centre:

Background:

The gateway provides the visible URL for an API, applies rules for use of the API, and then directs the API call to the back-end implementation. Rules can cover actions such as:

- Authentication and authorization
- Certificate management, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) termination and Mutual TLS
- Rate limiting and throttling
- Payload inspection (including payload size and the means to validate that the payload is structurally correct)
- Intelligent routing (routing based on the header or payload content)
- As importantly, from a security perspective, is the endpoint configuration, DNS standards, encryption, etc. to which API rules must be designed for

Other Cost Centres Dependent Upon This Cost Centre

- CRVS API – API Gateway Subcomponent Cost Centre

API – API Gateway Subcomponent Costs:

Costs will be borne by the Non-Profit – API Subcomponent Cost Centre section of this document.

Cost Centre: Rethought Notaries

Background:

One of the main functions of a notary is identifying the person appearing before the notary by reference to significant proofs of identity including passport, driving license, etc. In the old days, this worked because it was hard to fraud identities. The planet has changed.

I was the identity architect for a government's digital citizen identity and authentication project. I met with their security auditors. They told me they were the first jurisdiction in North America to use facial recognition on driver's licenses and now, many years later, it wasn't working so well. Why? Criminals were traveling across the country using fake birth certificates and wearing face masks. They'd successfully obtain driver's licenses, health care cards and then move up the identity food chain obtaining passports. I've heard, off the record, there are some jurisdictions with a hundred thousand of more fake identities.

So, when a person claiming to be Jane Doe shows up at a notary office, presenting her driver's license and passport, all of which seem to be legitimate, underneath the identity is Malicious Molly, who's masquerading as Jane Doe. My point? The planet's changed and so too must our legal identity framework, including notaries.

I like the concept of notaries, since they're independent of government, acting as a go-between between governments and citizens in proving their legal identities. Thus, I've included rethought notaries in the architecture.

The place to start is by rethinking how they verify entities identities. In today's planet, this can be very challenging, since a person, their smart digital version of them, or an AI system or bot, might be interacting digitally with a local notary, from the other side of the planet.

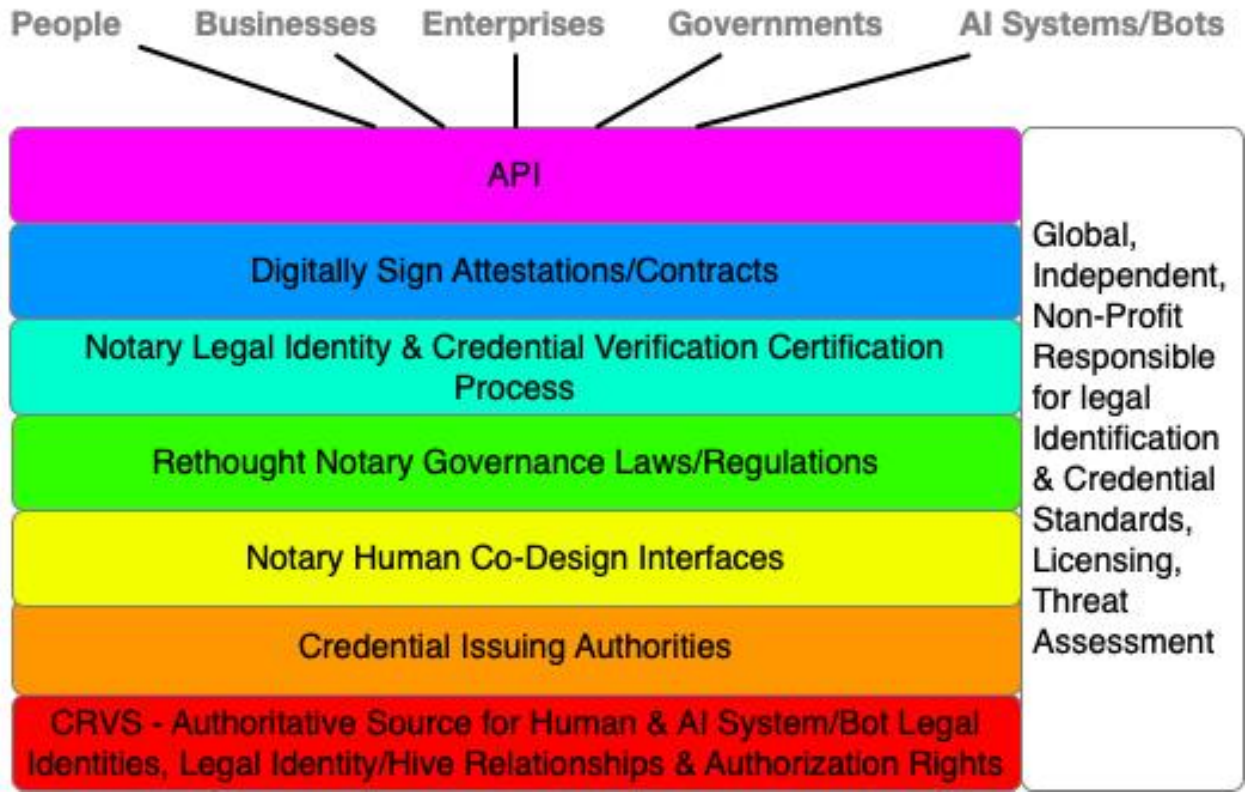
Another challenge is Jane Doe fleeing Jurisdiction X to Jurisdiction Y because the government deleted her CRVS record and any other government identity database of her. I could see Jane going to a local notary in Jurisdiction Y and, with her consent, giving her legal identity information plus her forensic biometrics, and the notary able to do a single search on the CRVS system to prove she's Jane Doe. When the search turns negative, the notary can search her SOLICT to see a special digital signature the CRVS signed when creating her SOLICT entry. They'd be able to decrypt it this confirming it's Jane Doe. They could then create a physical and digital attestation she's Jane.

Yet another challenge with notaries is their being able to work with citizens of all abilities and disabilities. Thus, I could see co-design assisting notaries in their work with all citizens re legal identity and credential proofing.

As with the rest of this architecture, it's visionary. I don't want to try to sell the planet on what a wonderful idea it is. Instead, my strategy is to find innovative funders, with 1-3 jurisdictions, with a willing business and notary community, to rethink notaries in small steps. That's what the cost centres call out for. Then, once we've figured it out in real life, rapidly scale.

I'M NOT A NOTARY EXPERT. Thus, what follows is only my best guess at beginning to rethink them. They are legal independent entities creating an independent balance between the role of government, its citizens, business and legal identities and signatures. So, having said this, here are my first guesses at rethinking them…

Rethought Notaries Subcomponent Cost Centres Diagram:



Note:

1. **I'M NOT A NOTARY EXPERT. So, the cost centres below might be substantially changed by the design team.**
2. **I've created, within the legal identity non-profit, a separate subcomponent cost centre devoted to notaries. Dependent upon the agreement of the funding countries notaries and their local state/provincial bodies overseeing notaries, the non-profit would likely:**
    a. **Oversee notary digital signature standards and threat assessments**
    b. **Oversee notary functions able to query CRVS, SOLICT interfaces**
    c. **Co-design functions for interacting with people re legal identity/credentials**
    d. **As well as continually doing threat analysis against the notary/CRVS/SOLICT interfaces and issuing rated threats**

Other Cost Centres Dependent Upon These Cost Centres:

- "Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre"
- "Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre"
- "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre"
- "Non-Profit - Manages Notary Standards For Legal Identity & Credentials Subcomponent Costs"
- Non-Profit – API Rule Sets Subcomponent Cost Centre
- Cost Centre: API (Application Programming Interface)

Notaries - CRVS - Authoritative Source for Human & AI System/Bot Legal Identities, Legal Identity/Hive Relationships & Authorization Rights) Subcomponent Costs:

Background:

The first place to begin rethinking them is with their independent verification of an entity's legal identity. With arrival of AI leveraged, smart digital identities of humans coupled with AI systems and bots, one can easily see contracts being created, requiring notarization, where the entity's identity mentioned within the contract need to be legally verified or, in the future, where one of more parties signing the contract might be an AI type entity. The contract might be an AI leveraged smart contract the notary notarizes.

I like the idea of a rethought notary who can play the role of an independent entity with the ability to:

- Collect an entity's legal identity information, plus for humans their forensic biometrics, and ask the entity to input their secret
- Compare the calculated value of the human's forensic biometric values, or the legal entity's data to the one from their LSSI device, and then do a double check against the CRVS system

Thus, there's a high degree of identity assurance it's who the person claims to be. This works anywhere on the planet. Government doesn't have to be involved. When the entity digitally signs a document, the notary has a high degree of assurance it's them. The notary can then use their own digital signature to also sign an identity verification e-document digitally (note this might be an AI leveraged, smart contract between the notary, the entity and a third party the entity wants to enter a contract with).

Note: The notary's legal identity plus their legal credential as a notary can easily be proven to the parties working with the notary, via the notary's own LSSI.

Notaries should be part of the design and implementation parts of the entire legal identity architecture cost centre document, since they will become parts of the legal identity verification framework for humans, AI systems and bots. That's why I've included them in the teams.

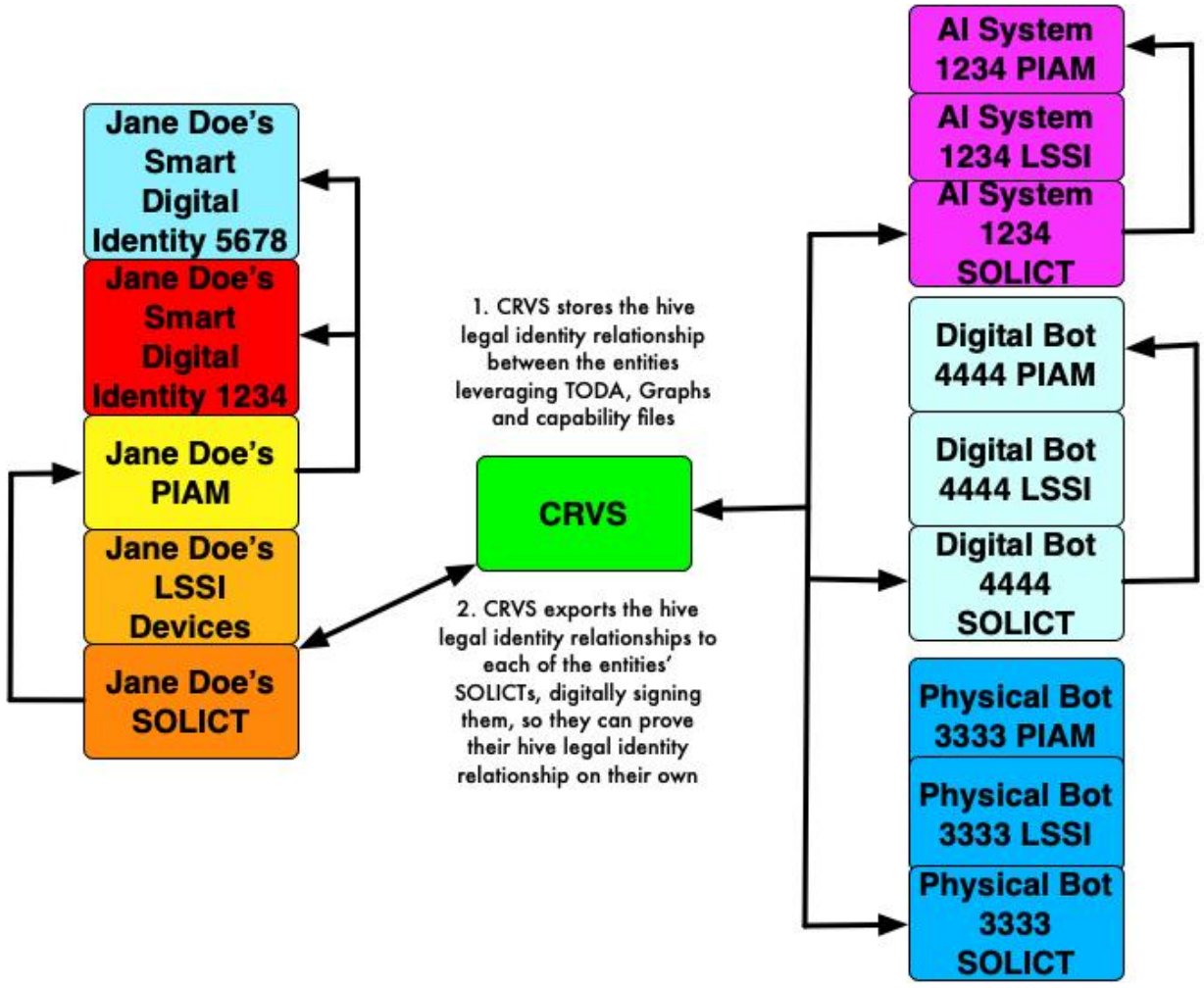
Notary- CRVS Authoritative Source for Human & AI System/Bot Legal Identities, Legal Identity/Hive Relationships & Authorization Rights) Subcomponent Costs:

Costs will be borne by the "Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre" section of this document.

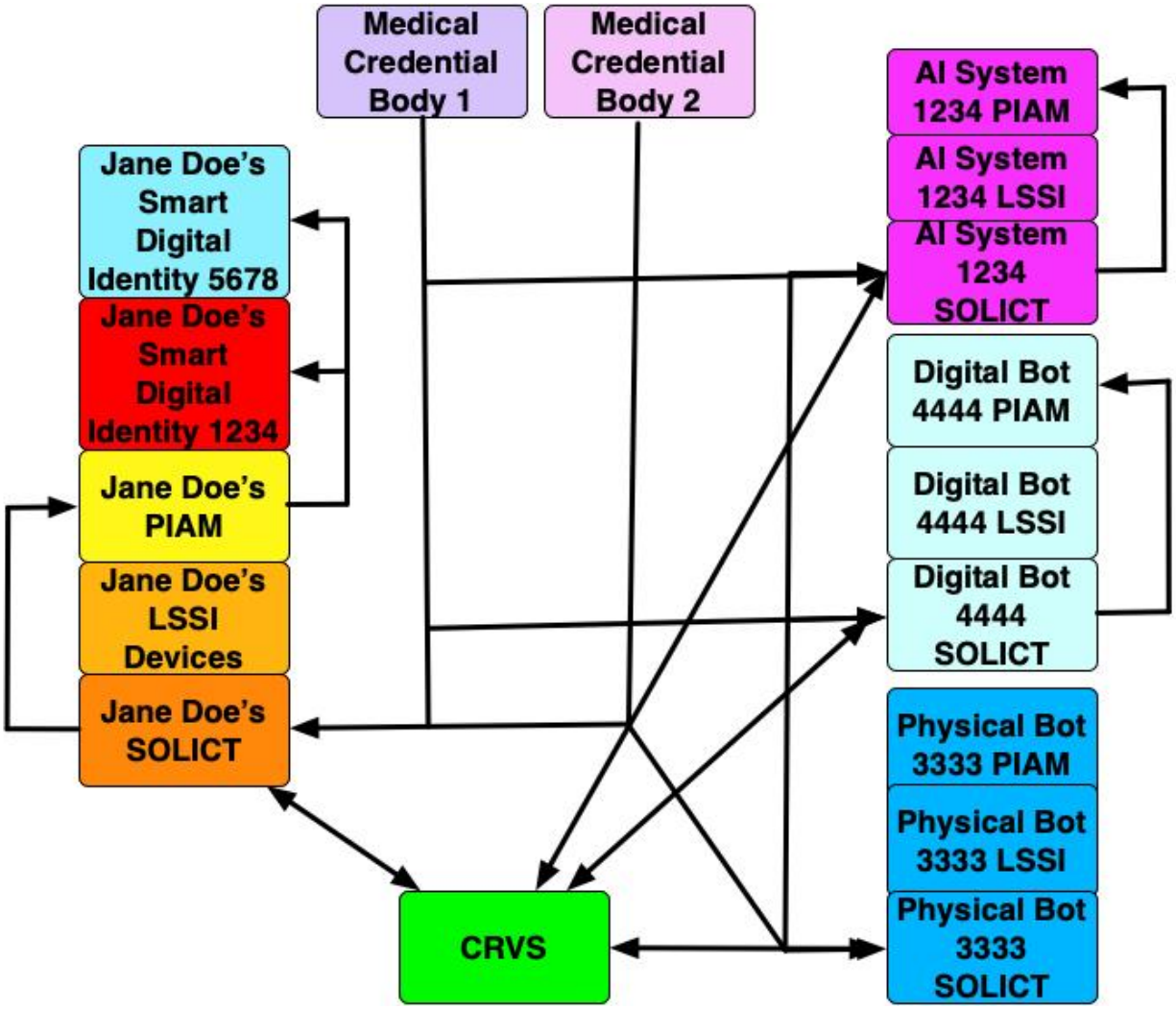
Notaries – Credential Issuing Authorities Subcomponent Costs:

Background:

I can see a rethought notary verifying an entity's credentials. Let's hypothetically use this diagram as an example of a hive relationship:



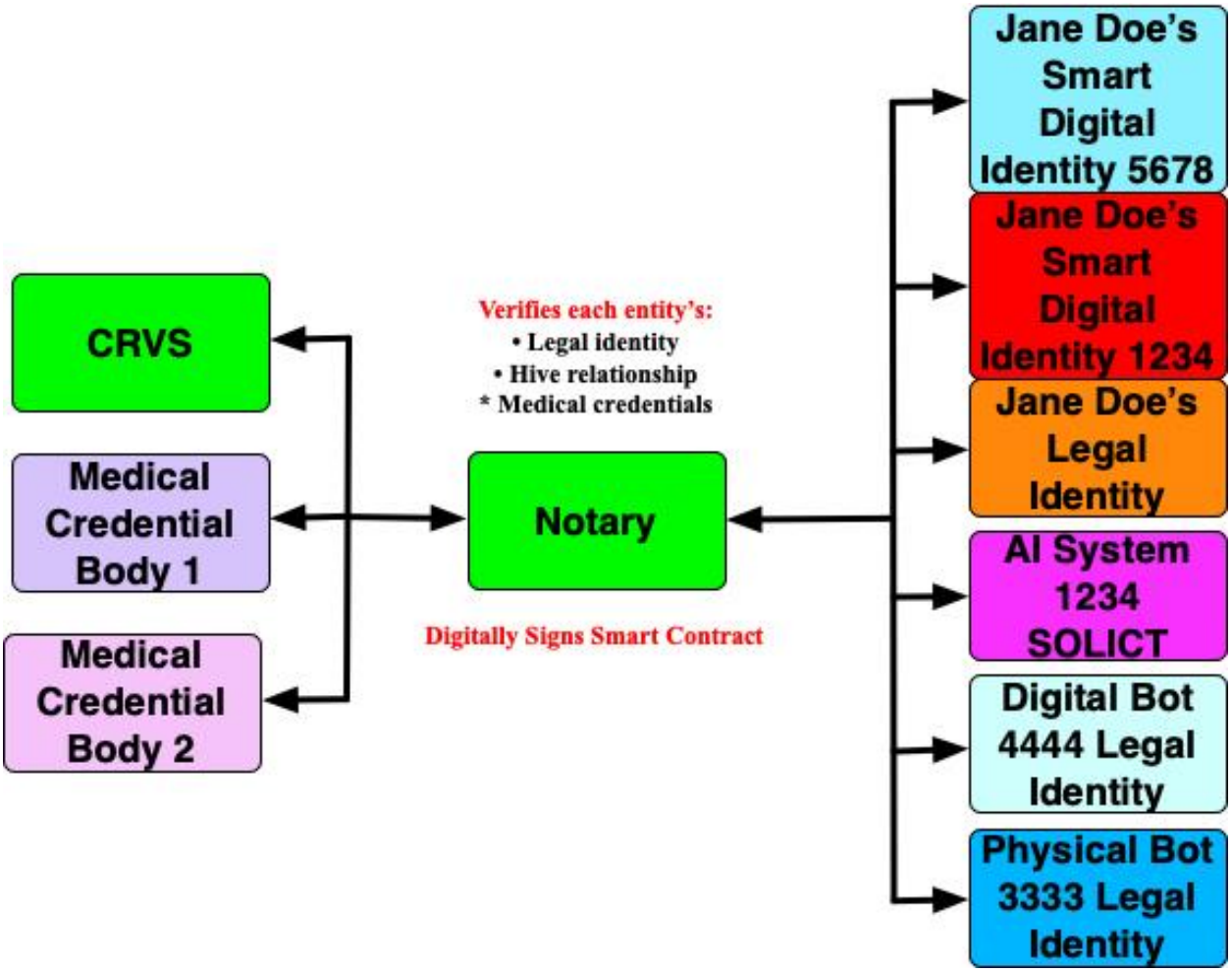
Now let's say the hive is part of Acme Health Inc. which Jane wants to enter a contract with, requiring identity verification of the entities, via a smart, AI leveraged contract. The two parties might be required to have a notary verify not only the legal identities above, but also their medical credentials.



Thus, the entities might approach the notary to verify:

- Each of the entity's legal identities above
- Their legal hive relationship
- Credentials for each entity

So, the notary would do the following:



It's this type of complicated example which I think Notaries can play a valuable, independent role in.

CRVS – Credential Issuing Authorities Subcomponent Costs:

Costs will be borne by the **Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre** section of this document.

Rethought Notaries Human Co-Design Interfaces Subcomponent Costs:

Background:

As stated in the "**Vision – Co-Design 'Nothing About Us Without Us**' section of this document,

"As I see it, these architectures two most important, critical challenges are:

1. **Creating a continually secure architecture for registering digital entities at transactional speeds**
2. **Creating citizen interfaces, designed from the ground up, enabling them to understand and use their SOLICT, LSSI devices, PIAM, DLT, IEP, LDV easily and securely. As well they must be able to easily work with local notaries. Without this, the architectures won't work in the field."**

This is why I've included in this notary cost-section a separate one devoted to co-design. All citizens, regardless of abilities or disabilities, MUST be able to work with their local notary re their legal identity and credentials.

Rethought Notaries Human Co-Design Subcomponent Costs:

Costs will be borne by "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre" section of this document.

Rethought Notaries Governance Laws/Regulations Subcomponent Costs:

Background:

Each jurisdiction around the planet has their own notary laws. Thus, just like legal identity, changing the underlying legal framework is a big political challenge, planet wide. As above, my suggested strategy is to find 1-3 jurisdictions, with a willing business and notary community to work with. Governance is the place to start with i.e., creating changes to an existing legal law and regulatory structure.

Rethought Notaries Governance Laws/Regulations Subcomponent Costs:

Cost will likely be borne by the Non-Profit - Manages Notary Standards For Legal Identity & Credentials section of this document.

Rethought Notaries- Legal Identity & Credential Verification Certification Process Subcomponent Costs:

Background:

This out of the box architecture allows a notary to:

- Verify an entity's:
  - Legal identity
  - Legal identity hive relationships
  - Authorization rights
  - Credentials issued to the entity
- Then there's the ability for a local notary to create attestations for a person claiming they don't have any legal identification documents, and the jurisdiction from which they were born in, having deleted them from their CRVS and other national identity systems

While this function of the notary is very desirable from a human rights perspective, it potentially opens the doors to a notary being able to troll all CRVS systems around the planet for an identity. I can easily see criminals leveraging a corrupt notary to do this.

THUS, MY VIEW IT TO NOT ALLOW A NOTARY TO BE ABLE TO TROLL CRVS SYSTEMS PLANET WIDE. Instead, limit them to being only able to do a search on a single legal identity, in one CRVS system at a time. Let's use Jane Doe as an example…

Jane has fled a country where they've deleted her CRVS and other jurisdictional legal identity databases. She goes to a local notary, claiming to be Jane Doe, from jurisdiction X, born on Y date at a certain location. She also claims she doesn't have any LSSI devices.

The local notary could then, with Jane's consent, take her forensic biometrics and do a search/comparison for the date and location within Jane's SOLICT. If it finds Jane's SOLICT, then the notary would be able to query a special digital signature Jurisdiction X's CRVS created when they wrote to Jane's SOLICT. The notary would be able to decrypt it, thus confirming Jane Doe's legal identity. The notary could then create a physical/digital attestation it's Jane Doe. Jane Doe could then take this and use it to prove her legal identity.

If Jane shows up at a local notary unable to recall which jurisdiction, she's from, date of birth, etc., and also unable to access Jane's SOLICT, the local notary would be unable to assist her. It would instead direct her to the local jurisdiction's CRVS office, where they would then use a special governance/business process to be able to obtain Jane's forensic biometrics, and search planet wide for her legal identity.

On a side note: In the paper "**Human Migration, Physical & Digital Legal Identity**", it discusses the fact that up to 50% of migrants are children. Some of these will have no parents, etc. They will fall under the above category, where the government CRVS system will have to prove their legal identities.

If the Notary is requited to do a hive legal relationship certification, then they'd have to do each entity, one at a time, with the CRVS where they were registered.

A very important security function will then be vetting new age notaries, and then granting them privileges as described above. The business processes in this case are very important. Why?

The Evil Inc's. and malicious states of the planet, will leverage weak business processes to put into place notaries who can search the planet's CRVS systems for identities.

Notary - Legal Identity & Credential Verification Certification Process Subcomponent Costs:

Cost will likely be borne by the "Non-Profit - Manages Notary Standards For Legal Identity & Credentials Subcomponent Costs" section of this document.

Notary - Digitally Sign Attestations/Contracts Subcomponent Costs:

Background:

The out of the box legal identity architecture, requires the ability for a notary to digitally sign an attestation or a contract confirming an entity's:

- Legal identity
- Legal identity hive relationships
- Authorization rights
- Credentials issued to the entity

THUS, THE NOTARY'S DIGITAL SIGNATURE BECOMES VERY IMPORTANT. Here are my thoughts:

1. At the beginning of the notary approval process, the actual legal identity of the notary will be determined via the CRVS to confirm it
2. Then I can see the local jurisdiction granting to the notary an ability to digitally sign documents as the notary

Let's use Jane Doe as a potential notary:

1. She'll have to go to the CRVS to, with her consent, provide her biometrics and her secret to see if they match the entry for her in the CRVS system
2. Assuming this is confirmed, she'll then go through the notary approval business processes
3. Assuming she passes this, then the local jurisdiction would grant her a "notary digital signature" assigned to her, to use in her notarization functions
4. Jane will then be able to sign attestations and documents using her two digital signatures:
    - Her personal one issued by the CRVS
    - Her notary one issued by the jurisdiction

Notary - Digitally Sign Attestations/Contracts Subcomponent Costs:

Cost will likely be borne by the "Non-Profit - Manages Notary Standards For Legal Identity & Credentials Subcomponent Costs" section of this document.

Notary – API Subcomponent Cost Centre:

Background:

As noted in the API Cost Centre section of this document, the API's become the electronic front door to the legal identity and credential functions, which includes notaries. Given privileges to the notary to search CRVS systems, the notary API becomes a prime attack vector. Thus, very careful security thought must be given to this.

Notary – API Subcomponent Costs:

Costs will be borne by the Non-Profit – API Rule Sets Subcomponent Cost Centre and the Cost Centre: API (Application Programming Interface) section of this document.

Cost Centre - Global, Independent Legal Identity & Credential Non-Profit

Background:

This curve frequently referred to in this document created problems that Albert Einstein was quoted as saying, "**We can't solve problems by using the same kind of thinking we used when we created them.**" Change happens faster and faster, potentially creating new attack vectors each hour.

Our old legal identity systems weren't built for this. **The curve requires out of the box thinking for out of the box times.** That's why, together with Michael Kleeman, I created the concept of a global, independent legal identity & credential non-profit. Its job is to do the following:

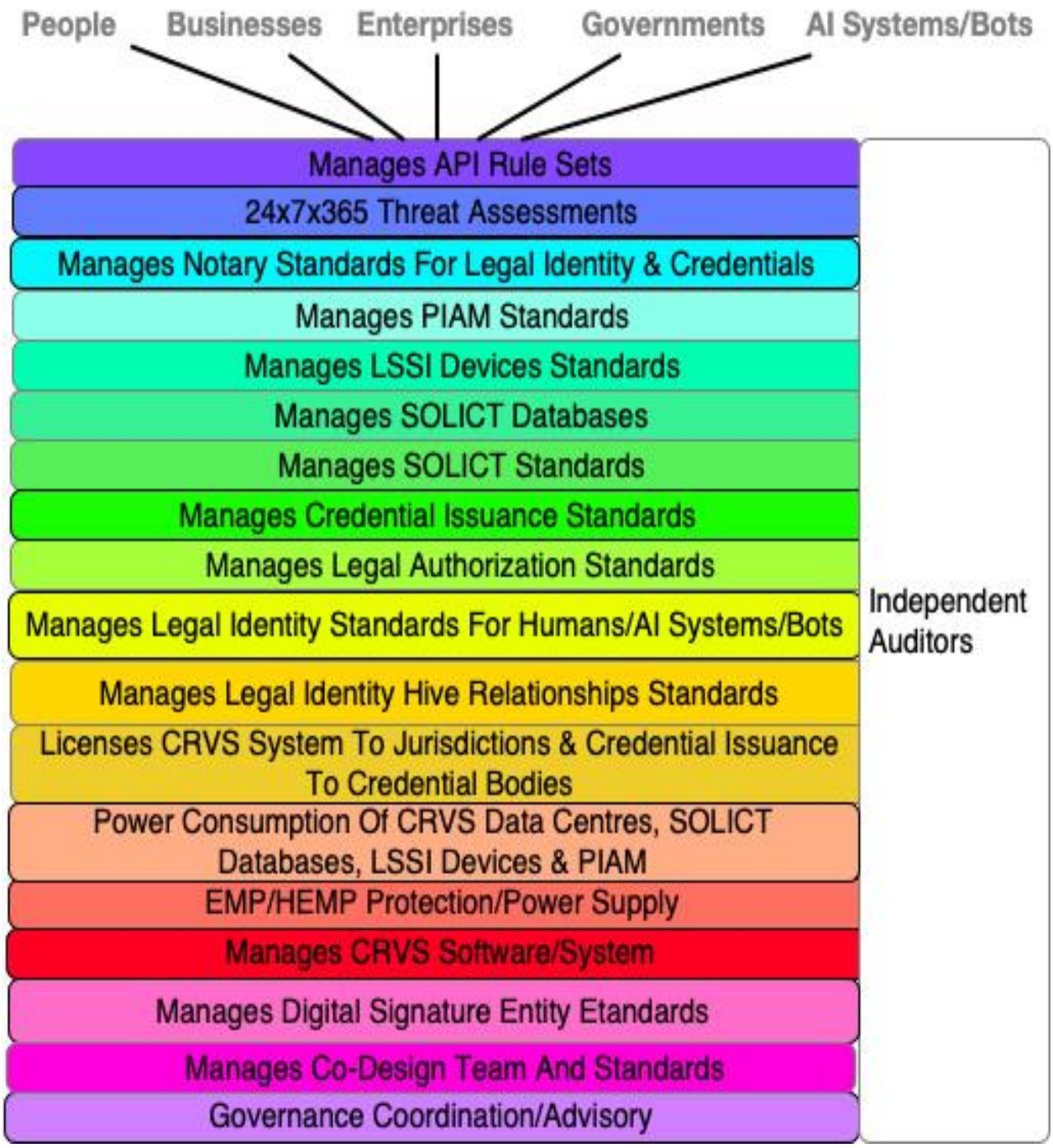
- Establish and maintain new legal identity data standards for humans and AI systems/bots
- Manage digital signature standards for humans, AI systems and bots
- Establish CRVS system standards, including legal identity relationships/hives and authorization
- Manage a co-design team to create the following for all citizens regardless of their abilities or disabilities:
    - CRVS jurisdiction interface for citizens
    - Understand what their SOLICT is, what data of theirs is in it, and how they can use it
    - Understand what their LSSI devices are, how they can use it, with their consent, to grant to others portions of their legal identity and/or credential information
    - Understand what their PIAM is, how they can use it, with their consent, to grant to others portions of their legal identity and/or credential information
    - Understand what the new age notary is, what services they can offer the citizen re their legal identity and/or credentials, and enable them to interact with them
- Create and maintain standards for SOLICT, LSSI, PIAM including API's
- Create standards for credential issuance API's
- Manage standards for notaries including API's used to access CRVS and credential authority data
- Manage SOLICT databases
- Offer low cost CRVS data conversion systems to rapidly get them converted to the new digital format
- Do 24x7x365 threat analysis against not only the tech used in legal identity framework, but also the governance, business processes and end users, issuing rated threat assessments, which governments, enterprises, and end users respond to according to the threat levels
- License CRVS systems to jurisdictions
- Manage power consumption of CRVS data centres, SOLICT databases, LSSI devices and PIAMs

The non-profit will exist in 3 different physical locations, 8 time zones apart. It begs the question, who'll pay for it?

The strategy is for the non-profit to license the CRVS to each jurisdiction, based on a low fee per CRVS transaction, up to a maximum yearly amount. The fee structure must be low enough enabling all jurisdictions to participate, yet enough to fund the likely very large costs associated with running the 24x7x365 threat centres.

Can an existing non-profit take on this responsibility? Likely not. Why? It must be politically squeaky clean, have a global board representing a wide range of different entities, and be nimble enough to rapidly create modifications to standards, et al, as well as running the SOLICT operations. That's what this cost centre delivers.

Global, Independent, Legal Identity & Credential Non-Profit Subcomponent Cost Centres Diagram:



Non-Profit – Governance Coordination/Advisory Subcomponent Cost Centre:

Background:

As I see it, the role and importance of the CRVS will exponentially change. Why? Answer - the introduction of AI systems, bots and AI leveraged smart digital identities of humans. These can be created at awesome speeds per second in one jurisdiction and, in the next instance, be operating in all other jurisdictions on the planet.

Thus, it requires a local/global legal identity framework. Which in turn leads to jurisdictional CRVS governance with international coordination re laws and regulations. So, while each jurisdiction must keep control over their own laws and regulations, it requires a new age governance framework.

Additionally, there are other jurisdictional governance laws and regulations requirements beyond the CRVS:

- SOLICT governance
- LSSI governance
- PIAM governance
- API governance
- Threat governance
- Credential governance re citizens/entities accessing them from their SOLICT/LSSI devices/PIAM
- Notary governance re legal identity & credentials access by citizens and/or entities

The non-profit must take over long-term governance advisory roles advising jurisdictions on governance.

The non-profit, who's operating in a VERY political world, must not be political. How can this be done? I suggest the following membership by type of representatives:

- Other global standards bodies
- Global non-profits
- UN
- Industry

I suggest the representative numbers chosen must ensure that to fundamentally change the global non-profit requires 66% of the members to support a change. This stops quick movements to take control of the board, yet it doesn't stop change from occurring to the non-profit.

I can see the body's headquarters being in a country well respected for being independent and stable. However, having said this, the actual operational piece of the global non-profit should be in three separate locations, roughly 8 time zones apart. Why?

Its job is to do 24x7x365 threat assessments as the planet turns. Further, if some type of disaster occurs in one or more locations, the non-profit keeps operating. So, this needs to be baked into the cost structure.

Governance costs also include management, HR, accounting, finance, payroll et al.

While a lot of the work of the non-profit will be done via the threat assessment part of it, an equally vital part is the legal team the non-profit has. Its work will cross over all jurisdictions, laws and regulations around the planet. Thus, it's very important to have a well-respected legal team, with LOTS of connections around the planet. Their job is to navigate potentially politically treacherous waters. I feel this non-profit must be created rather than assigning its functions to an existing non-profit body. It must be "politically squeaky clean" from the beginning.

The licensing aspect of the global non-profit is equally important from a governance perspective. Very careful political thought must be paid to how this is perceived around the planet.

Also, there's the SOLICT operations component, which also has a very political component to it as well. How the data is stored, where it's stored, how it's accessed all can quickly become political footballs. Thus, very careful political attention also needs to be given to this.
At a minimum, CRVS and SOLICT systems must be available at 5 9's availability (99.999% uptime is required) i.e., 5.26 minutes downtime per year. It would be desirable if it was 6 9's (99.9999%) i.e., 31.56 seconds downtime per year.

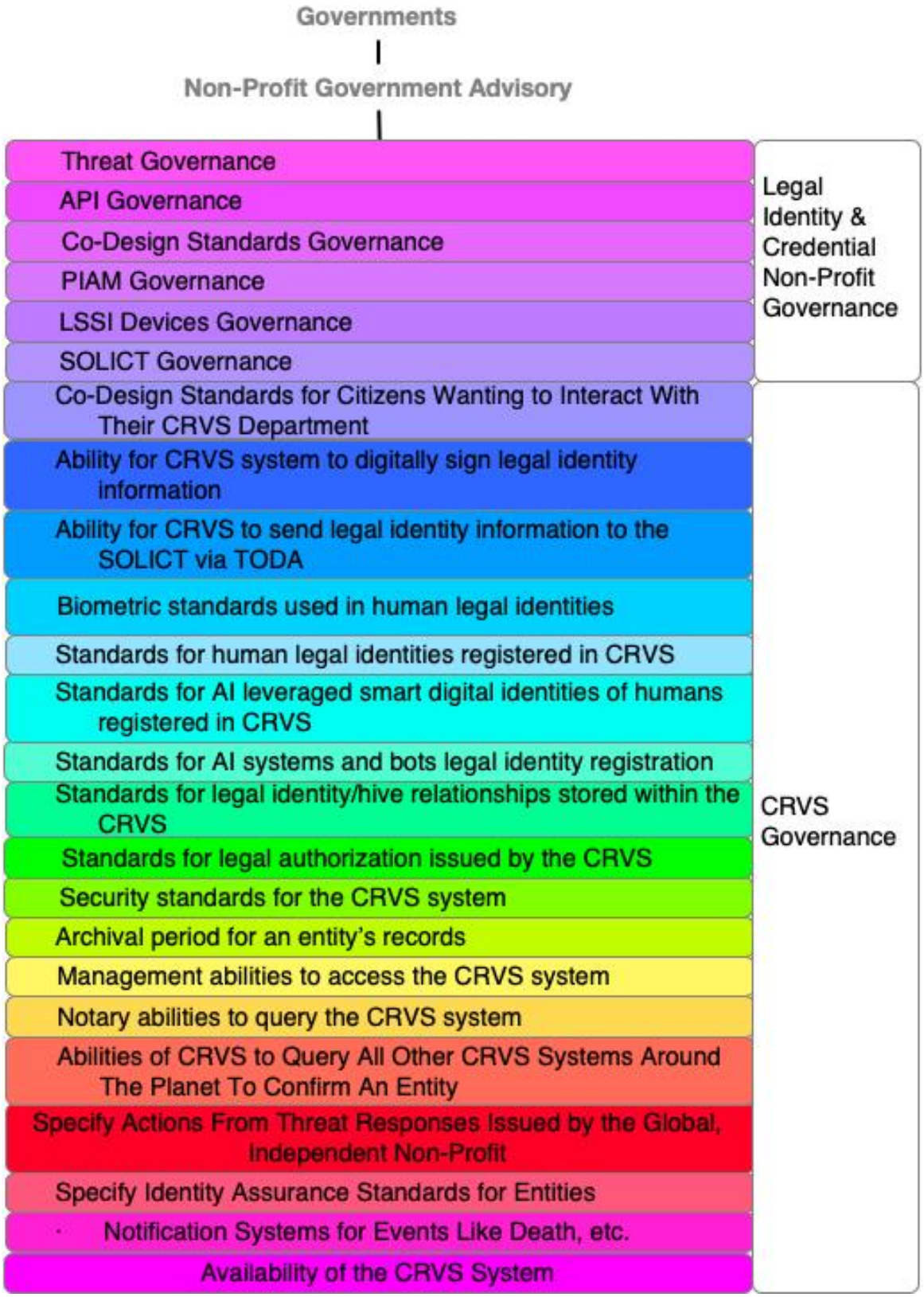
The governance of the non-profit must also take into consideration having representatives of people with disabilities. The architecture is built leveraging co-design to ensure it works for all people regardless of their abilities or disabilities.

Finally, management of the global, independent, non-profit must be done by a well-respected team. It's the heart of setting standards and protecting legal identity around the world. Thus, the management team must be of trusted people who can act independently, despite lots of political pressure from various groups.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Non-Profit – Governance Subcomponent Cost Centre

Governance Coordination/Advisory Centre Components:



Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Governance – Availability of the CRVS System Subcomponent Cost Centre
- CRVS Governance - Notification Systems for Events Like Death, etc. Subcomponent Cost Centre
- CRVS Governance - Specify Actions From Threat Responses Issued by the Global, Independent Non-Profit Subcomponent Cost Centre
- CRVS Governance - Abilities of CRVS to Query All Other CRVS Systems Around The Planet To Confirm An Entity Subcomponent Cost Centre
- CRVS Governance - Notary Abilities to Query the CRVS System Subcomponent Cost Centre
- CRVS Governance - Management Abilities to Access the CRVS System Subcomponent Cost Centre
- CRVS Governance - Archival Period for an Entity's Records Subcomponent Cost Centre
- CRVS Governance - Security Standards for the CRVS System Subcomponent Cost Centre
- CRVS Governance - Standards for Legal Authorization Issued by the CRVS Subcomponent Cost Centre
- CRVS Governance - Standards for Legal Identity/Hive Relationships Stored Within the CRVS Subcomponent Cost Centre
- CRVS Governance - Standards for AI Systems and Bots Legal Identity Registration Subcomponent Cost Centre
- CRVS Governance - Standards for AI Leveraged Smart Digital Identities of Humans Registered in CRVS Subcomponent Cost Centre
- CRVS Governance - Standards for Human Legal Identities Registered in CRVS Subcomponent Cost Centre
- CRVS Governance - Biometric Standards Used in Human Legal Identities Subcomponent Cost Centre
- CRVS Governance - Ability for CRVS to Send Legal Identity Information to the SOLICT via TODA Subcomponent Cost Centre
- CRVS Governance - Ability for CRVS System to Digitally Sign Legal Identity Information Subcomponent Cost Centre
- CRVS Governance - Co-Design Standards for Citizens Wanting to Interact With Their CRVS Department Cost Centre
- SOLICT Governance – Laws, Regulations & Management Subcomponent Cost Centre
- LSSI Governance – Laws & Regulations Cost Subcomponent Cost Centre
- API – Applications/API Rules/Governance Subcomponent Cost Centre
- CRVS Non-Profit – CRVS/Government Coordination/Advisory Subcomponent Cost Centre
- PIAM Governance Rules/Laws/Regulation Subcomponent Cost Centre
- Credential Standards Body Governance Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Note To the Reader:

Rather than break out each subcomponent cost above, I've decided not to. The pic above should be given to the team proposed below and used to get initial agreement arrived on what CRVS, notary, credential and non-CRVs governance (e.g., SOLICT, LSSI, PIAM, Co-design, etc.) will be. Then each sub-section should be tied to the other cost centres, and governance costs elucidated.

Non-Profit - CRVS Governance Coordination/Advisory Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

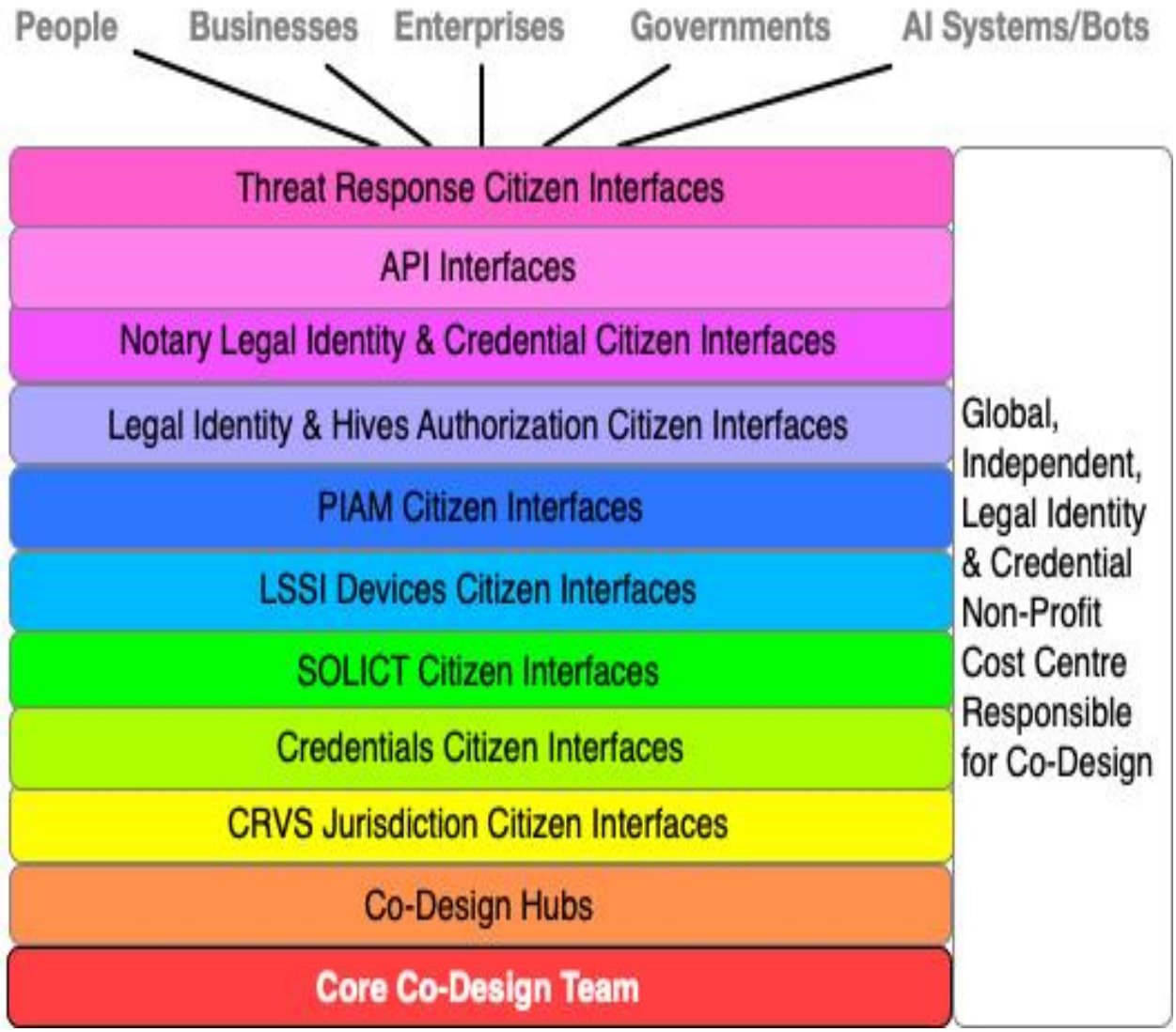
- Fund and create a small team composed of:
  - CRVS governance experts
  - Credential experts
  - Jurisdictional law experts
  - Standards experts
  - Political experts
  - CRVS experts
  - SOLICT experts
  - LSSI experts
  - PIAM experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Biometric/behavioral data experts
  - Business process experts
  - Security/red team experts
  - Network/connectivity experts
  - Data centre/cloud experts
  - EMP/HEMP experts
  - Co-design experts
  - Notary experts
  - Lesson learnt experts
  - Ensure representatives from the other non-profit teams
- Create use cases for the
  - CRVS governance requirements as noted in the pic above
  - The SOLICT, LSSI, PIAM, etc.
  - Notary legal identities
  - Credentials
  - Etc.
- Determine costs and legislation and regulation requirements
- Pilot them in 1-3 jurisdictions
- Learn what works, what doesn't work and then adjust
- Rapidly expand around the planet

Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Background:

As stated in "Vision – Co-Design 'Nothing About Us Without Us' and throughout this doc, co-design is mission critical in enabling people to understand and use the legal identity and credential architecture. As importantly, the section "Us "contains very useful lessons for the team managing this cost centre to learn from.

Non-Profit Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centres Diagram:



Cost Centres Dependent Upon This:

- CRVS - Creating a New CRVS System With Data Standards for Legal Identities and Vital Statistics Subcomponent Cost Centre
- CRVS – Manage Digital Signature Entities Standards Subcomponent Cost Centre
- Smart Digital Identities Co-Design Interface for Humans/Smart Digital Identities Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships - Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Subcomponent Cost Centre
- CRVS - Co-Design Driven Standards For Accessing Legal Authorization Rights Subcomponent Cost Centre:
- CRVS Citizen Co-Design Standards Cost Centre
- CRVS Governance - Ability for CRVS System to Digitally Sign Legal Identity Information Subcomponent Cost Centre
- CRVS Governance – Co-Design Standards For Citizens Interacting With Their CRVS Subcomponent Cost Centre
- Credential Co-Design Abilities to Use Credentials Subcomponent Cost Centre
- Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Cost Centre
- Legal Authorization Rights - Co-Design Driven Standards For Accessing Legal Authorization Rights Cost Centre
- SOLICT Citizen Co-Design Standards Subcomponent Cost Centre
- LSSI Device Co-Design Subcomponent Costs:
- PIAM Co-Design For Humans Subcomponent Costs:
- Rethought Notaries Human Co-Design Interfaces Subcomponent Costs:
- Learning Non-Profit – Co-Design Subcomponent Cost Centre

VERY IMPORTANT NOTE:

As stated throughout this document I'm NOT a co-design expert. Given this, here are my thoughts:

The learning architecture is built on top of the legal identity and credential architecture. Thus, in the beginning, the learning co-design team will be heavily reliant upon the legal identity and credential co-design team.

Therefore, I'm suggesting that in the early days, the learning co-design team become part of the legal identity and credential co-design team. While the learning co-design team focusses on "learning", I think that there will be lots of initial cross-over between the two teams. Both teams can leverage the same co-design hubs. When the time is right, the two teams can separate.

If co-design experts agree with this suggestion, then it complicates the budgeting and governance structures. Why? The two teams in the end will reside in separate non-profits. Thus, it requires an initial flexible approach in governance and budgeting until the two teams decide it's time to separate. Food for thought.

Non-Profit Core Co-Design Team Subcomponent Cost Centre:

Background:

Note: I'M NOT A CODESIGN EXPERT. THUS, WHAT'S WRITTEN BELOW WILL LIKELY BE EDITED AND ADJUSTED BY PEOPLE THAT ARE.

The core co-design team is composed of many different types of people including:

- People with a wide variety of disabilities
- People of different genders
- People of different first nations
- Experienced psychologists, psychiatrists and physiotherapists who work with people having disabilities
- VERY experienced co-design team leaders who've already successfully implemented co-design projects
- Legal experts who are experienced in laws and regs pertaining to people with disabilities having access to specific citizen facing systems
- Business process experts who are experienced in delivering services to people with disabilities
- Governance experts who are experienced in delivering citizen facing governance solutions involving co-design
- Security experts who are experienced in delivering citizen facing security solutions involving co-design
- Etc.

I suggest that a core team of co-design people be created which will be used for all the co-design subcomponent cost centres depicted in the pic at the beginning of this section. Where specific subcomponent cost centres require additional expertise or different types of people with disabilities, then the team will be expanded to include them.

Non-Profit Core Co-Design Team Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - People with a wide variety of disabilities
  - People of different genders
  - People of different first nations
  - People with a wide variety of ages
  - Experienced psychologists, psychiatrists and physiotherapists who work with people having disabilities
  - VERY experienced co-design team leaders who've already successfully implemented co-design projects
  - Legal experts who are experienced in laws and regs pertaining to people with disabilities having access to specific citizen facing systems
  - Business process experts who are experienced in delivering services to people with disabilities
  - Governance experts who are experienced in delivering citizen facing governance solutions involving co-design
  - Security experts who are experienced in delivering citizen facing security solutions involving co-design
  - Notary experts
  - Lesson learnt experts
  - Etc.
- Create high level requirements, use cases, and cost estimates for:
  - Annually running the core co-design team in one country and their local state/provinces jurisdictions for the following subcomponent cost centres:
    - Co-design hubs
    - CRVS Jurisdiction Citizen Interfaces
    - Credentials Citizen Interfaces
    - SOLICT Citizen Interfaces
    - LSSI Devices Citizen Interfaces
    - PIAM Citizen Interfaces
    - Legal Identity & Hives Authorization Citizen Interfaces
    - Notary Legal Identity & Credential Citizen Interfaces
    - Threat Response Citizen Interfaces
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work, and then adjust the core team accordingly
- Next, prepare the core co-design team to scale as other countries and their local jurisdictions adopt the new legal identity and credential architectures
- Rapidly scale around the planet

VERY IMPORTANT NOTE:

1. **THE NON-PROFIT MANAGEMENT TEAM MUST NOT ALLOW GOVERNMENTS TO EXPAND CO-DESIGN SERVICES, LEVERAGING THIS TEAM, TO OTHER GOVERNMENT SERVICES. THIS WAS THE ONE OF THE KISSES OF DEATH TO THE NADIA CO-DESIGN PROJECT IN AUSTRALIA**
2. **THE CITIZEN SERVICES OFFERED THROUGH THE LEGAL IDENTITY ARCHITECTURE ARE BOUNDED. THUS, ONLY THESE SERVICES SHOULD BE ADDRESSED AND NOTHING MORE**
3. **FURTHER, THE SERVICES OFFERED SHOULD NOT TELL THE CITIZEN WHAT TO DO. THEY SHOULD EDUCATE THEM ABOUT THE CHOICES AND LEAVE THE DECISION MAKING TO EACH CITIZEN**

Non-Profit – Co-Design Hubs Subcomponent Costs:

Background:

Note: I'M NOT A CODESIGN EXPERT. THUS, WHAT'S WRITTEN BELOW WILL LIKELY BE EDITED AND ADJUSTED BY PEOPLE THAT ARE.

While reading Marie Johnson's excellent book, **Nadia – Politics, Bigotry, Artificial Intelligence",** I was educated about why co-design hubs are critical for enabling people with disabilities to participate in co-design. Thus, I've created this cost centre embracing this.

Depending on the country that initially funds, the number of co-design hubs required will likely vary. To create my first high-level cost guesstimate, I've used the number of 30 co-design hubs to begin with. Whatever the final number, my advice to the team responsible for this subcomponent cost centre is drive out a budget cost per co-design hub which can be used within the initial country to calculate total guesstimated costs for all the hubs.

Non-Profit Co-Design Hubs Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - People who've created co-design hubs before
- Create high level requirements, use cases, and cost estimates for:
  - Cost guesstimates to create each co-design hub
  - Total number of co-design hubs required
  - Annual costs for running the
  - Annually running the co-design hubs in one country and their local state/provinces jurisdictions for the following subcomponent cost centres:
    - CRVS Jurisdiction Citizen Interfaces
    - Credentials Citizen Interfaces
    - SOLICT Citizen Interfaces
    - LSSI Devices Citizen Interfaces
    - PIAM Citizen Interfaces
    - Legal Identity & Hives Authorization Citizen Interfaces
    - Notary Legal Identity & Credential Citizen Interfaces
    - Threat Response Citizen Interfaces
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design hubs, and then adjust the hubs accordingly
- Next, prepare to adjust co-design hubs to scale as other countries and their local jurisdictions adopt the new legal identity and credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design CRVS Jurisdiction Citizen Interfaces Subcomponent Costs:

Note: Other Cost Centres Dependent Upon This:

- CRVS - Creating a New CRVS System With Data Standards for Legal Identities and Vital Statistics Subcomponent Cost Centre
- Smart Digital Identities Co-Design Interface for Humans/Smart Digital Identities Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships - Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Subcomponent Cost Centre
- CRVS - Co-Design Driven Standards For Accessing Legal Authorization Rights Subcomponent Cost Centre:
- CRVS Governance - Co-Design Standards for Citizens Wanting to Interact With Their CRVS Department Cost Centre

Background:

All the above cost centres require people with various abilities and disabilities to interact with their CRVS driven legal identity data systems, applications, and department. The co-design team assigned to this subcomponent cost centre must be involved from day one with the subcomponent teams listed above to create citizen interfaces.

Non-Profit – Co-Design CRVS Jurisdiction Citizen Interfaces Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re CRVS noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity and credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design Credentials Citizen Interfaces Subcomponent Costs:

Note: Other Cost Centres Dependent Upon This:

- Credential Co-Design Abilities to Use Credentials Subcomponent Cost Centre

Background:

As stated in the "Cost Centre: Authoritative Credentials Source" section of this document:

> "Thus, the architecture is built on a global, independent non-profit responsible for credential issuance standards, which the credential standards bodies can adopt. Over time, as the non-profit detects new attack vectors against the credential issuing standards, it can automatically notify the standards body, with the body taking appropriate action based on the threat risk level.
>
> **This approach leaves the credential standards body still in control over their management of the credential, but ensures as it's issued, both physically and digitally, it will be secure. Thus, it's politically acceptable.**
>
> Further, how citizens with different abilities and disabilities use credentials can now be standardized. Leveraging co-design, the new global, independent, legal identity and credential non-profit can create a wide variety of citizen interfaces to their credentials via their LSSI devices and/or PIAM. As security conditions change due to this curve, the citizen interfaces to the credentials can be updated based on threats."

Co-design is mission critical in ensuring citizens of all abilities and disabilities:

- Understand what's stored in their SOLICT re credentials
- Understand how to use their LSSI devices and/or PIAM to release portions of their credentials to other parties

Non-Profit – Co-Design Credentials Citizen Interfaces Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the Credential Co-Design Abilities to Use Credentials Subcomponent Cost Centre
- As the above subcomponent cost centre work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design SOLICT Citizen Interfaces Subcomponent Costs:

Note: Other Cost Centres Dependent Upon This:

- SOLICT Citizen Co-Design Standards Subcomponent Cost Centre
- Non-Profit - Manages Digital Signature Entity Standards Subcomponent Cost Centre

Background:

As stated in the "Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) " section of this document:

> **"Citizens Understanding What Their SOLICT Is and Does:**
> Literally billions of people around the planet will be leveraging their SOLICT to prove their legal identity and credentials. Regardless of their abilities or disabilities, they need to understand:
>
> - What their SOLICT is
> - How they can manage it via their LSSI devices and/or PIAM
>
> This is where co-design comes into major play to deliver it to them around the planet and around the clock."

Non-Profit – Co-Design SOLICT Citizen Interfaces Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the SOLICT Citizen Co-Design Standards Subcomponent Cost Centre
- As the above subcomponent cost centre work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design LSSI Devices Citizen Interfaces Subcomponent Cost Centre:

Other Cost Centres Dependent Upon This:

- LSSI Device Co-Design Subcomponent Costs
- LSSI - Legal Physical ID Cards Subcomponent Costs
- LSSI - Digital LSSI App Subcomponent Costs
- LSSI - Biometrically Tied LSSI ID Wristband Subcomponent Costs
- LSSI - Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs

Background:

From a citizen's perspective, the LSSI devices is the front end of the architecture, they'll first meet. Thus, it's my own personal view that the success of LSSI devices, for humans, regardless of their abilities or disabilities, resides on how co-design can:

1. **Educate them, re what their LSSI devices are**
2. **Explain how to use them**
3. **Let citizens make their choices re what portions of their legal identity and/or credentials to release**
4. **Then rapidly, securely assist the citizen in implementing their choice via their LSSI devices and/or their PIAM**
5. **When security updates require changes to their LSSI devices, it's imperative that all citizens understand what the change is and why they must adjust**

THE CO-DESIGN TEAM MUST GET THIS RIGHT FOR ALL CITIZENS.

Non-Profit – Co-Design LSSI Devices Citizen Interfaces Subcomponent Costs

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re these cost centres:
  - LSSI Device Co-Design Subcomponent Costs
  - LSSI - Legal Physical ID Cards Subcomponent Costs
  - LSSI - Digital LSSI App Subcomponent Costs
  - LSSI - Biometrically Tied LSSI ID Wristband Subcomponent Costs
  - LSSI - Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs
- As the above subcomponent cost centre work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design PIAM Citizen Interfaces Subcomponent Costs:

Other Cost Centres Dependent Upon This:

- PIAM Co-Design For Humans Subcomponent Costs

Background:

Following my comments in the prior Co-Design LSSI subcomponent cost, the next most critical thing for judging success of the architecture is leveraging co-design to:

1. **Educate citizens of all abilities and disabilities on what their PIAM is**
2. **Then educating them on how to use it**
3. **Allowing them to make their own choices**
4. **And then rapidly, securely assist the citizen in implementing their choice via their LSSI devices and/or their PIAM**
5. **When security updates require changes to their PIAM, it's imperative that all citizens understand what the change is and why they must adjust**

THE CO-DESIGN TEAM GET THIS RIGHT FOR ALL CITIZENS.

Non-Profit – Co-Design PIAM Citizen Interfaces Subcomponent Costs

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the PIAM Co-Design For Humans Subcomponent Costs
- As the above subcomponent cost centre work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design Legal Identity & Hives Authorization Citizen Interfaces Subcomponent Costs:

Note: Cost Centres Dependent Upon This:

- Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Cost Centre
- Legal Authorization Rights - Co-Design Driven Standards For Accessing Legal Authorization Rights Cost Centre

Background:

As stated in the "Cost Centre – Legal Authorization Rights" section of this document, legal authorization is complicated. It could be a very legal and political complex can of worms to open. Thus, my suggestion is for the team to keep their initial deliverables very tight i.e., don't try to solve the world's legal authorization problems.

Non-Profit – Co-Design Legal Identity & Hives Authorization Citizen Interfaces Subcomponent Costs

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the Co-Design Driven Standards for Citizen Use of Legal Identity Relationships Cost Centre and the Legal Authorization Rights - Co-Design Driven Standards For Accessing Legal Authorization Rights Cost Centre
- As the above subcomponent cost centres work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design Notary Legal Identity & Credential Citizen Interfaces Subcomponent Costs:

Note: Cost Centres Dependent Upon This Cost Centre:

- Rethought Notaries Human Co-Design Interfaces Subcomponent Costs

Background:

A notary is a publicly commissioned official who serves as an impartial witness to the signing of a legal document. Document signings where the services of a notary are generally necessary are real estate deeds, affidavits, wills, trusts, power of attorney, bills of sale, or other official transactional documents. Notaries were created centuries ago to deter fraud. As stated in "Cost Centre: Rethought Notaries" section of this document:

> "I like the concept of notaries, since they're independent of government, acting as a go-between between governments and citizens in proving their legal identities. Thus, I've included rethought notaries in the architecture.
>
> The place to start is by rethinking how they verify entities identities. In today's planet, this can be very challenging, since a person, their smart digital version of them, or an AI system or bot, might be interacting digitally with a local notary, from the other side of the planet.
>
> Another challenge is Jane Doe fleeing Jurisdiction X to Jurisdiction Y because the government deleted her CRVS record and any other government identity database of her. I could see Jane going to a local notary in Jurisdiction Y and, with her consent, giving her legal identity information plus her forensic biometrics, and the notary able to do a single search on the CRVS system to prove she's Jane Doe. When the search turns negative, the notary can search her SOLICT to see a special digital signature the CRVS signed when creating her SOLICT entry. They'd be able to decrypt it this confirming it's Jane Doe. They could then create a physical and digital attestation she's Jane.
>
> Yet another challenge with notaries is their being able to work with citizens of all abilities and disabilities. Thus, I could see co-design assisting notaries in their work with all citizens re legal identity and credential proofing.
>
> As with the rest of this architecture, it's visionary. I don't want to try to sell the planet on what a wonderful idea it is. Instead, my strategy is to find innovative funders, with 1-3 jurisdictions, with a willing business and notary community, to rethink notaries in small steps. That's what the cost centres call out for. Then, once we've figured it out in real life, rapidly scale."

Thus, co-design is a critical component, allowing all citizens, regardless of abilities or disabilities to knowledgably interact with the new age notary the architecture calls out for.

Non-Profit – Co-Design Notary Legal Identity & Credential Citizen Interfaces Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the "Rethought Notaries Human Co-Design Interfaces Subcomponent Costs" subcomponent section of this document
- As the above subcomponent cost centres work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design API Interfaces Subcomponent Costs:

Note: Cost Centres Dependent Upon This Cost Centre:

- API- Interfaces Co-Design Subcomponent Cost Centre
- CRVS API – Co-Design Interfaces Subcomponent Cost Centre

Background:

The legal identity, credential and notary architecture is built around ensuring all citizens, regardless of their abilities or disabilities can leverage their SOLICT, LSSI devices, PIAM, credentials and interact with a notary regarding these. Thus, any API interface pertaining to citizens, must be designed, and tested allowing all citizens to interact with the above. That's what this cost centre delivers.

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the above noted subcomponent
- As the above subcomponent cost centres work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit – Co-Design Threat Response Citizen Interfaces Subcomponent Costs:

Note: Cost Centres Dependent Upon This Cost Centre

- Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs

Background:

As noted throughout this document, the new architecture for CRVS, SOLICT, LSSI Devices, PIAM and notaries results in them becoming prime attack vectors for the Evil Inc.'s and the malicious states of the planet. They'll leverage this curve, to create each day, new attack vectors against the legal identity and credential governance, business processes, tech infrastructure and end users, be they human, AI systems or bots.

One of the reasons I created the new, global, independent, legal identity and credential, extremely well-funded, non-profit was to do 24x7x365 threat analysis against legal identity and credential governance, business processes, tech infrastructure and end users. They'll issue rated threats. So, a very high threat will require governments, companies, enterprises, people, and entities to make changes within hours. This brings current industry best practices to the world of legal identity.

Where all this might fail is if the human citizen doesn't understand what a highly rated threat is, nor why they might have to change how they interface with their LSSI devices and/or PIAMS. Thus, co-design is a mission critical component in handling threat responses. It's why I've broken out this as a separate co-design cost centre.

Non-Profit – Co-Design Threat Response Citizen Interfaces Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re the Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs section of this document
- As the above subcomponent cost centres work begins, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new credential architectures
- Rapidly scale around the planet

Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre:

Background:

TODAY, ON THE PLANET, THERE IS NO LEGAL IDENTITY STANDARDS FOR AUTHORITATIVE CRVS (CIVIL REGISTRATION VITAL STATISTICS) SYSTEMS FOR HUMANS AND AI SYSTEMS/BOTS. It creates the crappy, very costly, mess detailed in "**Legal Identity Problem Statements**". **Thus, the door is wide open for the new, global, independent, legal identity & credential non-profit to create and manage global legal identity standards for these types of entities.**

As per the CRVS, SOLICT, LSSI, legal identities for smart digital identities and AI systems/bots cost centres of this document, it's highly likely the global, independent non-profit will manage standards for this. Yes, it's complicated and political. Thus, as per the governance subcomponent section of this document, it requires very careful thought in membership of the various committees overseeing the standards bodies.

I have an underlying premise about standards bodies in general. This curve means that new attack vectors are being created each hour not only against the tech used in standards, but also the governance, business processes and end users. Since legal identity is a high value attack target, one can expect criminals and malicious states expending lots of money to try to successfully attack the legal identity framework.

Thus, when a very high-risk attack threat is determined, it comes home to roost in standards bodies, laws, and regulations. It means the standards body MUST have processes allowing for a very streamlined approval process for changes to standards for very high-risk threats.

Also, the same applies to regulations jurisdictions use, which will likely be based on the standards. Thus, they too must have similar very streamlined processes for rapidly changing regulations standards for very high-risk threats. Having said all of this, regular type changes to standards, laws and regulations MUST be done using traditional processes, ensuring there is appropriate consideration, and approval from the right folks and jurisdictions.

Bottom line: Standards bodies and regulations will have to become nimbler to deal with the effects of the curve.

Finally, there's all the different standards and standard operating processes for collection and use of biometrics (review the CRVS Biometric Cost Centre section of this document). It's likely many of these will be managed by other bodies, but the standards must be referenced within the global, independent, non-profit for licensing use of CRVS, SOLICT, LSSI etc.

Biometric Cost Centres Which Will Feed Into This Cost Centre:

- Biometric Standards for Infant Fingerprints Subcomponent Cost Centre
- Biometric Standards/Operating Procedures for People Who Don't Have Fingerprints or Iris's Subcomponent Cost Centre
- Biometric Standards for Legally Determining Physical Identity of a Deceased Person Subcomponent Cost Centre
- Research & Standards for Anonymous Biometric Identifiers Subcomponent Cost Centre
- Standardized, Secure Methods for Obtaining Biometrics Out in the Field/Urban Locations Subcomponent Cost Centre
- Age Determination of When Children's Iris Registration Can Safely Occur Subcomponent Cost Centre
- Automation of Forensic Biometric Collection Subcomponent Cost Centre
- Research Confirming Fingerprints/Iris Are Enough to Legally Differentiate Human Clones Subcomponent Cost Centre

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Governance - Standards for AI Systems and Bots Legal Identity Registration Subcomponent Cost Centre
- CRVS Governance - Standards for AI Leveraged Smart Digital Identities of Humans Registered in CRVS Subcomponent Cost Centre
- CRVS Governance - Standards for Human Legal Identities Registered in CRVS Subcomponent Cost Centre
- CRVS Governance - Biometric Standards Used in Human Legal Identities Subcomponent Cost Centre
- CRVS Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre
- SOLICT Authoritative Legal Identity, Credential, Legal Identity Relationships/Hive and Authorization Rights Sources Subcomponent Cost Centre
- PIAM –Authoritative Data Source SOLICT Subcomponent Cost Centre
- Learners, Teachers, Bots Legal Identity, Relationships/Hives, Legal Authorization Rights and Credentials Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships Authoritative Data Source CRVS Subcomponent Costs:
- CRVS API - CRVS Authoritative Sources Databases Subcomponent Cost Centre
- Legal Identity & Hive Relationships - Authoritative Entity Data Source – CRVS Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:
- Learner's Legal identity Subcomponent Cost Centre
- Notaries - CRVS - Authoritative Source for Human & AI System/Bot Legal Identities, Legal Identity/Hive Relationships & Authorization Rights) Subcomponent Costs
- Local/Global Legal Identity, Credentials and Notary Framework Subcomponent Cost Centre

Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Standards experts
  - Political experts
  - CRVS experts
  - SOLICT experts (database plus legal)
  - LSSI experts (devices plus legal)
  - PIAM experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Biometric/behavioral data experts
  - Legal experts
  - Business process experts
  - Security/Red team experts
  - Standards experts
  - Network/connectivity experts
  - Data centre/cloud experts
  - EMP/HEMP experts
  - Co-design experts
  - Notary experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for legal identities of:
  - Humans
  - AI systems
  - Bots
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground

Non-Profit - Manages Digital Signature Entity Standards Subcomponent Cost Centre:

Background:

As I see it, here's the whopper sized challenge approaching us. Digital and physical bots will soar in numbers into the billions or more. Based on risk, many of them will have legally registered identities. They might or might not be required to digitally sign as an entity.

The Evil Inc.'s of the planet are going to want to be able to masquerade as these entities. Thus, they'll leverage this curve, to create new attack vectors against digital signatures. One of the attack vectors will be against the CRVS components issuing the entity digital signatures.

Thus, the architecture includes the non-profit with responsibility for digital signature standards. Its job is to constantly do threat assessments against digital signatures and then change, as required:

- Digital signature standards
- Digital signature issuing standards
- Laws and regulations pertaining to digital signatures

As importantly, is educating all citizens, regardless of their abilities or disabilities, on:

- **What their digital signature is**
- **How they can use it via their LSSI devices and/or their PIAM**

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Governance - Ability for CRVS System to Digitally Sign Legal Identity Information Subcomponent Cost Centre
- CRVS Non-Profit - Manages Digital Signature Entity Standards Subcomponent Cost Centre
- Creation of Legal Authorization Rights With Digital Signature Within CRVS Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Very Important Note:

Rather than create a team to manage legal identity standards and another to manage digital signatures, it makes more sense to combine the two costs centres under the same team. For this version of the spreadsheet, I HAVE NOT DONE SO. If this makes sense it will save on the order of $48-90 million over three years.

Non-Profit - Manages Digital Signature Entity Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Standards experts
  - Digital signature experts
  - Political experts
  - CRVS experts
  - SOLICT experts
  - LSSI experts
  - PIAM experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Legal experts
  - Business process experts
  - Red team experts
  - Network/connectivity experts
  - Data centre/cloud experts
  - EMP/HEMP experts
  - Co-design experts
  - Notary experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for digital signatures of:
  - Humans
  - AI systems
  - Bots
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground

Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre:

Background:

I realized long ago the underlying CRVS framework was badly flawed. So, I set out to rethink it. In the front of my mind, was the fact in many jurisdictions on the planet, legal identity is managed by laws and regulations at the local state/provincial level. Thus, I knew this was a political hill I didn't want to die on in pitching a new age legal identity framework. I wanted to architect something that still left local jurisdictions in control over their legal identity laws and regulations but worked globally.

I also realized the effects of Pat Scannell's tech change curve on CRVS systems. I knew, from my own past professional experience, that local governments don't have the resources, budget, and expertise to combat new hourly attacks on the legal identity governance, business processes, tech infrastructure and end users (be they humans, AI systems or bots). Thus, I knew I had to create an architectural solution giving them constant guidance on changes to their underlying CRVS systems, governance, business processes and end users.

I also realized citizens of all abilities and disabilities will interact with their local CRVS jurisdiction. Thus, I've included co-design as part of the CRVS solution framework.

All of the above was why I created, with Michael Kleeman, the concept of a new, global, independent non-profit, to create the new age CRVS system and constantly update it based on 24x7x365 threat analysis.

I architected for each local CRVS jurisdiction to keep running their own CRVS system, but under license from the global, independent, non-profit. The license agreement would state that based on threat levels, the local jurisdiction MUST change their underlying CRVS governance, business process, tech infrastructure within an agreed upon amount of time. For example, a very high level of threat must be responded to by the local CRVS within hours. This brings current industry best practices to the world of legal identity.

That's what this cost centre delivers. It's an end-to-end CRVS solution framework constantly kept up to date by the global, independent, well-funded, non-profit.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Data Centres 99.999% Availability Subcomponent Cost Centre
- CRVS Servers (Physical & Cloud)/Data/Network Subcomponent Cost Centre
- CRVS Processes Updating Servers/Apps/Network Subcomponent Cost Centre
- CRVS Backup Strategy/Processes Subcomponent Cost Centre
- CRVS Disaster Recovery Subcomponent Cost Centre
- CRVS Governance – Availability of the CRVS System Subcomponent Cost Centre

- CRVS Governance - Notification Systems for Events Like Death, etc. Subcomponent Cost Centre
- CRVS Governance - Abilities of CRVS to Query All Other CRVS Systems Around The Planet To Confirm An Entity Subcomponent Cost Centre
- CRVS Governance - Notary Abilities to Query the CRVS System Subcomponent Cost Centre
- CRVS Governance - Management Abilities to Access the CRVS System Subcomponent Cost Centre
- CRVS Governance - Archival Period for an Entity's Records Subcomponent Cost Centre
- CRVS Non-Profit - Manages CRVS Software/System Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Non-Profit - Manages CRVS Software/System Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Standards experts
  - Political experts
  - CRVS experts
  - SOLICT experts (database plus legal)
  - LSSI experts (devices plus legal)
  - PIAM experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Biometric/behavioral data experts
  - Legal experts
  - CRVS business process experts
  - Security/red team experts
  - Standards experts
  - Network/connectivity experts
  - Data centre/cloud experts
  - EMP/HEMP experts
  - Co-design experts
  - Notary experts
  - CRVS governance experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for managing end-to-end the CRVS system
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, adjust and rapidly scale around the planet

Non-Profit – EMP/HEMP Protection/Power Supply Subcomponent Cost Centre:

Background:

Over my business life as an identity architect, I've led many leading edge, visionary, identity projects. They were often the first within an enterprise requiring high availability i.e., 99.999%. Thus, my teams would work on things like:

- Being able to continually update software without taking down all servers
- Highly available data centres
- Cloud

All of this was in the back of my mind while architecting a new legal identity trust framework. As the planet madly digitizes, I realized the digital legal identity trust framework of the new age CRVS system I was proposing had a very big potential weakness. It required electricity to run 24x7x365.

So, I asked myself this dumb question – "What could bring all of this down?" I strongly suggest readers read "**When Our Digital Legal Identity Trust Goes Poof!**". **There's a 1 in 8 chance this decade our electrical grids could go down!**

IT WON'T BE POLITICALLY POPULAR TO ADDRESS. Why? It requires governments and industry to invest lots of money reengineering their electrical grid networks. Industry won't want to voluntarily do this in short time frames. Governments won't want to invest since it takes money away from other high-profile budgets. I sum it up in one word – YIKES!!!!!

Couple this with the fact AI systems are on track to consume most of the planet's energy by the 2040's (skim Figure 1 in "**AI Power Consumption Exploding**").

Then add in the fact that the new age CRVS and SOLICT systems must be available at 5 9's 99.999%_ or even 6 9" s availability (99.9999%). **(5 9's is a downtime of 5.26 minutes per year, while 6 9's is a downtime of 31.56 seconds per year).**

Which is why I've created a separate subcomponent cost centre to draw attention to all the above.

My strategy is to leverage the desire for governments to create a new legal identity framework, by raising the red flag about electricity. I can see in my head governments acknowledging this, by incrementally funding changes to their existing grid networks.

The place to start is by ensuring government data centres holding vital legal data, like the CRVS are fully protected from EMP/HEMP events and have sustainable power supplies. I can also see how CRVS licensing agreements can raise these issues as part of the licensing discussions/agreements.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS EMP/HEMP Protection/Power Supply Subcomponent Cost Centre
- CRVS Data Centre Electrical Supply Plan/Processes Subcomponent Cost Centre
- CRVS Non-Profit - Manages EMP/HEMP Protection/Power Supply Subcomponent Cost
- Learning Non-Profit EMP/HEMP Protection/Power Supply Subcomponent Costs

Non-Profit - EMP/HEMP Protection/Power Supply Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - EMP/HEMP experts
  - Data centre/cloud experts
  - Electrical grid experts
  - CRVS experts
  - SOLICT experts (database plus legal)
  - Smart digital identity experts
  - AI systems and bots experts
  - Legal experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Notary experts
  - Learning non-profit EMP/HEMP experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - Protecting CRVS, SOLICT, LDV and Learning Non-Profit data centres
  - Upgrading jurisdiction's electrical grid
  - Reducing power consumption from AI systems
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots for 1-3 CRVS jurisdictions
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre:

Background:

There are five trends I see affecting power consumption:

1. Global warming affecting cheap availability of power
2. This AI power consumption curve depicted in Figure 1 of "AI Power Consumption Exploding" which shows by 2040-ish AI will be consuming most of the planet's power
3. Every legal entity on the planet leveraging their LSSI devices, many of which will consume power
4. Every person on the planet leveraging AI enabled PIAM's (Personal Identity & Access Management) systems which will consume power
5. Every legal entity on the planet having their own SOLICT database which will consume power

Thus, that's why I've broken it out as a separate cost centre which the non-profit keeps focussing on to deliver power friendly ways of delivering the architecture.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Data Centre Electrical Supply/Consumption Plan & Processes Subcomponent Cost Centre
- CRVS EMP/HEMP Protection/Power Supply Subcomponent Cost Centre
- CRVS Non-Profit - Manages EMP/HEMP Protection/Power Supply Subcomponent Cost
- SOLICT Data Centre Subcomponent Cost Centre
- LSSI Devices Power Consumption Subcomponent Cost Centre
- PIAM Power Consumption Subcomponent Cost Centre
- Learning Non-Profit – Power Consumption Of LDV, DLT and Learning Assessments Subcomponent Cost Centre

Very Important Note:

The Learning Non-Profit is undergoing a similar exercise re power consumption of LDV, DLT, and Learning Assessment Devices. Thus, my suggestion is to combine the two costs centres, at least in the early years, to leverage resources, expertise, and budgets. Which is why costs associated with the Learning Non-Profit's cost centre are borne by this cost centre.

Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Supply Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Power consumption experts
  - Data centre/cloud experts
  - CRVS experts
  - SOLICT experts (database plus legal)
  - LSSI device experts
  - PIAM experts
  - Smart digital identity experts
  - AI systems and bots experts
  - LDV experts
  - DLT experts
  - Learning Assessment experts
  - Legal experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Co-design experts
  - Notary experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - Reducing power consumption and associated costs from:
    - CRVS data centres
    - SOLICT databases
    - LSSI devices
    - PIAM
    - AI/bot legal entities
    - LDV
    - DLT
    - Learning Assessments
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Licenses CRVS System to Jurisdictions & Credential Issuance Standards to Credential Bodies Subcomponent Cost Centre:

Background:

Of all the cost centres within this long document, this one is the most critical. Why? Politics.

There are two major challenges national government face in designing and deploying the new legal identity and credential learning architectures:

1. Rapidly getting their local state/provincial CRVS jurisdictions to politically buy into rethinking their existing CRVS systems
2. Funding the new non-profit such that it has very significant funds to continually invest in latest super computers, etc., to continually defend against the Evil Inc.'s and malicious states

Local states/provinces are very territorial. How can this be done?

Subsidies To Local State/Provincial CRVS Jurisdictions:

The federal government will have to pay for the local state/province to rapidly buy-in to and convert their old CRVS systems to the new one. By offering to do this, the feds can rapidly get the local CRVS jurisdictions to quickly come to the table, buying into the design, POC, pilot and implementation phases.

Licensing The New CRVS System At A Very Low Cost:

The architecture solution framework proposes licensing the CRVS system to jurisdictions based on a very small charge per CRVS event up to a yearly maximum amount. It also proposes licensing credential issuance standards to credential bodies on a very small charge per credential issued. My goal was to annually fund the non-profit more than $1 billion a year.

Why so much? The non-profit MUST have continual access to the best supercomputers, tech, resources and expertise on the planet.

IT'S VERY POLITICAL:

It requires great tactful political skill in creating the first subsidies and licensing agreements. The team doing this must be able to model future non-profit costs versus rapid growth in legal registration identities of AI systems and bots, with accompanying credentials and potential licensing revenue streams.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Non-Profit - Licenses CRVS System to Jurisdictions & Credential Issuance To Credential Bodies Subcomponent Cost Centre

Subsidies To Convert Old CRVS To New Standards Subcomponent Costs:

VERY IMPORTANT NOTE:

The actual subsidy costs, per local jurisdiction will be high i.e., likely on the order of hundreds of millions of dollars. Until the system is under design, realistic budgeting costs can't be determined. Depending on the number of local CRVS state/provincial jurisdictions involved, it will significantly increase the total budget. For the purposes of the budget guesstimates in the Excel spreadsheet, I've used a low of $500 million to a high of $800 million per local state/provincial jurisdiction, with an assumption of 13 jurisdictions to start with

Non-Profit - Licenses CRVS System to Jurisdictions & Credential issuance Standards to Credential Bodies Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Finance experts
  - Legal experts
  - Political experts
  - CRVS experts
  - Credential bodies experts
  - SOLICT experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Co-design experts
  - Notary experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - License agreements with jurisdictions
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre:

Background:

The Legal Identity Hive Relationship cost centre section of this document dives deep into the fast-emerging new waters of legal identity hive relationships. It discusses leveraging both TODA capability files and graphs to begin to solve the challenges (skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**)". The tech change curve dramatically and continually alters how hive relationships are created, maintained, terminated, etc.

The global, independent non-profit MUST create, maintain, and rapidly update legal identity hive relationship standards. I feel they'll likely be bombarded with increasing demands from industry to rapidly change the standards (which may or may not be a good idea). THUS, THIS TOO, LIKE OTHER PARTS OF THE NON-PROFIT, IS VERY POLITICAL

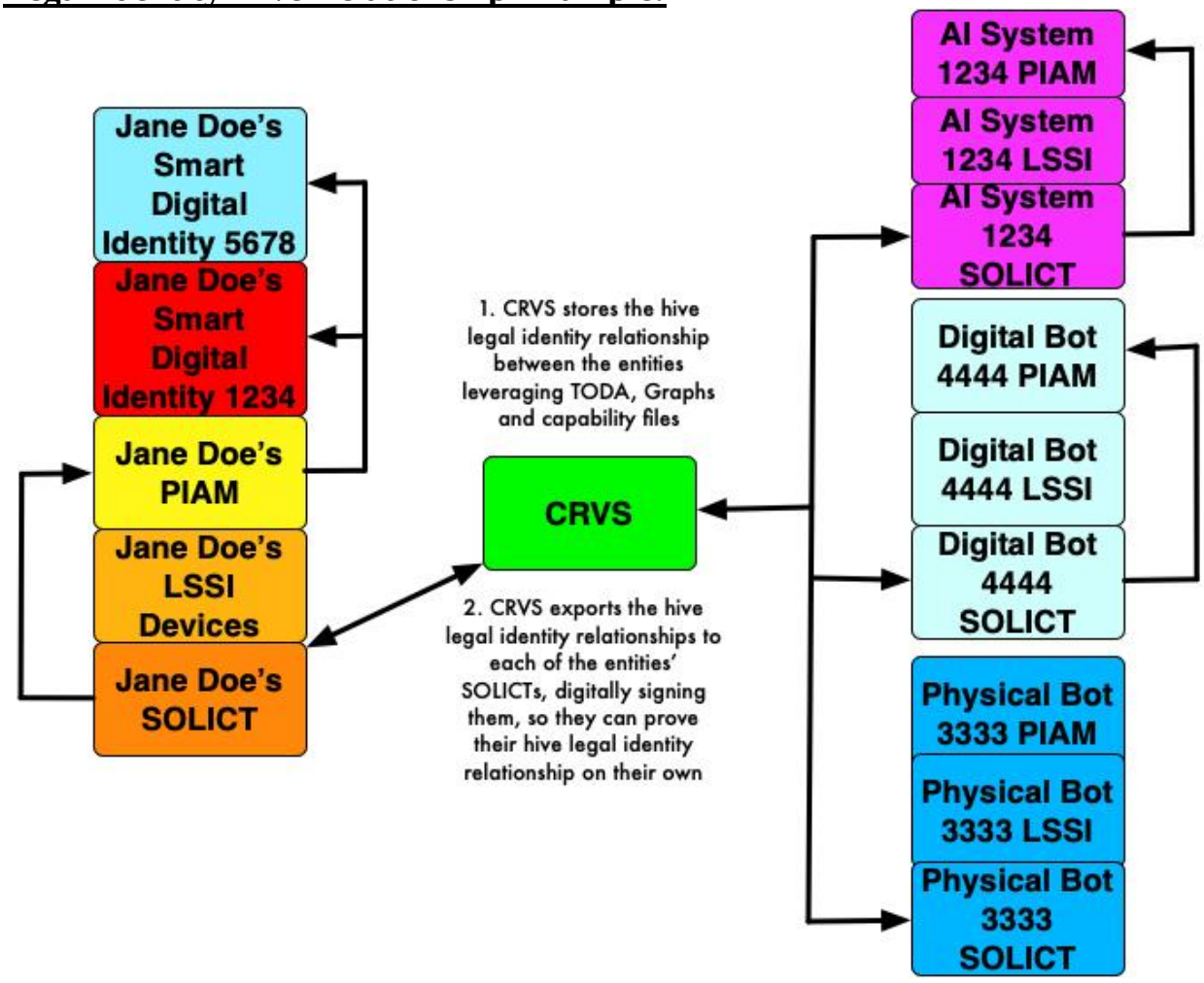
Finally, all citizens, regardless of their abilities or disabilities, must understand:

- What legal identity/hive relationships are
- Be able to release portions of them to third parties via their LSSI devices or PIAM

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS - Legal Identity Hive Relationship Standards Subcomponent Costs
- Legal Identity Hive Relationship Standards Subcomponent Cost Centre
- Smart Digital Identities Legal Identity Relationships (Including Hives) Subcomponent Cost Centre
- AI/Bots Legal Identity & Hive Relationships Subcomponent Cost Centre
- CRVS Governance - Standards for Legal Identity/Hive Relationships Stored Within the CRVS Subcomponent Cost Centre
- CRVS Non-Profit Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre
- Legal Identity & Hive Relationships - Authoritative Entity Data Source – CRVS Subcomponent Cost Centre
- Legal Identity & Hive Relationships - Graph Databases Store Relationships Cross-Linking Between Different Entities Subcomponent Cost Centre
- SOLICT Authoritative Legal Identity, Credential, Legal Identity Relationships/Hive and Authorization Rights Sources Subcomponent Cost Centre
- Learners, Teachers, Bots Legal Identity, Relationships/Hives, Legal Authorization Rights and Credentials Subcomponent Cost Centre
- Legal Authorization Rights - Co-Design Driven Standards For Accessing Legal Authorization Rights Cost Centre

Legal Identity Hive Relationship Example:



Manages Legal Identity Hive Relationships Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Legal relationship experts
  - Political experts
  - CRVS experts
  - SOLICT experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Co-design experts
  - Notary experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - Legal identity relationship including hive relationships
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre:

Background:

The Authorization Cost Centre section of this document addresses the growing need for an entity to have legal authorization with abilities to delegate section of it to other entities. It discusses leveraging TODA capability files to begin to solve the challenges (skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age)**".

As stated in the last section, all I can see in my head is Pat Scannell's tech change curve dramatically and continually altering how legal authorization rights for literally trillions of entities is managed. YIKES!!!! Which brings me to standards.

The global, independent non-profit MUST create, maintain, and rapidly update legal authorization standards. I feel they'll likely be bombarded with increasing demands from industry to rapidly change the standards (which may or may not be a good idea). **THUS, THIS TOO, LIKE OTHER PARTS OF THE NON-PROFIT, IS VERY POLITICAL**

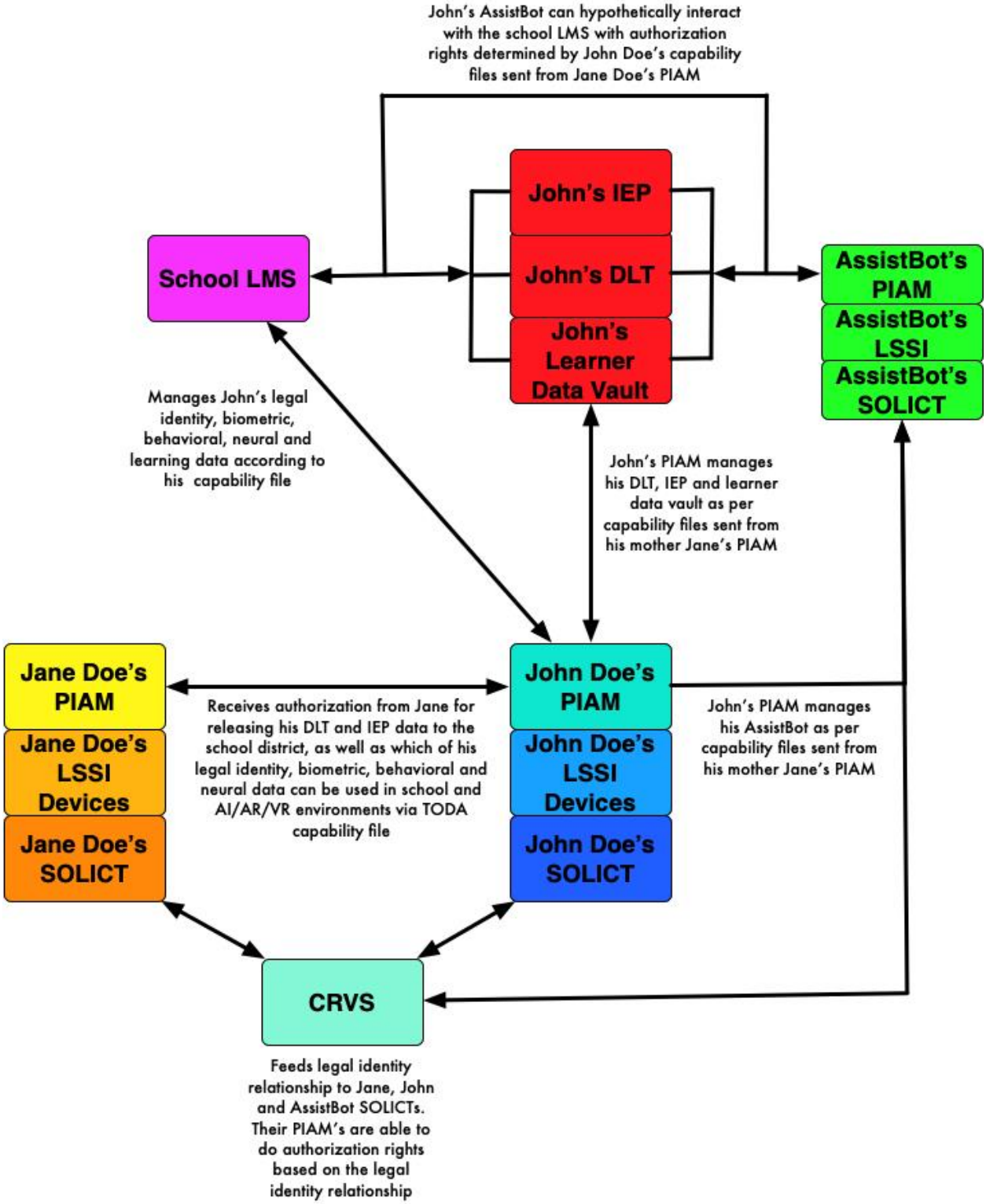
Thus, my advice is to keep the scope limited on authorization rights to only legal identity authorization rights pertaining to what sections of the entity's legal identity can be delegated and managed by others.

Note: How the citizen understands and delegates these rights will be managed by the co-design team.

Cost Centres Dependent Upon This Cost Centre:

- Smart Digital Identities Legal Authorization Rights Subcomponent Costs
- Legal Authorization Standards Subcomponent Cost Centre
- AI/Bots Legal Authorization Rights Subcomponent Cost Centre
- CRVS Governance - Standards for Legal Authorization Issued by the CRVS Subcomponent Cost Centre
- CRVS Non-Profit - Manages Legal Authorization Standards Subcomponent Cost Centre
- Legal Authorization Rights - Transmission of TODA Authorization Capability File to SOLICT Subcomponent Cost Centre
- SOLICT Authoritative Legal Identity, Credential, Legal Identity Relationships/Hive and Authorization Rights Sources Subcomponent Cost Centre
- Learners, Teachers, Bots Legal Identity, Relationships/Hives, Legal Authorization Rights and Credentials Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Authorization Rights Example:



Very Important Note:

The legal identity and hive relationship team is managing legal identity relationships while this team is managing legal authorization rights. My suggestion is to combine the two teams, leveraging expertise and resources while reducing costs. This version of the Excel spreadsheet DOES NOT DO THIS. If it makes sense to do this the cost savings will be on the order of between $60-100 million over three years.

Manages Legal Authorization Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Legal identity authorization experts
  - Political experts
  - CRVS experts
  - SOLICT experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Notary experts
  - Co-design experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - Legal identity authorization
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre:

Background:

The Credentials Issuing Source Cost Centre section of this document discusses the complex world of tens of thousands of credential bodies on the planet, each issuing their own credentials to humans. Here's the challenges:

- There are no global standards for credentials, which works locally and globally, physically, and digitally
- There are no global standards for creating credentials for AI systems and bots

Skim "**Verifiable Credentials For Humans and AI Systems/Bots**".

The political challenges in having to deal with thousands of credential bodies is yet another hill one can die upon. So, when architecting the solution framework, I wanted to keep the credential bodies mostly in control of their credential processes. HOWEVER, what I wanted to do is to get them to adopt new, global standards on credential issuance. They're still left in control, but now use the same architecture for issuing credentials.

Pat Scannell's tech change curve means, hypothetically, each hour, new attack vectors are being created against the credential issuance architecture. Thus, I wanted the new, global, independent non-profit to set credential issuance standards, and then keep them up to date with 24x7x365 threat analysis.

Thus, the architectural solution framework has the non-profit establishing credential issuance standards. This includes:

- Data standards for the credentials
- Digital signatures required by the credential issuing body
- TODA file used to deliver the credentials to the entity's SOLICT
- End-point DNS, encryption, security, etc.
- Consent agreements between the credential issuing body and the entity for delivery of the credential
- Co-design such that a user can understand:
    - What credentials they have are
    - How to release them to third parties via their LSSI devices and/or their PIAM

Other Cost Centres Dependent Upon This Cost Centre:

- Smart Digital Identities Authoritative Credentials Source Subcomponent Cost Centre
- Authoritative AI Systems Bots Credential Sources Subcomponent Cost Centre
- Credentials Issuing Standards Subcomponent Cost Centre
- CRVS Non-Profit - Manages Credential Issuance Standards Subcomponent Cost Centre
- SOLICT Authoritative Legal Identity, Credential, Legal Identity Relationships/Hive and Authorization Rights Sources Subcomponent Cost Centre
- PIAM –Authoritative Data Source SOLICT Subcomponent Cost Centre
- Notaries – Credential Issuing Authorities Subcomponent Costs
- Learners, Teachers, Bots Legal Identity, Relationships/Hives, Legal Authorization Rights and Credentials Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:
- Local/Global Legal Identity, Credentials and Notary Framework Subcomponent Cost Centre
- Credential Co-Design Abilities to Use Credentials Subcomponent Cost Centre
- Learning Non-Profit Learning Competencies/Credentials Subcomponent Cost Centre

Note: This cost centre bears the costs of the Learning Non-Profit's Competencies/Credentials Cost Centre

Manages Credential Issuance Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Credential experts
  - Political experts
  - SOLICT experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - Business process experts
  - Red team experts
  - Standards experts
  - API experts
  - Network/connectivity experts
  - Co-design experts
  - Notary experts
  - Learning experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - Credential issuance to entities
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, adjust and rapidly scale around the planet

Non-Profit – Manages SOLICT Standards Subcomponent Cost Centre:

Background:

The SOLICT Cost Centre section of this document lays out the complexity of providing each entity they're own SOLICT. To see some of the coming complexities:

- Skim "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**". Does each of the nanobots in Jane Doe's body require their own SOLICT?
- What type of standards and business processes need to be in place when a malicious state changes Jane Doe's entry within their CRVS to dead but Jane's alive and well?
- What type of consent data standards are required to input the thousands of consent agreements into an entity's SOLICT?
- What are the management standards used for the non-profit to manage all entity's SOLICTS on the planet without having abilities to see into them?
- What are the standards for keeping the SOLICT databases secure?
- What is the standard for a SOLICT?
- How will standards be immediately updated when a high threat risk is found for a SOLICT?
-

As one can see, it's very, very complicated. Thus:

- THE ACTUAL SOLICT STANDARD MUST BE BASED ON A WIDE VARIETY OF USE CASES
- AS MUST BUSINESS PROCESS AND SECURITY STANDARDS RE SOLICT BE BASED ON A WIDE VARIETY OF USE CASES

Note:

1. **Not quite three years ago, I wrote "A Database Per Entity on the Planet - A Deeper Dive on SOLICT". I haven't found time to update it re legal hive relationships and authorization rights for humans, AI systems and bots. So, with this caveat, it's an excellent background read for the SOLICT standards team.**
2. **As importantly is educating all citizens on the planet what their SOLICT is. how it works and how they can interact with it. This is where the co-design team comes into play.**

Other Cost Centres Dependent Upon This Cost Centre:

- Smart Digital Identities SOLICT Subcomponent Cost Centre
- SOLICT Data Standards Subcomponent Cost Centre
- CRVS Governance - Ability for CRVS to Send Legal Identity Information to the SOLICT via TODA Subcomponent Cost Centre
- CRVS Non-Profit - Manages SOLICT Standards Subcomponent Cost Centre
- Credential Standards SOLICT (Source of Legal Identity & Credential Truth) Subcomponent Cost Centre
- Legal Identity & Hive Relationships - Transfer to SOLICT (Source of Legal Identity & Credential Truth) Via Digitally Signed TODA File Subcomponent Cost Centre

- SOLICT Business Processes Subcomponent Cost Centre
- SOLICT Consent Standards/Agreements/Contracts Subcomponent Cost Centre
- PIAM –Authoritative Data Source SOLICT Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships - SOLICT Stores Legal Identity/Hive Relationship Subcomponent Cost Centre
- CRVS - Transmission of TODA Legal Authorization Capability File to SOLICT Subcomponent Cost Centre
- Legal Authorization Rights - Transmission of TODA Authorization Capability File to SOLICT Subcomponent Cost Centre
- LSSI Device Interfaces/Updating from SOLICT
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Manages SOLICT Standards Subcomponent Costs:

Note: It's highly likely this standards group should also be part of the SOLICT Governance – Laws, Regulations & Management Subcomponent Cost Centre.

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - SOLICT experts
  - CRVS experts
  - Credential experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - Business process experts
  - Security/red team experts
  - Standards experts
  - Network/connectivity expert
  - Database experts
  - Cloud experts
  - Political experts
  - Lesson learnt experts
  - Notary experts
  - Co-design experts
- Create high level requirements, use cases, and cost estimates for:
  - SOLICT standards
  - SOLICT database standards
  - SOLICT standards for business processes
  - Etc.
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Manages SOLICT Databases Subcomponent Cost Centre:

Background:

When creating the new legal identity framework, I wanted to architect it such that a malicious state couldn't delete all identity records for an identity. When Scott David, University of Washington, gave me the idea of creating, for each person, a separate database, which they can control, that exists in the cloud, outside of a jurisdiction's reach, I realized this was the solution I'd been looking for. **YET, THERE'S A BIG BUT WHICH COMES WITH IT. WHO PAYS FOR, RUNS AND SECURELY MANAGES THE LIKELY TRILLIONS OF SOLICT DATABASES?**

I figured out a way for the global, independent, non-profit to fund it via licensing (see the prior cost section). It's the performance and security which most concerns me. Which is why I've broken this database management cost sub-section on its own.

As stated in the SOLICT Cost Centre section of this document:

Security Challenges – Performance & Security

SOLICT will become key to entities wanting to write to the SOLICT, interactions with an entity's LSSI (legal self-sovereign identity) devices and their PIAM (personal identity access management) system.

Performance:

I could see in my mind the awesome speeds at which say digital bots can be created. Over time, it could easily be in the millions or billions per second/. Thus, I saw the CRVS local/global systems struggling not only with registration/validation performance, BUT ALSO CREATING A SOLICT FOR EACH NEW ENTITY. Thus, this must be addressed in design use cases.

Security:

I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks against the new age CRVS systems. They could effectively "drown the CRVS" with creations of new entities and sending out to the global, independent non-profit, who's managing the SOLICTS, LOTS of SOLICT creations. Thus, this must be addressed in design use cases.

Updating:

I could also see the business process problems of keeping track of trillions or more AI system and bots legal identities. How would the CRVS be able to be notified an entity had changed, been adopted into another entity, terminated, etc. and then how would it notify the entity's SOLICT?
%
Then there's the high availability of the end-to-end SOLICT system. Updates must be made live with little or no downtime i.e. 5'9's or 6'9's (99.999-99.9999% availability).

All of the above must be addressed in design use cases.

Then there's the issue of the actual underlying database. As described in "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**", I can see graph databases being used to map the many, fast changing, legal identity hive relationships. **Yet, a question in my mind is can graphs perform at these very fast, very high-volume speeds and loads? TODA can but I'm not sure of graphs.**

Add to this the overall security framework for the graph databases. **How can say Jane Doe be sure her SOLICT data isn't being seen or worse, modified by the global, non-profit's analysts, AI systems, bot or management?**

Finally, the SOLICT is the key architectural performance linchpin for an entity operating second-by-second in today's world. **How will the underlying data centres, clouds, etc. be managed to be available at a minimum of 5 9's (99.999%) or even 6 9's (99.9999%)? (**5 9's is a downtime of 5.26 minutes per year, while 6 9's is a downtime of 31.56 seconds per year**).**

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Legal Identity & Hive Relationships - SOLICT Stores Legal Identity/Hive Relationship Subcomponent Cost Centre
- SOLICT Database Application Subcomponent Cost Centre
- CRVS Non-Profit - Manages SOLICT Databases Subcomponent Cost Centre
- SOLICT Data Centre Subcomponent Cost Centre
- SOLICT Database Application Subcomponent Cost Centre
- SOLICT Infrastructure Updating Subcomponent Cost Centre
- Learning Non-Profit Manages LDV Databases Subcomponent Cost Centre

VERY IMPORTANT NOTE:

This cost centre will be responsible for billions of SOLICT databases. In the Learning Non-Profit, it will be responsible for billions of LDV databases. Thus, here's my suggestion…

Rather than initially have each non-profit figuring out how to cost effectively and securely operate billions of databases, it makes much more sense, in the early days, for the two non-profits to leverage resources, expertise and costs, by creating them together. As lessons are learnt, then after 2-3 years, the two non-profits may decide to split operation of the two or, continue on. Thus, this cost centre is responsible for both the SOLICT and LDV database cost centres.

Manages SOLICT Databases Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - SOLICT experts
  - PIAM experts
  - CRVS experts
  - API experts
  - Credential experts
  - Smart digital identity experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - LDV experts
  - Consent standards experts
  - Business process experts
  - Security/red team experts
  - Standards experts
  - Network/connectivity expert
  - Database experts
  - Cloud experts
  - Political experts
  - Notary experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - SOLICT databases
  - SOLICT data centres
  - SOLICT security
  - LDV databases
  - LDV data centres
  - LDV security.
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit – Manages LSSI Standards Subcomponent Cost Centre:

Background:

In the LSSI Devises Cost Centre section of this document, it describes the five different types of LSSI devices:

- Physical, smart legal identity
- Legal identity application
- Physical, wristband, containing the legal identity/credential information, biometrically tied to the wearer
- A chip implanted into the entity
- Writing legal identity and credential information to the source code of an entity

Given Pat Scannell's tech change curve, it likely means these LSSI devices will rapidly change. As well, it also hypothetically means each hour, day or week, new security attacks against the LSSI devices will be created.

All of which comes to bear in LSSI device standards. As the non-profit threat centre detects new types of attacks, depending on risk, the LSSI device standard might be required to rapidly change.

Finally, its highly probable that companies will mass produce some types of LSSI devices for consumers to buy. Thus, from a security and entity user perspective, it requires standards addressing the following:

- TODA file transfer from the SOLICT to the LSSI devices
- LSSI device standards
- LSSI device security standards
- PIAM interfacing with LSSI device standards
- API standards addressing the above
- **AND MOST IMPORTANTLY CO-DESIGN FOR EACH OF THE LSSI DEVICES SUCH THAT ALL CITIZENS CAN KNOWLEDGABLY USE THEM**

Other Cost Centres Dependent Upon This Cost Centre:

- Smart Digital Identities TODA LSSI Devices (Legal Self-Sovereign Identity) Subcomponent Costs:
- LSSI Devices Standards Subcomponent Cost Centre
- CRVS Non-Profit - Manages LSSI Devices Standards Subcomponent Cost Centre
- Credential Standards LSSI (Legal Self-Sovereign Identity) Subcomponent Cost Centre
- Legal Identity & Hive Relationships - SOLICT to LSSI (Legal Self Sovereign Identity) Devices Via TODA File Subcomponent Cost Centre
- SOLICT Pushes Out Authorization Rights to LSSI Devices via TODA Capability File Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships - SOLICT to LSSI Devices Via TODA Files/LSSI Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Non-Profit LSSI Standards - Legal Physical ID Cards Subcomponent Costs:

Background:

In today's smart card world, there's a limit to the amount of data the card can hold. This might be limitations when wanting to write LSSI files to them. The challenge with LSSI, over time, not overnight, is the amount of data will likely increase as one has different credentials. Each LSSI entry will also likely require a digital signature issued by the local authority. Thus, consideration must be given to thinking of producing a very small, secure LSSI database on the card or, devising an alternate solution allowing for secure data scaling on the card, to common global LSSI standards.

The current legal ID cards typically have a face image and/or name type data on the front of them. It limits the ability of a person to prove they're a human legally, anonymously and/or above age of consent

There are limited abilities for a person to provide their consent. How will a person provide their consent? Can voice be used on physical cards? How will the card and third party know where to securely send the consent to the person's SOLICT URL address?

Then there's the issues of how legal identity delegation will occur for two people and their LSSI physical legal ID cards e.g., a parent and child. How will this work? Each person's TODA capability LSSI files will need to be present on the devices with appropriate processes allowing say a parent to control their child's physical LSSI ID card.

The rapid tech changes caused by this curve, mean that new attack vector is being rapidly created. Thus, the physical ID cards must be continually assessed by the global, non-profit with continuous threat assessments being issued.

Finally, practical things like a person acquiring a new credential, vaccination, changing them, etc. requires rapid update processes to the card.

All of these are design factors in implementing LSSI on to existing legal ID physical cards. It might require design teams to accept limitations in the short term to get rapid adoption or, to issue new legal ID cards to people having capabilities addressing the above. All these factors affect costs.

Other Cost Centres Dependent Upon This Cost Centre:

- LSSI - Legal Physical ID Cards Subcomponent Costs
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Non-Profit LSSI Standards - Legal Physical ID Cards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for creating LSSI physical ID cards
    - The team should include the following types of people:
      - ID Smart card experts
      - Security and red team experts
      - Database experts
      - ID smart card standards experts
      - Business process experts
      - Legal experts
      - Co-design experts
      - Notary experts
      - Lessons learnt experts
- Start with:
  - Assessment of the current ID smart card landscape
  - Create use cases for physical LSSI cards
  - Determine a strategic approach i.e., determine if in the short-term accepting current card limitations is acceptable or not. If not, then create the strategy for rolling out a new LSSI physical ID card
  - For this, develop cost estimates
- Then do a series of rapid POC's, proving out the use cases
- Then do a small, controlled pilot it in 1-3 jurisdictions expanding the team
- Transition management of this to the global, independent, non-profit

Non-Profit LSSI Standards - Digital LSSI App Subcomponent Costs:

Background:

In today's world, there's some common standards for things like digital driver's licenses, passports et al. I can see a need for a Digital LSSI app, which applies to:

- Young children through to very old people i.e., cradle to grave
- Entity creation to termination

This app will allow for use of Toda LSSI file being written to it or, to a small LSSI database within the app, or connecting through to an entity's SOLICT.

Then there's the way the entity will grant consent to a third party to release their legal identity and credential data to. Hypothetically, in addition to typical consent buttons, for humans, different types of biometric and behavioral factors could be used to provide consent.

Then there's the issues of how legal identity delegation will occur for two people and their LSSI Digital LSSI apps e.g., a parent and child. How will this work? Each person's TODA capability LSSI files will need to be present on the devices with appropriate processes allowing say a parent to control their child's legal identity LSSI app.

The rapid tech changes caused by this curve - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf, mean that new attack vector are being rapidly created. Thus, the Digital LSSI app must be continually assessed by the global, non-profit with continuous threat assessments being issued.

Finally, practical things like a person acquiring a new credential, vaccination, changing them, etc. requires rapid update processes to the card. As well, changes caused by the curve might require digital LLSI app updating.

All of these are design factors in implementing LSSI on to existing digital legal identity apps. It might require design teams to accept limitations in the short term to get rapid adoption or, to issue new legal identity LSSI apps to people having capabilities addressing the above. All these factors affect costs.

Other Cost Centres Dependent Upon This Cost Centre:

- LSSI - Digital LSSI App Subcomponent Costs
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Non-Profit LSSI Standards - Digital LSSI App Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for creating a LSSI digital app
    - The team should include the following types of people:
      - ID digital app experts
      - Security and red team experts
      - Database experts
      - ID digital app standards experts
      - Business process experts
      - Co-design experts
      - Notary experts
      - Legal experts
- Start with:
  - Assessment of the current legal digital identity app landscape
  - Create use cases for digital LSSI app
  - Determine a strategic approach i.e., determine if in the short-term accepting current card digital legal apps is acceptable or not. If not, then create the strategy for rolling out a new LSSI digital app
  - For this, develop cost estimates
- Then do a series of rapid POC's, proving out the use cases
- Then do a small, controlled pilot it in 1-3 jurisdictions expanding the team
- Transition management of this to the global, independent, non-profit

Non-Profit LSSI Standards - Biometrically Tied LSSI ID Wristband Subcomponent Cost Centre:

Background:

Billions of people around the planet don't have access to tech or, are unable to use it. They all require LSSIT capabilities to use in their life. The requirements are it must be:

- Made of a durable material able to withstand lots of physical abuse
- Able to function after being dropped in dirt, mud, urine and feces
- Washable by hand or machine
- Able to function in hot, cold, dry, or wet environments
- Biometrically linked to the wearer
- Color differentiated allowing people to recognize which is their wristband
- Updateable via some form of wireless API
- Have enough memory to contain legal identity and credential data
- Low cost

Of all the LSSI devices subcomponent cost centres, I think this will be the toughest one to figure out and create.

Other Cost Centres Dependent Upon This Cost Centre:

- LSSI - Biometrically Tied LSSI ID Wristband Subcomponent Costs
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Non-Profit LSSI Standards - Biometrically Tied LSSI ID Wristband Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for creating a LSSI digital app
    - The team should include the following types of people:
      - Smart textile experts
      - Smart wristband experts
      - TODA experts
      - Security and red team experts
      - Business process experts
      - Legal experts
      - NFC experts
      - Connectivity experts
      - AI consent experts
      - Voice command experts
      - Behavioral experts
      - Biometric experts
      - Co-design experts
      - Notary experts
      - Lessons learnt experts
- Start with:
  - Assessment of the current legal digital identity app landscape
  - Create use cases for digital LSSI app
  - Determine a strategic approach i.e., determine if in the short-term accepting current card digital legal apps is acceptable or not. If not, then create the strategy for rolling out a new LSSI digital app
  - For this, develop cost estimates
- Then do a series of rapid POC's, proving out the use cases
- Then do a small, controlled pilot it in 1-3 jurisdictions
- Transition management of this to the global, independent, non-profit and other standards bodies who might be responsible for LSSI digital app

Non-Profit LSSI Standards - Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs:

Background:

The speed of this curve, means the technology is rapidly evolving resulting in creation of the hypothetical possibility of inserting chips into people containing their TODA LSSI file. This concept is typically met in older people with disdain, fear, and mistrust, while younger people are more open to it. Scientific, legal and privacy research is required for this.

Other Cost Centres Dependent Upon This:

- LSSI - Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Non-Profit LSSI Standards - Chips Inserted Into People Containing Their LSSI Information Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of research experts to lay out high-level deliverables and create the first use cases for creating an insertable chip
    - The team should include the following types of people:
      - Researchers /medical experts who've done work on chips inserted into people
      - Security and red team experts
      - LSSI experts
      - Database experts
      - Legal experts
      - Ethics/privacy experts
      - Business process experts
      - Co-design experts
      - Notary experts
      - Lessons learnt experts
  - Start with:
    - Assessment of the current insertable chip landscape both from a research perspective as well as existing deployments
    - Create use cases for insertable LSSI chip
    - Determine a strategic approach i.e., determine if it's ethically, legally and technically feasible to impellent LSSI chips into people
    - If it is determined to be feasible, then move to the second stage of funding
      - Flesh out the use cases
      - Then do a series of rapid POC's, proving out the use cases
      - Then do a small, controlled pilot it in 1-3 jurisdictions expanding the team and then rapidly scale

Non-Profit LSSI Standards - Writing LSSI Information to an Entity's Source Code Subcomponent Costs:

Background:

The explosion of AI systems, bots and AI leveraged, smart digital identities of humans require the ability to write LSSI information to the source code. This is the same challenge facing CRVS design of writing legal identity information to the entity's source code.

Other Cost Centres Dependent Upon This:

- LSSI - Writing LSSI Information to an Entity's Source Code Subcomponent Costs

Non-Profit LSSI Standards - Writing LSSI Information to an Entity's Source Code Subcomponent Costs:

This cost centre will be borne by the AI/Bots Writing to Source Code Legal Identity/Credential Registration Subcomponent Costs section of this document.

Non-Profit – Manages PIAM Standards Subcomponent Cost Centre:

Background:

The PIAM Cost Centre of this document, lays out how PIAMs will become the focus of companies wanting to sell to the customer because it puts them closest to the customer. It also discusses how Jane Doe leverages it in her daily life (skim "**An Identity Day in the Life of Jane Doe**"). Thus, I can see LOTS of commercial industry interest in PIAM standards.

Then there's Pat Scannell's tech change curve to consider with PIAMs. As the API's and PIAM's are the electronic front door to an entity, they become primate targets by the Evil Inc's and malicious states of the planet. Thus, any PIAM standard must be continually updated by the non-profit threat analysis.

Also, there's the PIAM AI power consumption to consider. Look at Figure 1 in "**AI Power Consumption Exploding**". It shows, if current AI power consumption trends continue, by 2040-ish AI will be consuming most of the planet's power supply.

Then consider the PIAM. Each person on the planet will have one i.e., there will literally be billions of these. Thus, it becomes imperative to create a PIAM will very low power consumption requirements. Skim "**Decentralized AI – Risks, Legal Identity, Consent & Privacy**" to see a possible strategy addressing this.

Equally important is creating interfaces such that all citizens on the planet, regardless of their abilities or disabilities ae able to knowledgably use their PIAM. Note: The education of the citizen by the co-design team must not "tell" the citizen what to do. This is outside the bounds of the deliverables. Instead, it must educate the citizen as to the risks and then let the citizen decide, assisting them with release of their legal identity and credential information.

All of which comes down to having a robust set of PIAM standards, with the ability to update them hourly, daily, weekly, etc. as and when required. That's what this cost centre delivers.

Other Cost Centres Dependent Upon This Cost Centre:

- Smart Digital Identities PIAM (Personal Identity Access Management) Subcomponent Costs
- CRVS Non-Profit - Manages PIAM Standards Subcomponent Cost Centre
- Credential Standards PIAM (Personal Identity Access Management) Subcomponent Cost Centre

- Legal Identity & Hive Relationships - PIAM (Personal Identity Access Management) Consent Agreements/Contracts With Third Parties Subcomponent Cost Centre
- Legal Authorization Rights - PIAM Manages Authorization Rights With Other Entities Subcomponent Cost Centre
- LSSI Device PIAM Management Subcomponent Cost Centre
- PIAM Standards Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:

Manages PIAM Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - PIAM experts
  - LSSI device experts
  - SOLICT experts
  - CRVS experts
  - API experts
  - Credential experts
  - Co-design experts
  - Smart digital identity experts
  - Industry experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - Consent standards experts
  - Business process experts
  - Security/red team experts
  - Standards experts
  - Network/connectivity expert
  - Database experts
  - Cloud experts
  - Political experts
  - Lesson learnt experts
  - AI power consumption experts
  - Notary experts
  - Global power consumption experts
- Create high level requirements, use cases, and cost estimates for:
  - PIAM standards and PIAM energy consumption
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit - Manages Notary Standards For Legal Identity & Credentials Subcomponent Cost Centre:

Cost Centres Dependent Upon This Cost Centre:

- Rethought Notaries Governance Laws/Regulations Subcomponent Costs
- Rethought Notaries Human Co-Design Interfaces Subcomponent Costs
- Rethought Notaries- Legal Identity & Credential Verification Certification Process Subcomponent Costs
- Notary - Digitally Sign Attestations/Contracts Subcomponent Costs
- Local/Global Legal Identity, Credentials and Notary Framework Subcomponent Cost Centre

Background:

As stated in "Cost Centre: Rethought Notaries" section of this document:

> "I like the concept of notaries, since they're independent of government, acting as a go-between between governments and citizens in proving their legal identities. Thus, I've included rethought notaries in the architecture.
>
> The place to start is by rethinking how they verify entities identities. In today's planet, this can be very challenging, since a person, their smart digital version of them, or an AI system or bot, might be interacting digitally with a local notary, from the other side of the planet.
>
> Another challenge is Jane Doe fleeing Jurisdiction X to Jurisdiction Y because the government deleted her CRVS record and any other government identity database of her. I could see Jane going to a local notary in Jurisdiction Y and, with her consent, giving her legal identity information plus her forensic biometrics, and the notary able to do a single search on the CRVS system to prove she's Jane Doe. When the search turns negative, the notary can search her SOLICT to see a special digital signature the CRVS signed when creating her SOLICT entry. They'd be able to decrypt it this confirming it's Jane Doe. They could then create a physical and digital attestation she's Jane.
>
> Yet another challenge with notaries is their being able to work with citizens of all abilities and disabilities. Thus, I could see co-design assisting notaries in their work with all citizens re legal identity and credential proofing.
>
> As with the rest of this architecture, it's visionary. I don't want to try to sell the planet on what a wonderful idea it is. Instead, my strategy is to find innovative funders, with 1-3 jurisdictions, with a willing business and notary community, to rethink notaries in small steps. That's what the cost centres call out for. Then, once we've figured it out in real life, rapidly scale."

Non-Profit - Manages Notary Standards For Legal Identity & Credentials Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Notary experts
  - PIAM experts
  - LSSI device experts
  - SOLICT experts
  - CRVS experts
  - Smart digital identity experts
  - Red team experts
  - Security experts
  - Legal authorization experts
  - Co-design experts
  - API experts
  - Notary governance experts
  - Legal experts
  - Industry experts
  - AI systems and bots experts
  - Human legal identity relationship experts
  - Consent standards experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Political experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - Notary digital signatures
  - Ability for notary to be able to query an entity' SOLICT
  - Ability for a notary to query a CRVS entry
  - Ability for notary to create digital attestations re legal identity of a citizen when a jurisdiction's CRVS has deleted an entry from a living person
  - Co-design standards able to work with the above enabling all citizens, regardless of their abilities or disabilities, to interact with a notary
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Non-Profit - 24x7x365 Threat Assessment Subcomponent Cost Centre:

Background:

As mentioned throughout this document, this curve means a continually increasing array of attack vector threats against legal identity governance, business processes, tech used and end users. **The attacks will be against all components the different architectural/cost diagrams in this doc. YES, IT'S COMPLEX AND FAST CHANGING.**

To mitigate against this, threat assessments are composed of:

- People, resources, and infrastructure required to operate a global, 24x7x365 threat assessment centre, for human and AI system/bot legal identities, covering the governance, business processes, tech infrastructure used and end users
- Communication structure for the threats including standardized threat assessments
- Licensing requirements requiring licenses of CRVS or Credential issuance API's to react to different levels of threat assessments, in different ways, within certain time periods

I note, because of the rapidly changing nature of the attack vectors, it's highly likely significant, recurring investment in new tech, like quantum computers etc. will be required i.e., it won't be cheap. The planet's trust in the legal identity framework rests on the backs of the threat assessment teams.

Equally important is the ability to rapidly educate citizens, governments, companies, enterprises, and different levels of government of new threats with rapid abilities to address very high threats. This is where co-design comes into play.

Other Cost Centres Dependent Upon This Cost Centre:

- CRVS Physical/Cyber Security Management/Processes Subcomponent Cost Centre
- CRVS Governance - Specify Actions From Threat Responses Issued by the Global, Independent Non-Profit Subcomponent Cost Centre
- CRVS Governance - Security Standards for the CRVS System Subcomponent Cost Centre
- CRVS Non-Profit 24x7x365 Threat Assessments Subcomponent Cost Centre
- SOLICT Security Subcomponent Cost Centre
- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre:
- Non-Profit – API Subcomponent Cost Centre

Non-Profit - 24x7x365 Threat Assessment Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level threat assessment deliverables and create the first use cases
    - Threat assessment team – the team should be composed of highly skilled people including but not limited to
        - Security/Red team experts
        - Biometrics experts
        - Cloning experts
        - AI Systems/bots experts
        - Networks experts
        - API experts
        - Software programming experts
        - API experts
        - CRVS experts
        - Credential experts
        - Databases experts
        - Physical and virtual security experts
        - Quantum computing experts
        - Communications experts
        - Encryption experts
        - Co-design experts
        - Lessons learnt experts
        - Notary experts
- Determine a wide range of use cases for threats against the cost centres in this document
- Drive out the suggested annual budgets, resources, and team requirements
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground including governance
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale use of non-profit threat analysis
- Transfer governance to the Non-Profit –Governance Coordination/Advisory Subcomponent Cost Centre
- Re APIs – Create standards for:
    - CRVS & Credential Authoritative Sources Databases API's
    - API – Applications/API Rules/Governance
    - API – Backend
    - API – Clients Internal/External
    - API – IAM (Identity Access Management)
    - API – Audit Trail
    - API – API Gateway

Non-Profit – API Subcomponent Cost Centre:

Background:

The API Cost Centre section of this document raises these questions of how to access:

- CRVS entity legal identification, identity/hive relationships and authorization data?
- Credential issuance data?
- Sending the above data to the SOLICT?
- SOLICT communicating with the LSSI devices?
- PIAM managing the LSSI devices?
- Third party's sending consent agreements to the SOLICT?

Which is where API's rule sets come into play. However, there's this tech change curve to consider. As the API is the electronic front door to the legal identity framework described throughout this document, it means the Evil Inc.'s and malicious states of the planet will leverage the tech change curve to constantly create new attack vectors against the API.

Thus, the non-profit must not only do continual 24x7x365 threat analysis against the API but constantly update the API rule sets, as and when required. That's what this cost centre delivers.

Other Cost Centres Dependent Upon This Cost Centre:

- API – Applications/API Rules/Governance Subcomponent Cost Centre
- API - CRVS & Credential Authoritative Sources Databases Subcomponent Cost Centre
- API - Backend Subcomponent Cost Centre
- API – Clients Internal/External Subcomponent Cost Centre
- API – IAM (Identity Access Management) Subcomponent Cost Centre
- API – Audit Trail Subcomponent Cost Centre
- API – API Gateway Subcomponent Cost Centre
- Smart Digital Identity API Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships - SOLICT to LSSI Devices Via TODA Files/LSSI Subcomponent Cost Centre
- CRVS Legal Authorization Rights SOLICT/LSSI API (Application Programming Interface) Subcomponent Cost Centre
- CRVS Legal Identity & Hive Relationships API (Application Programming Interface) Subcomponent Cost Centre
- CRVS API – Applications/API Rules Subcomponent Cost Centre
- CRVS API - Backend Subcomponent Cost Centre
- CRVS API – Clients Internal/External Subcomponent Cost Centre
- CRVS API – IAM (Identity Access Management) Subcomponent Cost Centre
- CRVS API – Audit Trail Subcomponent Cost Centre
- CRVS API – API Gateway Subcomponent Cost Centre
- CRVS Non-Profit - Manages API Rule Sets Subcomponent Cost Centre
- Credential Standards API (Application Programming Interface) Subcomponent Cost Centre
- Legal Identity & Hive Relationships API (Application Programming Interface) Subcomponent Cost Centre
- SOLICT API (Application Programming Interface) Subcomponent Cost Centre
- LSSI Device API Subcomponent Cost Centre
- PIAM API Subcomponent Cost Centre
- Notary – API Subcomponent Cost Centre
- Non-Profit - 24x7x365 Threat Assessment Subcomponent Cost Centre

Very Important Note:

A large part of this cost centre work is threat analysis and prevention. Thus, it makes sense for this cost centre to be part of the Non-Profit - 24x7x365 Threat Assessment Subcomponent Cost Centre. This maximizes resources, expertise and minimizes budget costs. Thus, in the Excel spreadsheet, that's what I've done.

Non-Profit – API Rule Sets Subcomponent Costs:

Costs will be borne by the Non-Profit - 24x7x365 Threat Assessment Subcomponent Cost Centre.

Non-Profit - Independent Auditors Subcomponent Cost Centre:

Background:

Who watches the watchers? This is a major concern in the governance and operations of the new, global, independent, non-profit. The architecture is built around having a group of independent auditors to audit the enterprise regularly.

Politics change over time. Thus, the global independent non-profit may fall to political attacks either internally within the non-profit, or externally. Thus, since the non-profit is a key centrepiece in global legal identity for both humans and bots, a mechanism MUST be created to keep intact its "political squeaky clean" functioning.

Careful thought needs to be applied here to prevent just one auditing firm doing the analyzing – for it could lead to leveraging against the auditing firm to produce the "desired audit results". I'm not sure of the mechanism to mitigate against this – but I know it needs to be thought through by the initial funders and the initial board.

The costs of operating this independent auditing function MUST be built into the global, independent non-profit's annual operating costs.

I'M NOT AN EXPERT ON THIS. Thus, what follows is only my best guess on where to start. People with much more experience in this area will likely recommend a change to below.

Non-Profit - Independent Auditors Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a group of non-profit and auditing experts including but not limited to:
    - Legal experts
    - Non-profit experts
    - Auditing experts
    - Political experts
    - Lessons learnt analysts
    - Co-design experts
    - Others?
  - Create high level requirements for how the independent auditing group could function, along with use cases and proposed annual budgets
  - Get political buy in from key groups
- Then create a plan to bring this into reality with budgets, resource requirements, et al

Cost Centre: Rethought Business Processes – Competitive Edge

Background:

Skim "**AI, Bots & Us - Examples of Rapid Change**" to see the myriad examples of how AI systems and bots, both physical and digital are changing how we work and live. Then skim "**AI Leveraged Smart Digital Identities of Us**". It discusses how AI leveraged smart digital identities of humans will radically rethink how businesses operate with employees. Finally, skim "**Entity Management System'**" to see how Acme Health Inc. leverages MedBot1, Nurse or Doctor Jane Doe's smart AI leveraged medical digital identity and hives to rethink how they work with their patients.

Give the Jurisdiction's AI/Bot Industry a Competitive Edge

My premise is the jurisdiction first adopting the new legal identity architecture, can offer their AI/bot industry new ways to do things faster, cheaper, and better with their global customers. How?

Read this one pager "**Why Should Your Government Invest $18-27 Billion?**". It describes how the AI/Bot industry can offer their customers, who are buying or leasing AI systems, physical/digital bots, or AI leveraged smart digital identities of humans, THE ABILITY, WITHIN SECODNDS, VIA A SMART AI LEVERAGED CONTRACT:

1. Create legal entity identities
2. Verify the legal identity of the entities
3. Verify their credentials
4. Creating legal identity hive relationships and legal authorization rights
5. State whom the entity can share or not share data with
6. Enter them into their new age "Entity Management System"
7. Assigning them authentication and authorization rights

It will radically transform the current time consuming and expensive processes of contracts, HRMS/CRM and IAM systems.

To see a more detailed view skim this:

Use Case Background:

The used case below refers to Graph databases and TODA. I strongly suggest reading "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

It describes small, architectural baby steps enterprise must take to get ready for this incoming tech revolution:

- Graph databases
- TODA

The use case below also leverages the story line/use case used in:

- "**Entity Management System'**"

Use Case:

AI/Bot Manufacturer Inc. is supplying to Acme Health Inc.:

- The services of MedBot1 (be it an AI system, a physical or digital bot or combination of these) which might be sold or leased
- Ai leveraged medical digital identities for Nurse or Doctor Jane Doe (which again might be sold or leased to Acme Inc. and/or to Jane Doe directly)
- Nanobots in the future to be used to diagnose and/or treat Sally Smith (refer to the article "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**"

The assumption for this use case/story is the following exists:

- Local/global legal identity framework for Ai systems, bots (both physical and digital) and humans from birth to death, to a high level of identity assurance, including, where risk requires it, the ability to register AI smart digital identities against the human's physical legal CRVS entry (Civil Registration Vital Statistics)
- The ability of the CRVS system to also leverage TODA and graph databases to map a bot's relationship to a bot hive
- The ability of the CRVS system to create legal authorization rights to an entity which they may in turn choose to delegate sections of to other entities
- Standards for rapidly querying entity identities (including secure source code entry of the legal identity, DNS/PKI/port security standards, TODA standards)
- Standards for rapidly querying entity credentials (including secure source code entry of the legal identity, DNS/PKI/port security standards, TODA standards)
- AI leverage smart contracts operating to new global legal and identity standards
- Acme Health Inc. leverages a new entity management system leveraging authoritative entity management systems (which the paper calls an EMS) leveraging graph databases to manage complex, fast changing relationships between entities

- Acme Health Inc. also leverages TODA internally in conjunction with graph-based identity and access management systems to allow for rapid assignment of authorization rights with the ability to delegate sections of them to an entity

In a few seconds, here's what can happen between AI/Bot Manufacturer Inc. and Acme Health Inc.:

- **AI/Bot Manufacturer Inc. registers the identity of MedBot1 and the hive it belongs to (MedBotHive ABCDE) into the local jurisdiction's CRVS**
    - Which instantly first checks across all other CRVS systems on the planet is MedBot1 exists or not, if MedBotHive ABCDE exists or not)
    - Assuming MedBot1 doesn't exist, then the process instantly continues
    - The local CRVS writes into MedBot1's source code it's unique legal identifier as well as a TODA file containing MedBot1's hive relationship with MedBotHive ABCDE
    - The local CRVS also writes into MedBotHive ABCDE's legal identity, a TODA file containing the relationship between the hive and MedBot1
- **AI/Bot Manufacturer Inc. registers MedBot1's medical credentials against the local jurisdictions medical credential granting institution**
    - Which uses standards set forth for writing credentials set by the new, global, independent non-profit
    - Note: The non-profit does continuous threat analysis against new attack vectors - any threats are given a rating, with medium to very high threats, requiring all credential bodies on the planet to respond and upgrade their credential issuing systems within a pre-agreed amount of time – this is how to bring industry best practices to the world of institution or commercial credential granting bodies
    - MedBot1's legal identity contained within its source code is updated with a TODA file containing the digitally signed credential
- **The AI smart contract between AI/Bot Manufacturer Inc. and Acme Health Inc. immediately takes these new entities and checks the legal identities and credentials from Acme Health Inc's perspective to confirm the legal identity and credentials are valid**
    - This is done via Acme being able to instantly query MedBot1's legal identity and credentials, taking the digital certificates issued by the CRVS and medical credential granting body and making a quick electronic trip to confirm the certs are still valid
- **The contract specifies what data MedBot1 can obtain, who it can be shared with i.e., entities/apps/humans etc.), what happens to the bot when it's terminated, merged into other hives/systems, etc.**
- **The AI smart contract is then instantly digitally signed by the parties Ai systems or, if humans are required, then humans digitally sign it**
- **Acme Inc. then instantly enters MedBot1 into its entity management system at the same time assigning the bot authorization rights with an ability, spelt out via the**

contract, to be able to delegate sections of its authorization to other entities, humans, etc.

Note: A similar process occurs for Jane Doe's AI leveraged smart medical digital identity as well as for any nanobots issued by AIBotManufacturer Inc. to Acme Inc. and Sally Smith, their patient.

To make the magic work requires:

- New legal identity framework
- Digital credentials framework
- Graph databases
- TODA
- AI leveraged smart contracts
- New entity management systems
- Change/standards to contract law, identity laws in each local state/province, credential standards, etc.

Regarding credentials, you might want to skim:

- "Verifiable Credentials For Humans and AI Systems/Bots"

Benefits:

- **The first country and their industry to do this, will gain a significant competitive edge over their competition**
  - They'll be able to offer their global customers entity management faster, cheaper, and better
- **Like the advent in the 90's of HRM and CRM systems, it will spur on creation of "EMS" (Entity Management Systems)**
- **It will also spur on rapid innovation with AI leveraged smart contracts**

It's out of the box thinking for out of the box times.

Rethought Business Process Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a group of non-profit and auditing experts including but not limited to:
    - Jurisdiction commerce experts
    - Jurisdiction legal expert
    - Jurisdiction AI system/bot experts
    - AI smart contract experts
    - Co-design experts
    - CRVS experts
    - SOLICT experts
    - LSSI device experts
    - PIAM experts
    - API experts
    - Hive Relationship experts
    - Legal authorization rights experts
    - Security red team experts
    - Business process experts
    - Lessons learnt analysts
  - Create use cases leveraging the example described above
  - Then create requirements
- Do rapid POC's to learn what doesn't work and what works
- Then do small, tightly controlled pilots to see how it works in the real world
- Then rapidly scale

The budget for this is based on 30 innovative projects, over three years, with each project receiving between $50-75 million.

Cost Centre: New Learning Vision Cost Centres to Rethinking Learning from Cradle to Grave

Background:

Skim these articles:

- "**Vision: Learning Journey of Two Young Kids in a Remote Village**"
- "**Sir Ken Robinson - You Nailed It!**"

They lay out a new learning vision starting when the learner is a toddler. It creates:

- DLT (Digital Learning Twin)
- Which in turn continuously produces updated IEP (Individualized Education Plan)
- Which is then leveraged by home/school LMS (Learning Management Systems)
- All leveraging the learner's LDV (Learner Data Vault).
- The learner is in control of their DLT and can, with their consent, allow employers, post-secondary et al, use the DLT to highly customize, streamline and lower costs for training/educating the learner
- It's all driven by co-design such that all learners, regardless of their abilities or disabilities, can learn
- It also enables all learners on the planet to learn, regardless of where they live i.e., no learner is left behind

It's highly transformational.

In "**Learning Vision Flyover**" it shows the architectural cost centre components required to create the vision. This document is the deeper dive into the costs associated with each component.

Given this curve, how are we going to keep learning systems secure 24x7x365, not only against attacks against the tech used, but also against the governance, business processes and end users?

In the legal identify architecture, I've included a global, independent, non-profit to do this. It's funded by licensing:

- New CRVS systems to jurisdiction, on a very low charge for every CRVS event, to a maximum yearly amount
- A very low charge to credential bodies for every credential issued

My underlying premise is most learning/education jurisdictions around the planet don't have the resources and expertise to continually address this. Thus, I'm proposing something similar for the new learning system.

State/provincial/national education departments/ministries of education would license out the learning assessment, DLT, IEP standards from a global, independent non-profit to a maximum yearly amount based on their student populations.

I can see this new learning non-profit in effect piggybacking the legal identity & credential non-profit24x7x365 threat assessments i.e., one looks after legal identity and threats, while the other looks after learning systems and threats. This new learning non-profit entity is depicted by the cost centre section titled, "Global, Independent, Learning Non-Profit Component Cost Centre" in the following picture.

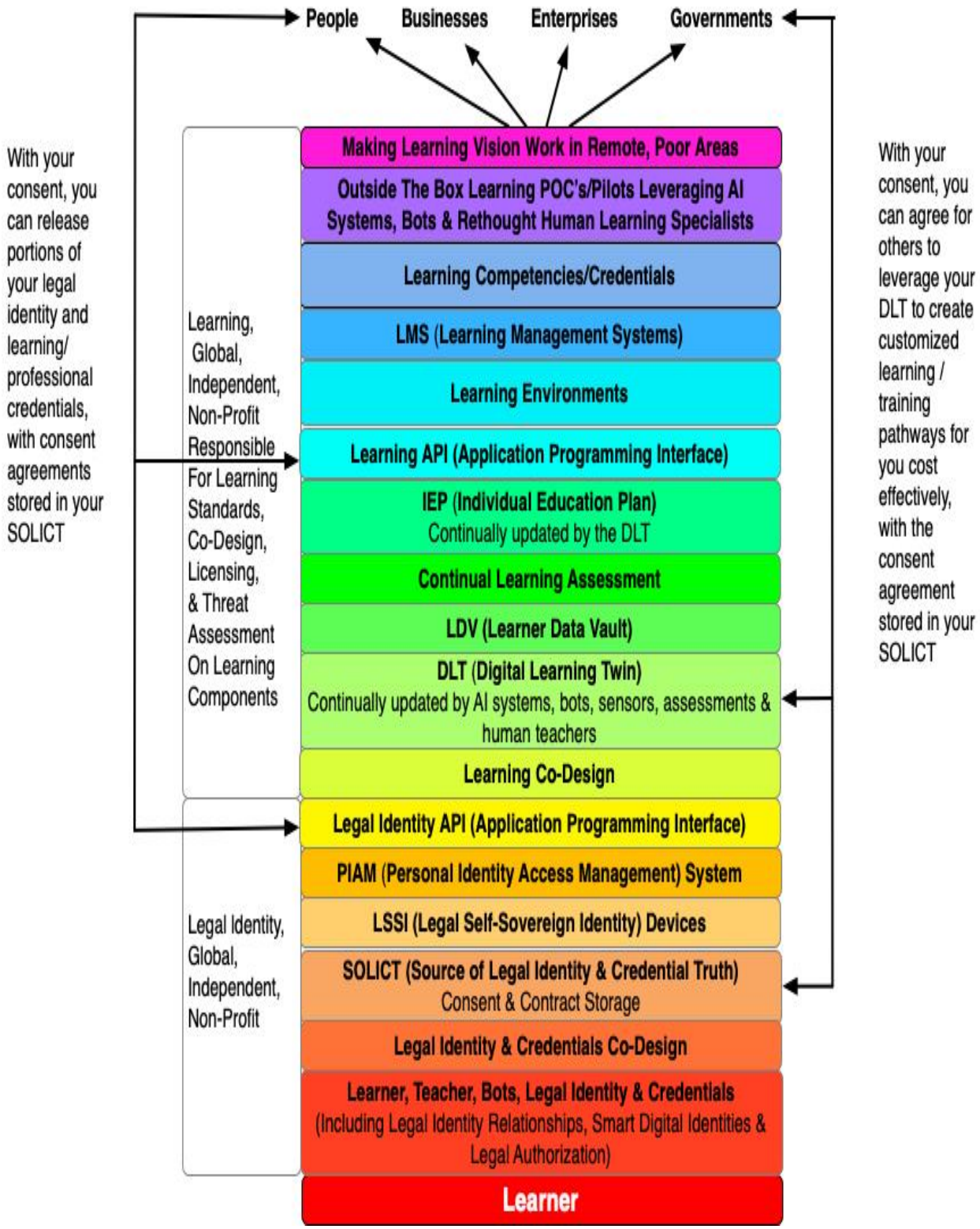
The "**Vision: Learning Journey of Two Young Kids in a Remote Village**" has the learning vision able to function in all sections of the planet. The challenges associated with this are large. They include lack of electricity, internet connectivity, criminals stealing bots, et al. Thus, included in this cost centre, I have a separate cost centre devoted to determining costs associated with piloting this in remote locations.

Next, watch the 19 minute 30 second of "The AI Dilemma". It shows how AI can read our brainwaves. Then skim this article, "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**" where it discusses how this tech will likely infiltrate schools from the home.

Finally, skim **The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom**". This is the new reality learning environments are going to be operating in.

The new learning architecture is built addressing all the above. It's out of the box thinking for out of the box times.

Rethinking Learning Subcomponent Cost Centre Diagram:



Learners, Teachers, Bots Legal Identity, Relationships/Hives, Legal Authorization Rights and Credentials Subcomponent Cost Centre:

Background:

Eight years ago, when I began to contemplate creating a new learning architecture, I realized it first requires a new legal identity and credentials framework for both humans and AI systems/bots. Why?

I could see in my mind how AI systems, physical/digital bots, IoT devices, smart AI leveraged digital versions of us, and new AI/AR/VR learning environments, would create the framework for a totally rethought learning system. The key building block is having a legal identity and credentials framework.

It's complicated. Why? Legal identity/hive relationships and legal authorization rights.

So, Jane Doe, mother of John Doe, needs to prove, both physically and digitally, her legal identity relationship as a parent of John. As well, she also must prove her legal ownership relationship with AssistBot, who's assisting John in his learning.

Further, she needs to be able to delegate, to say a school, which sections of John and AssistBot's legal identities can be used. This also applies to John's biometrics and learning data from his LDV (Learner Data Vault). The consents for all these agreements should be stored within her, John's and AssistBot's SOLICTS.

AssistBot's teaching assistant credentials also might need to be proved to the school John's entering.

All the above are the starting foundational building blocks for rethinking learning.

Learner Learner/Legal Identity, Relationships/Hives, Legal Authorization Rights and Credentials Costs:

- Human and AI system bot legal identities costs are borne in the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre section of this document
- Legal relationships and hives costs are borne in the Non-Profit – Manages Legal Identity Hive Relationships Standards Subcomponent Cost Centre section of this document
- Legal authorization costs are borne in the Non-Profit – Manages Legal Authorization Standards Subcomponent Cost Centre section of this document
- Credential issuance costs are borne in the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document

Legal Identity & Credentials Co-Design Subcomponent Cost Centre:

Background:

As described in "Vision – Co-Design 'Nothing About Us Without Us'" section, co-design is mission critical in allowing citizens of all abilities and disabilities to leverage the new legal identity and credential framework. That's what this cost centre delivers.

Legal Identity & Credentials Co-Design Subcomponent Costs:

Costs will be borne by the "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre" section of this document.

Rethinking Learning - SOLICT (Source of Legal Identity & Credential Truth) Cost Centre:

Background:

The SOLICT is the source of truth for an entity's legal identify and credentials. It's also the repository for all consents given on behalf of, or by the entity, to third parties, from creation to termination of the entity.

The architecture is based on privacy by design. I wanted to create a design mitigating against where a malicious state couldn't delete an entity's legal identity information within their data systems, effectively screwing the entity from proving their identity. The global, independent, legal identity non-profit thus takes data from the CRVS (Civil Registration Vital Statistics) system and creates a new database per entity on the planet.

I had some performance and security concerns with this. Skim "Background" in Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) section of this document for more details about why I'm concerned.

Finally, all citizens of the planet, regardless of their abilities or disabilities MUST be able to:

- Understand what a SOLICT is
- Know what legal identity and credential data about them is stored within it
- Understand how to use their LSSI devices and/or PIAM to share portions of their information with third parties

This is what co-design delivers.

Rethinking Learning - SOLICT (Source of Legal Identity & Credential Truth) Costs:

SOLICT costs will be borne in the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) and the "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre" section of this document.

Rethinking Learning - LSSI (Legal Self-Sovereign Identity) Devices Cost Centre:

Background:

How can a learner easily prove their learning credentials, physically or digitally, locally, or globally? What if the learner is very poor and doesn't have access to tech? What if the learner has disabilities? How can a learner like John Doe prove his legal identity relationship with his mother Jane Doe? How can a teaching bot easily prove its identity and teaching credentials?

All of the above are where LSSI devices come into play. There are five types of LSSI devices:

- Physical, smart legal identity card
- Legal identity digital application
- Physical wristband, containing the legal identity/credential information, biometrically tied to the wearer
- A chip implanted into the entity
- Writing legal identity and credential information to the source code of an entity

Thus, it meets the needs of all the above challenges. The source of truth for the LSSI device is the SOLICT. LSSI devices are fed their legal identity and credential data, from the SOLICT, via TODA files (skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" to understand TODA).

Finally, all citizens of the planet, regardless of their abilities or disabilities MUST be able to:

- Understand what a SOLICT is
- Know what legal identity and credential data about them is stored within it
- Understand how to use their LSSI devices and/or PIAM to share portions of their information with third parties

This is what co-design delivers.

To see a story about how a person leverages their LSSI/PIAM in their daily life skim, "**An Identity Day in the Life of Jane Doe**".

Rethinking Learning - LSSI (Legal Self-Sovereign Identity) Devices Costs:

Costs will be borne by the LSSI Devices Cost Centre and the "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre" section of this document.

Rethinking Learning - PIAM (Personal Identity Access Management) Cost Centre:

Background:

Imagine Jane Doe walking down a street, wearing AI/AR glasses/contact lenses where she's both in the online and offline world simultaneously. She'll likely be bombarded by requests for her to share her identity. She's not going to want to have to manually do this. That's why I created the concept of a PIAM.

It leverages AI for Jane to then pre-determine who she wants to share her legal identity and credential information to. If you skim, "**An Identity Day in the Life of Jane Doe**" you'll see how Jane's PIAM allows her to mostly live privately except with those third parties she wants to share her information with.

Now making this vision become a reality requires security standards, since the PIAM will become a prime point of attack by criminals. Further, given this curve, it means today's best security standards can quickly become tomorrow's turd. Which is why the architecture calls out for PIAM standards to be managed by the global, independent non-profit, which also does 24x7x365 threat analysis against it. Thus, the architecture keeps the PIAM secure.

A person will use their PIAM to control their smart digital identities as well as any AI systems/bots they have a contractual relationship with. Yes, it's complex. Which is why the PIAM cost centres start out with a series of small, rapid POC's and pilots to work our way through the many challenges in designing, implementing and maintain PIAMs.

All citizens of the planet, regardless of their abilities or disabilities MUST be able to:

- Understand what a SOLICT is
- Know what legal identity and credential data about them is stored within it
- Understand how to use their LSSI devices and/or PIAM to share portions of their information with third parties

This is what co-design delivers.

Rethinking Learning - PIAM (Personal Identity Access Management) Costs:

Costs will be borne by the Cost Centre - PIAM (Personal Identity Access Management) System the "Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre" section of this document.

Rethinking Learning – Legal Identity API (Application Programming Interface) Cost Centre:

Background:

A major performance and security question is how to securely access:

- CRVS entity legal identification, identity/hive relationships and authorization data?
- Credential issuance data?
- Sending the above data to the SOLICT?
- SOLICT communicating with the LSSI devices?
- PIAM managing the LSSI devices?
- Third party consent agreements sent to the SOLICT?

Answer - Create standard API's (Application Programming Interface).

It addresses the problems of how to query billions of us with AI leveraged, smart digital identities and trillions of AI systems and bots for their legal identities and/or for them to present it to a third party. So, I've included this in the architecture to get discussion and debate going on how this will be addressed.

Add to the above complexity the rapid attack new attack vectors being created against the legal identity framework from this curve. The API is the electronic front door. Which is why the architecture has the new, global, independent, well-funded, non-profit. One of its tasks is to do 24x7x365 threat analysis and produce rated threats and threat responses. Thus, the API's created will likely be very frequently updated.

Rethinking Learning - Identity API (Application Programming Interface) Costs:

Costs will be borne by the Cost Centre: API (Application Programming Interface) section of this document.

Rethinking Learning – Co-Design Cost Centre:

Background:

Learners have different learning abilities. Some have learning disabilities. I wanted to think outside the box, enabling all learners to learn.

As per the earlier section of this doc, "**Vision – Co-Design 'Nothing About Us Without Us'**", it lays out why use of co-design, from the outset of design, is critical in delivering government and learning services to the citizen, regardless of their abilities or disabilities. Thus, rather than each local CRVS and education jurisdiction invent their own citizen legal identity, credential and learning interfaces physically and digitally, it makes much more sense for the two new, global, independent, non-profits to use co-design to create this. As well, it also makes sense for each non-profit to continually update it as this tech change curve occurs and/or new security attacks occur against a CRVS.

This cost centre focusses on learning co-design.

Rethinking Learning - Co-Design Costs:

Costs will be borne by the Learning Non-Profit – Co-Design Subcomponent Cost Centre.

Rethinking Learning DLT – Digital Learning Twin (DLT) Cost Centre

Background:

I wanted to do in learning what industry has done in manufacturing and health i.e., creating digital twins to model with. I could see how a digital learning twin would know the learner best, thus prescribing for them, the optimal learning tools, methods, situations, etc.

However, in my discussions with computing experts, they've told me, while they like the concept of a digital learning twin, they don't think the computing power is here yet to do many people's DLT's continually. I accept this.

Thus, my strategy is to edge our way into this revolution, using limited sections of computing to create a DLT, which in turn will create first draft IEP (Individualized Education Plan). Then to only do periodic updates to the DLT. Over time, as computing power increases and costs drop, increase the frequency of the updates along with richer data from biometric, behavioral, and other learning data sources.

My other strategy in creating the DLT is to first focus on the learning assessment piece. It's the initial source of data for the DLT. Thus, by first starting with things like ADHD/ASD learning assessments, it brings in a rich data set to the DLT to work upon.

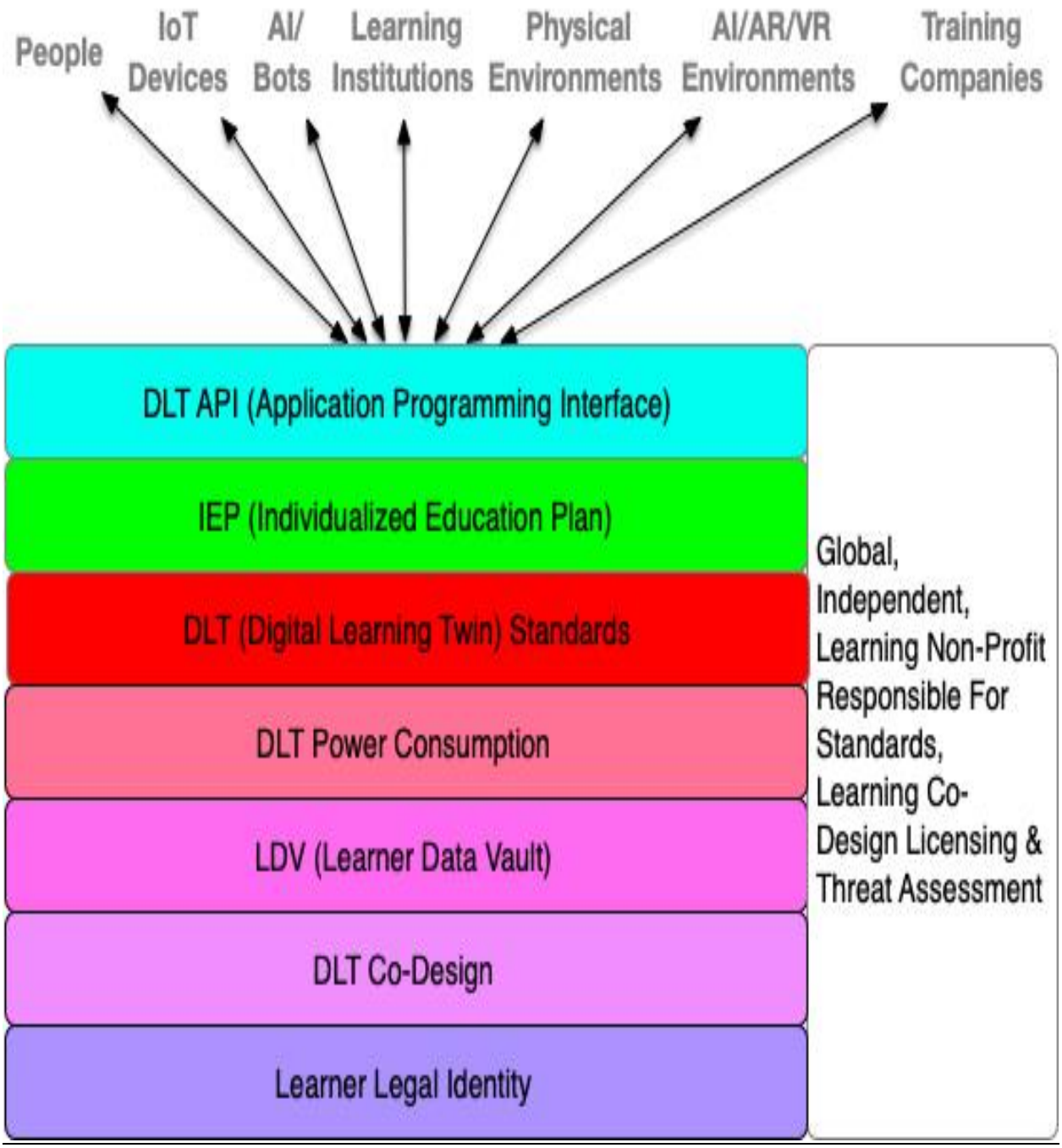
The longer-term strategy is to integrate learning assistant bots et al as sources of continual learning data about each learner into the DLT. It's hypothetically possible to off-load from the DLT to a bot, some of the computing power required to process DLT type information. Thus, this too should be a consideration of the DLT design and implementation team.

I suggest readers skim "**Decentralized AI – Risks, Legal Identity, Consent & Privacy**". It discussed the emergence of decentralized AI. I can easily see this being adopted by the DLT and learning assessment architectures to off-load AI computing requirements closest to the entity.

I also suggest readers skim "AI Power Consumption Exploding". Look at Figure 1. It shows, by 2040-ish, AI consuming most power on the planet. Beyond computing power required for AI, this is something as critical, yet not on most people's radar screens yet.

Note: A person's DLT MUST be legally registered against the learner's legal physical identity in the local CRVS. However, also note that in the beginning, while doing DLT development, the legal human and AI system/bots framework isn't required.

DLT Subcomponent Cost Centres Diagram:



DLT - Learners Legal Identity Subcomponent Cost Centre:

Background:

The leaner's legal identity comes from the legal identity framework described earlier in this document.

The learner might not always be the physical learner. Skim "**AI Leveraged Smart Digital Identities of Us**". Further, it's possible, in the not-so-distant future that we'll be able to write to our brains. All of which requires the learner's consent as well as being sure it's the legal identity of the learner and not someone else masquerading as them.

All of which are reasons why when thinking about creating the new learning architecture several years ago, I realized it first required a rethought human and AI system/bot legal identity framework.

I strongly suggest readers skim, "Rethinking Human Legal Identity" to get a 100,000-foot level overview of the human legal identity architecture.

DLT - Leaners Legal Identity Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre and the Cost Centre: Rethought CRVS (Civil Registration Vital Statistics section of this document.

DLT – Co-Design Subcomponent Cost Centre:

Background:

The DLT is all about leveraging co-design to create learning for people of all abilities and disabilities. As importantly, a learner, regardless of their abilities or disabilities should be able to understand:

- What they're DLT is
- What it can do for them
- How it works

Thus, it's mission critical that the co-design team responsible for the DLT be part of the design, testing, implementation and maintenance process from the beginning.

DLT – Co-Design Subcomponent Costs:

Costs will be borne by Learning Non-Profit – Co-Design Subcomponent Cost Centre section of this document.

DLT – LDV (Learner Data Vault) Subcomponent Cost Centre:

Background:

The LDV is the heart of learner data. It's controlled by the learner, existing outside the control of a jurisdiction. The LDV is managed by the new, global, independent, learning non-profit.

The DLT leverages LDV data from learning assessments, etc., to create the IEP (Individualized Education Plan). The LDV is continuously fed data about the learner, with which the DLT continually updates the IEP.

DLT – LDV (Learner Data Vault) Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages LDV (Learner Data Vault) Standards section of this document.

DLT – Power Consumption Subcomponent Cost Centre:

Background:

Each learner on the planet will be given and leverage their own AI leveraged DLT i.e., there will be billions of them. Each one consuming power.

Since it's so critical to sustainable deployment, I broke this out as its own cost centre. The main deliverable is to create low power consumption per DLT.

DLT – Power Consumption Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Power Consumption of LDV and DLT Subcomponent Cost Centre section of this document.

DLT – DLT (Digital Learning Twin) Standards Subcomponent Cost Centre:

Background:

This rapid tech change curve means rapid changes to AI. Thus, as the tech changes, so to must the DLT. Which is why I created this DLT Standards subcomponent cost centre.

Further, a learner can be interacting with the following entities/environments at the same time:

- Physical people
- Smart, AI leveraged, digital identities of people
- IoT devices
- AI systems and bots
- Physical environment
- AI/AR/VR environments

Based on how a learner learns, works, or doesn't work with others, and how their environments they're in, it will continually change their DLT.

Further, I can see is a rapid rate of change with not only the DLT/IEP's but also desired learning outcomes. Why? The introduction of AI leveraged digital identities. Skim "**AI Leveraged Smart Digital Identities of Us**". Thus, what we do, who we do it with, how we learn, how we use the knowledge, etc. will all likely rapidly change over the next 5-10 years.

Bottom line: Each learner's DLT/IEP's will change as learning outcomes rapidly change.

Then there's the power consumption rom each DLT. Look at Figure 1 in "**AI Power Consumption Exploding.**" It shows, if current AI power consumption trends continue, by 2040-ish Ai will be consuming most of the planet's power supply.

Of course, this is untenable. Yet, sadly, it's not even on most peoples' and policy makers' radar screens. It's on mine. Why?

The learning architecture produces a DLT for each person on the planet. Thus, there will be literally billions of AI DLT's. Thus, this needs to be studied and very carefully planned for. Readers might want to skim "**Decentralized AI – Risks, Legal Identity, Consent & Privacy**" to see a possible solution.

Finally, the curve also creates new attack vectors against the DLT. Thus, from a security perspective, it too must be constantly kept up to date.

The new, global, independent, learning non-profit will administer the DLT standards. As well, it will also conduct 24x7x365 threat analysis, constantly updating the DLT as and when required.

DLT – DLT (Digital Learning Twin) Standards Subcomponent Costs:

Costs will be borne by the Learning Non-Profit Manages DLT (Digital Learning Twin) Standards Subcomponent Cost Centre section of this document.

DLT – IEP (Individualized Education Plan) Subcomponent Cost Centre:

Background:

The IEP was introduced in schools in 1975:

> "The IEP describes how the student learns, how the student best demonstrates that learning, and what teachers and service providers will do to help the student learn more effectively. Developing an IEP requires the team to evaluate the student in all areas of suspected disability, consider the student's ability to access the general education curriculum, consider how the disability affects the student's learning, and choose a federal placement for the student." - https://eric.ed.gov/?id=EJ1013681 .

My vision is to give each student on the planet, regardless of their learning abilities, an IEP highly tailored for them, which is continually updated from an increasing rich array of resources i.e., learning assistant bots, teaching assistant bots, humans, and a wide variety of different sensors and assessment devices.

I was told by a winner of the Teaching Award of Canada, that often for ADHD/ASD students the diagnosis is to do one on one instruction. However, since school districts can't afford this, they're often put into small groups, which may or may not work well for the learner.

If one scans current IEP standards (which vary around the planet), you'll find them requiring extensive human input, since currently, there's not lots of different sources of learning data, continually available, to draw upon. My point is I don't want to reduce human interaction, but I want to rethink when humans are used, based on each person's learning needs and learning deliverables required. **AI systems and bots, both physical and virtual, plus a wide variety of sensors, can fill this need. Thus, it's time to rethink IEP's leveraging this.**

DLT – IEP (Individualized Education Plan) Subcomponent Costs:

The costs will be borne by the Learning Non-Profit Manages IEP (Individualized Education Plan) Standards section of this document.

DLT – API (Application Programming Interface) Subcomponent Cost Centre:

Background:

The API is the electronic front door to the DLT. Consider this curve. It hypothetically means each hour, new attack vectors are being created against the DLT's API, endpoints, networks, DNS, encryption etc. My point? Most learning institutions and enterprises around the planet DON'T have the expertise, budgets and staff to continually detect new attack vectors and rapidly change API standards to defend.

This is a similar problem described in the Legal Identity Cost Centre: API (Application Programming Interface) section of this document. Thus, I've taken a similar approach when creating the learning architecture.

The new, global, independent, learning non-profit has a subcomponent cost centre addressing API's. Its job is to keep the DLT API up to date and secure.

DLT – API (Application Programming Interface) Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards section of this document.

Rethinking Learning LDV - Learner Data Vault Subcomponent Cost Centre

Background:

The old data model we use today, in most applications, is a person's personal data is typically stored by other third parties in their applications' data systems. This equally applies to schools. Thus, a learner has little to no control over their learning data within the applications, databases et al, which they produce daily. THIS IS NOT PRIVACY BY DESIGN. I want to flip this on its head.

Just as in SOLICT, I want to begin to think about giving each person on the planet a personal learning data vault, which they control. This puts any entity wanting to interact with the learner, first requiring their consent to use the data. Then, I'm also proposing storing the data in the learner data vault i.e., the enterprise is now no longer the keeper of the learning data. This is privacy by design.

Is this all possible today? No. Is it possible, as the cost of data storage continually drops? Yes. Are there potentially large operational costs associated with this? Yes. Are there security risks associated with this? Yes. Thus, prudence is required in any design, governance and implementation model proposed for this.

All of this begs the question who's going to pay for it and operationally run it? My strategy is to use a similar approach used with SOLICT i.e., have a global, independent, non-profit manage the LDV. However, I strongly note it should not be the same non-profit running the legal identity framework.

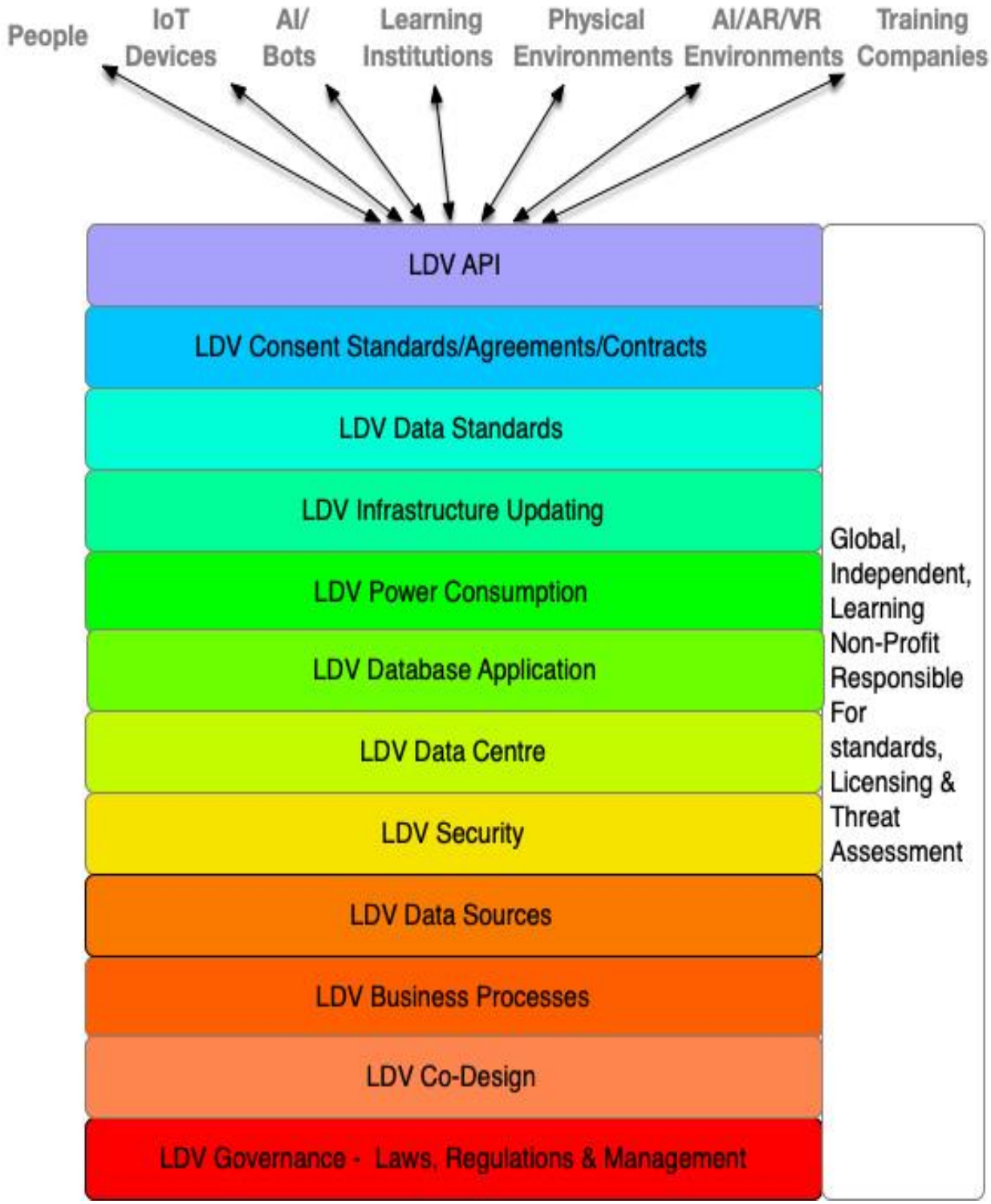
Why? The adage "stick to your knitting" applies. Keep the non-profits focussed on what they do best. So, the non-profit assigned for managing legal identity should stay focussed on legal identity. The learning, global, independent proposed in this cost centre document, should be focussed on learning and nothing else.

In the cost centre section, it proposes a funding model similar to the legal framework non-profit i.e., licensing it out to jurisdictions. The funding model sees a very small fee per student on the planet, to license the standards and security associated with learning assessment, DLT, IEP, credential API and the LDV. Hypothetically, there could be enough money to fund the LDV.

This architectural cost centre document is visionary. As continually stated throughout this doc, a vision doesn't happen overnight. Thus, as with all other sections of this doc, I'm recommending a crawl, walk and run strategy to get from where we are today, to the promised learner data vault land.

Start small, with a design goal to rapidly scale once we've figured out what to do and how to do it. Very careful thought must be placed on the potential sizing of each learner's LDV over time, the associated costs in maintaining it and security.

LDV – Subcomponent Cost Centres Diagram:



LDV Governance – Laws, Regulations & Management Subcomponent Cost Centre:

Background:

LDV will be managed by the proposed global, independent learning non-profit. It will become the authoritative source for an entity's learning data.

Learning data sources feeding the LDV:

- People
- IoT devices
- AI systems and bots
- Learning institutions
- Physical environments
- AI/AR/VR environments
- Training companies

ALL OF THIS MUST BE VERY SECURLEY DONE LEVERAGING API'S AND TODA.
Skim these:

- API Cost Centre section of this document
- "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"

Laws/Regulations:

Jurisdictional laws and regulations will need to be created and/or modified acknowledging the LDV as well as legally accepting it as the mostly authoritative source of an entity to manage learning data on their own. Here's one of the challenges in doing this. Cross-border prosecution enforcing LDV laws and regulations.

Skim, "Fighting cybercrime – what happens to the law when the law cannot be enforced?" It shows the pathetic 0.05% success rate of prosecuting cybercrime. Thus, Jane Doe might be screwed in protecting her LDV from Evil Inc. who's operating out of a jurisdiction where they can't be prosecuted.

Laws and regulations need to be created clarifying how learning data can be used and also not used.

Management:

The new, global, independent non-profit will have management abilities over the billions of LDV's. This is both good and bad. It gives them potential abilities to misuse LDVs.

LDV Governance Requirements:

- Be legally recognized by the jurisdiction as a place the learning institutions within the jurisdiction can write to with a person's learning data
- The LDV will accept an authorized learning source digital signature as part of the TODA information package being written
- Each LDV will have its own learner's digital signature to digitally verify itself to local authoritative source
- Each LDV will have a governance contract determining which entities can manage a LDV on behalf of another person via SOLICTS (Source of Legal Identity & Credential Truth)
    - Jane Doe, as mother of John Doe, would be assigned by the local jurisdiction as his mother at birth, with the jurisdiction cryptographically cross-linking both John and Jane's SOLICT files establishing the relationship
    - John Doe's SOLICT would issue a contract to his mother's SOLICT specifying what she can do to manage his legal identity, etc. as per the legal governance requirements, to new global standards, set forth and managed by the global, independent non-profit
    - If Jane dies, the local jurisdiction assigns a legal guardian, Sally Smith, for John. The jurisdiction writes the changes to both Sally and John's SOLICT files, as well as changing the status of Jane's SOLICT to deceased. The contract between Jane and John is now void. Sally would then receive a new contract from John's SOLICT, setting forth what she can do to manage his legal identity
- Have governance processes for changes to a person's LDV data
- Have governance processes for storage and archival of a person's LDV
- Have governance processes for managing LDV consent contracts which are stored in the learner's SOLICT

LDV Governance Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
    - The team should include the following types of people:
      - Legal experts
      - Learning experts
      - Jurisdiction law experts
      - Business process experts
      - Database experts
      - Red team experts
      - Smart digital identity experts
      - AI system/bot experts
      - Global, learning non-profit experts
      - Co-design experts
      - Lesson learnt expert
  - Create a draft LDV governance model
  - Do small, controlled POC's and pilots to see what governance works and what doesn't work
  - Learn from it, and then rapidly scale
  - Transition management of this to the global, independent, learning non-profit

LDV Co-Design Subcomponent Cost Centre:

Background:

Every learner on the planet, regardless of their abilities or disabilities MUST know:

- What their LDV is
- What's stored in it
- What they can and can't do with the data stored within it
- How they can use their LSSI devices and PIAM to release portions of their learning data, with their consent, to third parties

That's what this cost centre delivers.

LDV- Co-Design Subcomponent Costs:

Costs will be borne by Co-Design - LDV (Learner Data Vault) Subcomponent Cost Centre section of this document.

LDV Business Processes Subcomponent Cost Centre:

Background:

LDV's are an entity's learning data storage repository. This requires some kind of legal agreement/contract agreed by the entity with another party which is either feeding data into the LDV or using data from the LDV.

Note that weak business processes are an attack vector against an entity's LDV.

Business process use cases must be prepared detailing the business process flow for entering, changing, storing, and archiving of data. There's a problem when perhaps data was erroneously written to an LDV, etc. Thus, these are just some of the use cases that will need to be developed and worked through by a team. In effect, the business processes drive how a LDV will be used.

LDV Business Process Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
        - The team should include the following types of people:
            - Business process experts
            - Legal experts
            - Learning experts
            - Jurisdiction law experts
            - Database experts
            - DLT experts
            - IEP experts
            - Red team experts
            - AI system/bot experts
            - Global, learning non-profit experts
            - Co-design experts
            - Lesson learnt expert
    - Create LDV business process use cases
    - Do small, controlled POC's and pilots to see what business processes works and what doesn't work
    - Learn from it, and then rapidly scale
    - Transition management of this to the global, independent, learning non-profit

LDV Data Sources Subcomponent Cost Centre:

Background:

Data sources feeding the LDV:

- People
- IoT devices
- AI systems and bots
- Learning institutions
- Physical environments
- AI/AR/VR environments
- Training companies

I can see all the above becoming very complicated and large in terms of data volumes. Why? Let's use learner John Doe as an example…

- John wears smart clothing able to record in real time his physical environment
- He's interacting with a human learning specialist, Mary Goodteacher in an outdoor setting
- At the same time, John's wearing AI/AR glasses – thus he's also in an AI/AR learning environment
- John has with him his learning assistant bot - AssistBot
- Fellow learners are with John, AssistBot and the learning specialist all also wearing smart clothing with IoT devices
- Mary GoodTeacher has with her a teaching assistant physical bot – PattyBot and a digital teaching assistant BobBot

All of the above will generate large volumes of data each second – YIKES!!!! So, in today's world there isn't enough data space to store all of this in each learner's LDV. Which then leads to creating consent contracts with the learners about what of their data will be stored and used by Mary Goodteacher, Patty and BobBot and what will be stored in the learner's LDV.

Yes, it will quickly become very complicated at the consent and data levels. That's what this cost centre must address.

LDV Data Sources Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
    - The team should include the following types of people:
      - Learning data experts
      - Learning experts
      - IoT device experts
      - AI system/bot experts
      - Learning institution experts
      - Training company experts
      - AI/AR/VR experts
      - Business process experts
      - Database experts
      - Red team experts
      - Smart digital identity experts
      - Global, learning non-profit experts
      - SOLICT consent experts
      - Co-design experts
      - Lesson learnt expert
  - Create LDV data source use cases
  - Do small, controlled POC's and pilots to see what LDV data works and what doesn't work
  - Understand data volumes and ways to control it
  - Learn from it, and then rapidly scale
  - Transition management of this to the global, independent, learning non-profit

LDV Security Subcomponent Cost Centre:

Background:

Using the same use case as above to illustrate my concerns re security, let's use learner John Doe as an example…

- John wears smart clothing able to record in real time his physical environment
- He's interacting with a human learning specialist, Mary Goodteacher in an outdoor setting
- At the same time, John's wearing AI/AR glasses – thus he's also in an AI/AR learning environment
- John has with him his learning assistant bot - AssistBot
- Fellow learners are with John, AssistBot and the learning specialist all also wearing smart clothing with IoT devices
- Mary GoodTeacher has with her a teaching assistant physical bot – PattyBot and a digital teaching assistant BobBot

All the above are potential attack vectors into the LDV or, creating false, large amounts of data to effectively create a DNS (denial of service) type attack. Couple this with having large numbers of potential attackers (i.e., digital bots), creating large amounts of data for numerous learners, again creating DNS type attacks. It could bring down the entire LDV system with its billions of databases.

There's LOTS of Security Attack Vectors to Consider:

Examples include but aren't limited to:

- Data sources
- API's (including DNS, port security, encryption, etc.)
- Network
- Databases
- Digital signatures
- Business processes
- Non-profit governance and management
- Cloud/servers

Rapid Rate of Change Creating New Attack Vectors:

The rate of change depicted by this curve hypothetically means, EACH HOUR, new attack vectors are being created. To address this, that's why on the right-hand side of the cost component diagram is a global, independent learning non-profit who does 24x7x365 threat analysis against all the LDV attack vectors noted above. It will constantly produce attach threat risk assessments. Thus, a very high threat risk MUST be responded to in an LDV, data source writing to the LDV, LDV API, etc., within hours.

LDV Security Subcomponent Costs:

Costs associated with this Learning Non-Profit - 24x7x365 Threat Assessments Subcomponent Costs section of this document.

LDV Data Centre Subcomponent Cost Centre:

Background:

LDV was created to protect an entity's learning data, mitigating risk of a jurisdiction deleting the learning data of a person. It does this by having all learning data written to a LDV for each person, which exists in the cloud, outside the jurisdiction's control. All of this sounds good on paper, but how will it be deployed, such that it's always available 24x7x365, year after year, and can withstand events like sun GMD EMP/HEMP events noted in "**When Our Digital Legal Identity Trust Goes Poof!**"?

Then there's the sheer volume of the number of databases i.e., billions. How will the data centre/cloud strategy address this? What is the associated design, implementation and maintenance costs associated with this?

My thinking when creating the idea of LDV was the operational cost would be borne by the global, independent learning non-profit. I saw in my mind the global, independent, learning non-profit collecting revenue from each local jurisdiction by licensing to them, at a very low amount, access to the learner's LDV, up to a fixed amount.

All the above is the design and cost challenge of the data centre/cloud strategy LDV will use.

LDV Data Centre/Cloud Subcomponent Costs:

Cost will be borne by the global learning non-profit's Manages LDV Databases Subcomponent Cost Centre section of this document. Also, LDV's EMP/HEMP data centre availability costs will be borne by the non-profit's EMP/HEMP Protection/Power Supply Subcomponent Cost Centre section of this document.:

LDV Database Application Subcomponent Cost Centre:

Background:

LDV is an out of the box idea for out of the box times. My thinking is to explore out of the box database applications as well for LDV rather than simply deferring to use of existing database types.

I'M NOT A DATABASE EXPERT. However, I have a friend, Derek Small, CEO of Nulli, who for the past several years has his company pioneering use of graph databases with IAM (Identity Access Management) systems. I strongly suggest readers read "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

A consideration will be the mapping of legal identity/hive relationships between entities. This will range from:

- One to one
- One to many
- Many to many

The future is telling us many of these relationships might only last seconds to minutes. Skim "**Nanobots, Microbots, Manufacturing, Risk, Legal Identity & Contracts**". Thus, the type of database used must be low cost, efficient, secure, easily upgradeable and function well in a cloud, at very, very fast speeds.

I'M NOT SAYING TO USE GRAPHS WITH LDV. WHAT I AM SAYING IS NOW IS THE TIME TO CONSIDER ALL OPTIONS WHEN ARCHITECTING THE UNDERLYING LDV DATABASE DESIGN.

LDV Database Application Subcomponent Costs:

Costs associated with this will be borne by the Manages LDV Databases Subcomponent Cost Centre section of this document.

LDV Power Consumption Subcomponent Cost Centre:

Background:

Each learner on the planet will have their own LDV database i.e., there will literally be billions of them. Each one consuming electricity.

Thus, as power availability becomes an issue, along with costs, I decided to break out power consumption as its own cost centre. The deliverable of this cost centre is to drive down power consumption per LDV.

Other Cost Centres Dependent Upon This Cost Centre:

- Learning Non-Profit – Power Consumption of LDV and DLT Subcomponent Cost Centre

LDV Power Consumption Subcomponent Costs:

Costs associated with this will be borne by the Learning Non-Profit – Power Consumption of LDV and DLT Subcomponent Cost Centre section of this document.

Very Important Note:
As noted in the Learning Non-Profit – Power Consumption Of LDV and DLT Subcomponent Cost Centre section, the costs will actually be borne by the Legal Identity Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre section of this document.

LDV Infrastructure Updating Subcomponent Cost Centre:

Background:

LDV will likely have billions of learner's databases, which resides in the cloud. This also includes the associated infrastructure from the firewalls, load balancers, API's, network to the actual servers. The entire end-to-end infrastructure must be able to be upgraded on either a regular basis or, in an emergency fix.

EACH LDV must always be available. Finally, as this tech curve unfolds, it means that new tech will rapidly evolve, which hypothetically could mean replacing or rapidly updating the LDV database. All this means, right from the beginning, a secure infrastructure updating model needs to be well thought through, allowing for these possibilities.

LDV Infrastructure Updating Subcomponent Costs:

Costs will be borne in the Learning Non-Profit's Manages LDV Databases Subcomponent Cost Centre section of this document.

LDV Data Standards Subcomponent Cost Centre:

Background:

The driving force behind having a LDV is it's interoperable around the planet both physically and digitally. THUS, AS I SEE IT, ALL OF THE DATA STORD WITHIN EACH ENTITY'S LDV MUST BE TO GLOBAL STANDARDS. This includes data from:

- People
- IoT devices
- AI systems and bots
- Learning institutions
- Physical environments
- AI/AR/VR environments
- Training companies

This is easier said than done. It requires global coordination on learning data standards and standardized learning consent agreements. My advice is to start small i.e., don't boil the ocean. Start with traditional learning data sources and establish standards. Then work from there.

LDV Data Standards Subcomponent Costs:

Costs will be borne by the Non-Profit – Manages LDV (Learner Data Vault) Standards Subcomponent Cost Centre section of this document.

LDV Consent Standards/Agreements/Contracts Subcomponent Cost Centre:

Background:

Our consent legal framework around the planet is badly broke. The "2017 Deloitte Global Mobile Consumer Survey; US Edition" states "**For ages 18 to 34, the rate of acceptance of terms and conditions, without reading them, reaches 97 percent**." Once a person's given their consent, the data can easily flow out of apps, each second, into colossal predictive behavior companies databases like Google, Facebook, Oracle, Acxiom, Alibaba, etc. This data can then be used to predict their behavior and sold to others.

I can see, over time, not overnight, learning consent contract agreements will become standardized. This will help reduce the identity friction and costs, especially as AI (artificial intelligence) leveraged PIAM (personal identity access management) come into being.

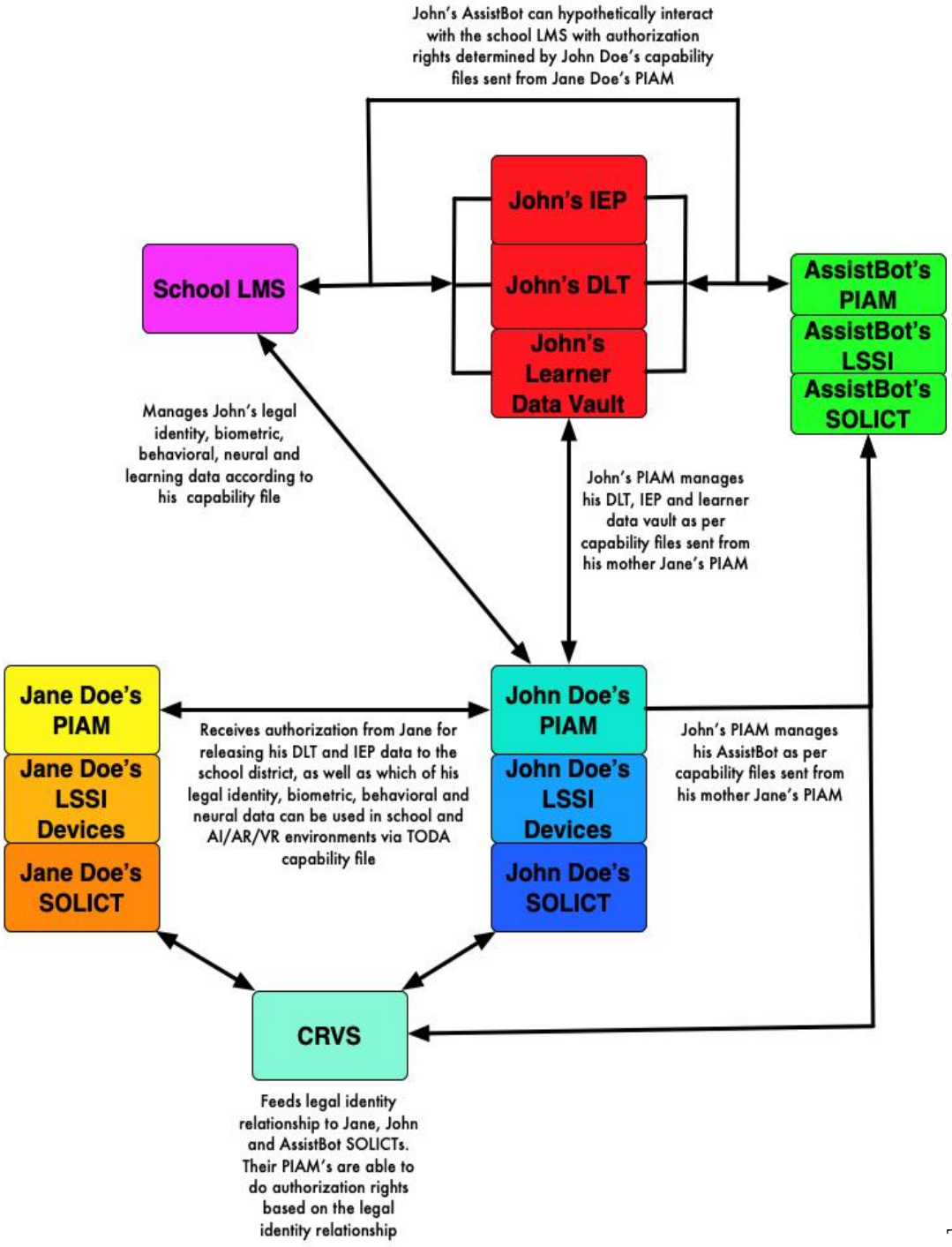
It requires a new toolkit. Skim these:

- "**TODA, EMS, Graphs – New Enterprise Architectural Tools for a New Age**"
- Kantara UMA (User Managed Access)

All learning consent agreements will be stored in the learner's SOLICT.

Learning Consent Agreement Example:

Look at this example to see Jane Doe, giving her consent to a school district, for use of her son and AssistBot's legal identity and learning data.



To make this

LDV Consent Standards/Agreements/Contracts Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
  - The team should include the following types of people:
    - Consent legal experts
    - Learning experts
    - Institutional learning institutions
    - Training companies
    - Database experts
    - Security and red team experts
    - Business process experts
    - Smart digital identity experts
    - AI systems/bots experts
    - IoT devices experts
    - TODA experts
    - Kantara UMA experts
    - Co-design experts
    - Lesson learnt experts
- Suggested Starting Strategy:
  - Don’t boil the ocean trying to determine all types of learning consent contracts i.e., keep the initial focus tight
  - Create use cases for consent agreements with entities like school districts and training companies
  - Create use cases for this
  - Create draft consent agreements
  - Do POC’s and small controlled pilots to see what works and what doesn’t work with the new consent standards
  - Transition management of this to the global, independent, learning non-profit or, to a global standards body administering consent standards

LDV API (Application Programming Interface) Subcomponent Cost Centre:

Background:

The API is the front door to an entity's LDV. It will quickly become an attack target by the Evil Inc.'s and malicious states of the planet. Couple it with this curve. It hypothetically means, EACH HOUR, new attack vectors are being created against the learning framework, of which the LDV is a key part.

I have an underlying premise – only the largest countries and companies around the planet have the resources, expertise, and budgets to continually defend against these new rapid attacks. The rest of us don't i.e., we'll be prone to repeatedly successful attacks against us, including our LDV's.

Which is why the new, global, independent, non-profit is part of the architecture. Its job is to do 24x7x365 threat analysis against the end-to-end legal identity architecture. It will produce rated threat assessments with jurisdictions, companies, enterprises, and entities being required to update in a pre-determined time. This is how to bring current industry best practices to the world of legal identity.

All of which comes to bear with the LDV, and APIs used to write, read and manage each entity's LDV.

LDV API Subcomponent Costs:

The costs associated with this will be borne by the Learning Non-Profit's Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Rethinking Learning - Continual Learning Assessment Subcomponent Cost Centre

Background:

In "**Sir Ken Robinson - You Nailed It!**" it states the following:

> "When John's between 3-4 years old, Jane takes him to a local health clinic. There a physical bot does a learning assessment on John. It measures things like sight, sound, hearing, smell, hand-eye coordination, how he learns, how he doesn't learn, how he works or doesn't work with others, etc. It also measures things like eye blinks per second, where his eyes look, etc. In the not-so-distant future, it will also measure his neurological activity.
>
> All this data is fed into John's new **"Digital Learning Twin" (DLT)**. It's legally tied to John's legal identity. It produces John's first **"Individualized Education Plan" (IEP)**. The IEP is highly tailored to John.
>
> The health clinic gives Jane a learning assistant bot to take home with them, called "AssistBot". AssistBot is designed to work with John each day, measuring how John learns, updating his IEP. All the data about John goes into his **"Learner Data Vault" (LDV)**. Note that John, via Jane, is in control of all his learning data until he comes of legal age.
>
> Also note it's not just the "bot" i.e., tech, working with John. AssistBot watches John at play with other children. Over time, not overnight, AssistBot can build a highly predictive DLT for John, highly tailored to his needs."

At the heart of it is a continual assessment of the learner. My main point? Tech is emerging which has the potential to upend our view of learning. Like what? Go to 19:30 minute mark of "The AI Dilemma". It shows how an AI system can accurately read our minds.

Then read this section I wrote not quite two years ago in "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**":

“John's Neural Data

I was recently introduced to Divya Chander, a physician, neuroscientist, and futurist who trained at Harvard, UCSF, UCSD, and the Salk Institute. She is Chair of Neuroscience and Faculty of Medicine at Singularity University, Visiting Scholar in Medicine (Bioinformatics) at Stanford (where she was on the Anesthesiology faculty for 8 years), and Senior Fellow at the Atlantic Council GeoTech Center. She's been educating me on neural sovereignty and neural rights in the 21st Century. I'M NOT AN EXPERT IN THIS AREA.

She's told me rapid advances in the neural sciences:

Enable us to read and write to the brain

- Connections to computers outside the brain can even enable one to surf the internet
- Brain waves can uniquely identify you, i.e. a "brain print"
- Brain waves and your body can be hacked
- An emerging wide number of neural indicators are increasingly being used to assist companies et al predict our behavior

At which point, even me, a visionary guy, was overwhelmed by the sheer pace and scope of developments. She's working on new rights for all of this, as well as defining standards.

With her permission, she stated in one doc she shared with me about new ethics required:

"**If you believe that these things are true:**

- Each human being has the right to mental privacy
- Each human being has the right to own and control their brain’s data and identifying features
- Each human being has the right to freedom from mental manipulation (their free will)
- A person’s brain, mind, psyche, and memories are part of one’s very Selfhood, and neural rights

can be considered human rights…

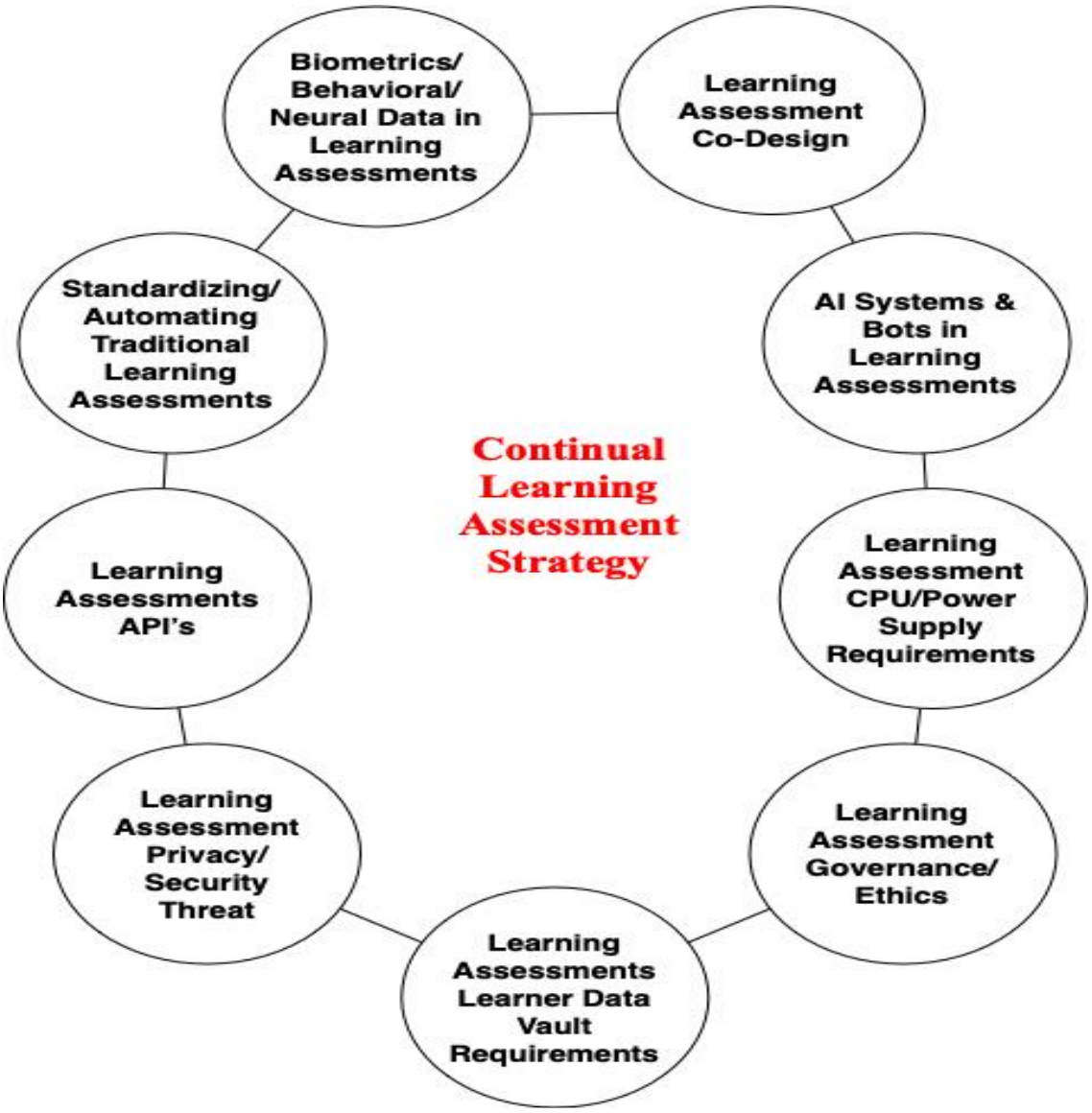
…then we should be arguing for a new code of ethics surrounding neural data and define human rights’ principles that will safeguard them. Those principles should be drafted and reinforced by governments the international community and followed by independent adjudicators. They should also be willingly undertaken by companies in the private sector, especially as there really are no geographic boundaries any longer within which companies operate."

Couple this with the arrival of bots. Skim this website about QTRobot, a bot devoted to Human AI Research and Teaching and their website about leveraging this to work with ASD learners.

Then consider this curve. It's what the people in "The AI Dilemma" were talking about i.e., the sheer rapid pace of tech change. Here's my next point – It will affect how we learn at faster and faster paces.

So, given all the above, here's my strategy to address learning assessments in 2024…

Continual Learning Assessment Strategy Subcomponent Cost Centres Diagram:



Learning Assessment Co-Design Subcomponent Cost Centre:

Background:

Each learner on the planet, regardless of their abilities or disabilities, MUST be able to:

- Understand what learning assessments are
- Know what type of learning assessments are being used with them
- Give their approval (or their parents/legal guardians do) to use their DLT and LDV data as part of the assessment via their LSSI devices and/or PIAM
- Have the assessment occur which is tailored to their learning style and abilities/disabilities
- With the resulting data stored within their LDV

Thus, co-design is mission critical in achieving this. That's what this cost centre is focused on.

Cost Centres Dependent Upon This Cost Centre:

- Co-Design - Continual Learning Assessment Subcomponent Cost Centre

Biometrics/Behavioral/Neural Data in Learning Assessments Subcomponent Cost Centre:

Background:

As mentioned in the above background section, it's now possible for AI to read our brainwaves and write to the brain. Couple this with rapid advances in biometrics and behavioral technology allowing for measurement of biometrics and behavior allowing prediction of our future behavior. All of which can be leveraged in learning assessments.

This subcomponent cost centre focusses on rapid innovation leveraging this to determine what can and can't be used in learning assessments. Its job is to correlate learning assessment with biometrics, behavioral and neural data.

Biometrics/Behavioral/Neural Data in Learning Assessments Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for biometrics, behavioral and neural data in learning assessments
        - The team should include the following types of people:
            - Learning assessment experts
            - Biometric experts
            - Behavioral experts
            - Neural data experts
            - Data experts
            - Network experts
            - Security/red team experts
            - API experts
            - Co-design experts
            - Learning non-profit experts
            - Legal experts
            - Lesson learnt expert
- Start with:
    - Creating use cases for use of biometrics, behavioral and neurodata in learning assessments
    - Identify high level requirements
    - Then drill down to crawling steps, determining costs, resources, and requirements to achieve results
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale

Standardizing/Automating Traditional Learning Assessments Subcomponent Cost Centre:

Background:

Traditional assessments typically include:

- Written assessments
- Performance assessments
- Portfolio assessments

My points:

- The planet's a higgledy-piggledy mess re assessment standards
    - With globalization and digitization, it's time to create global learning assessment standards
- The arrival of technology potentially offers ways to automate sections of the learning assessment

This subcomponent cost centre's tasks are to:

1. Identify traditional learning assessments
2. Create new global learning assessment standards
3. Determine ways to automate some of them to reduce time and costs of conducting the learning assessments
4. Then to track new assessment techniques and create standards for them (like neuro brain reading/writing)

Standardizing/Automating Traditional Learning Assessments Subcomponent Costs:

Costs will be borne by the Non-Profit – Managed Learning Assessment Standards Subcomponent Cost Centre section of this document.

AI Systems & Bots in Learning Assessments Subcomponent Cost Centre:

Background:

In these vision articles, "**Sir Ken Robinson - You Nailed It!**" and "**Vision: Learning Journey of Two Young Kids in a Remote Village**" it describes use of learning assessment bots to evaluate young learners. It's early days for this since the tech is just emerging to do this. Examples include but aren't limited to:

- ADHD:
  - 2018 "**Robot-Assisted ADHD Screening in Diagnostic Process**"
  - 2020 "**A hybrid AI approach for supporting clinical diagnosis of attention deficit hyperactivity disorder (ADHD) in adults**"
  - 2015 "**New software can screen for ADHD by analyzing hand movement**"
  - 2021 "**Using AI technology to support ADHD diagnosis**"
  - 2017 "**Automatic Detection of ADHD and ASD from Expressive Behaviour in RGBD Data**"
- ASD:
  - 2021 "**Personalized Robot Interventions for Autistic Children: An Automated Methodology for Attention Assessment**"
  - 2021 "**The diagnosis of ASD using multiple machine learning techniques**"
  - 2021 "**Deep Neural Network-based Handheld Diagnosis System for Autism Spectrum Disorder**"
  - 2020 "**Automations in the Screening of Autism Spectrum Disorder**"
  - 2020 "**Automating autism assessment: What AI can bring to the diagnostic process**"
  - 2020 "**Automated Detection of Autism Spectrum Disorder Using a Convolutional Neural Network**"
  - 2020 "**Multi-modular AI Approach to Streamline Autism Diagnosis in Young Children**"
  - 2019 "**Effect of a Computer-Based Decision Support Intervention on Autism Spectrum Disorder Screening in Pediatric Primary Care Clinics -A Cluster Randomized Clinical Trial**"
  - 2018 "**An accessible and efficient autism screening method for behavioural data and predictive analyses** "
  - 2017 **An Automated Assessment Framework for Speech Abnormalities related to Autism Spectrum Disorder**"
  - 2016 "**Investigating machine learning techniques for the detection of autism**"

AI Systems & Bots in Learning Assessments Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for use of AI systems and bots in learning assessments
        - The team should include the following types of people:
            - Learning experts
            - Co-design experts
            - AI learning experts
            - Physical bot assessment experts
            - Digital bot assessment experts
            - Data experts
            - Network experts
            - Security/red team experts
            - API experts
            - ADHD/ASD experts
            - Lesson learnt expert
- Start with:
    - Creating use cases for use for leveraging AI, physical and digital bots in learning assessments
    - Identify high level requirements
    - Then drill down to crawling steps, determining costs, resources, and requirements to achieve results
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale

Learning Assessment CPU/Power Supply Requirements Subcomponent Cost Centre:

Background:

Skim "AI Power Consumption Exploding". It describes by 2040-ish, AI will be consuming most of the planet's power. This is unrealistic, yet it's off most peoples' radar screens.

Next skim "Designing AI systems: Fundamentals of AI software and hardware". It describes AI's mammoth CPU requirements.

Finally, skim "**Decentralized AI – Risks, Legal Identity, Consent & Privacy**". It describes the emerging design of decentralizing AI.

I'm NOT an AI or computing expert. However, as a solution architect, I can see major problems coming along with the use of AI and bots used in learning assessments. As the architecture laid out in this document scales across the planet for learning assessments, the challenges of CPU and power supply MUST be addressed. Which is why I've created a separate cost centre to address this.

Cost Centres Dependent Upon This Cost Centre:

- Learning Non-Profit – Power Consumption Of LDV, DLT and Learning Assessments Subcomponent Cost Centre

Learning Assessment CPU/Power Supply Requirements Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Power Consumption Of LDV, DLT and Learning Assessments Subcomponent Cost Centre section of this document.

Learning Assessment API's (Application Programming Interface) Subcomponent Cost Centre:

Background:

The plethora of emerging learning assessment techniques all come with security, privacy, governance and ethics challenges. Other learning assessment subcomponent cost centres address this. However, the API is the electronic front door to the learning assessment technology and data.

Consider this curve. It hypothetically means each hour, new attack vectors are being created against the API's, endpoints, networks, DNS, encryption etc. My point? Most learning institutions and enterprises around the planet DON'T have the expertise, budgets and staff to continually detect new attack vectors and rapidly change API standards to defend.

This is a similar problem described in the Legal Identity Cost Centre: API (Application Programming Interface) section of this document. Thus, I've taken a similar approach when creating the learning architecture.

The new, global, independent, learning non-profit has a subcomponent cost centre addressing API's. Its job is to keep the many learning API's (including learning assessment API's) up to date and secure.

Learning Assessment API's (Application Programming interface) Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning Assessment Privacy/Security Threat Subcomponent Cost Centre:

Background:

The learning architecture, like the legal identity architecture, is built on privacy by design. Thus:

- A learner's consent must be obtained to use their legal identity, biometric, neural and learning data
- Which is stored in their SOLICT (Source of Legal Identity & Credential Truth)
- All learning data about the learner is stored in their LDV (Learner Data Vault)
- Which exists outside a jurisdiction's control which the learner controls (this includes learning assessment data)
- A learner might grant a third party the right to use and store their learning data (like learning assessment data)
- HOWEVER, if the learner is lucky enough to live in a jurisdiction like the EU with GDPR Article 17, "Right to be Forgotten", then the learner can go back and ask the third party to remove their data from its databases

All the above must be "baked" into the learning assessment architecture, business processes, governance, etc.

As well, skim "**AI, Cheating & Future of Schools/Work**". It lays out how learners will leverage the tech to cheat. Thus, this too must be addressed in learning assessment designs.

Then look at this curve. It hypothetically means each hour, new attack vectors are being created against the learning solution framework, including learning assessments. My point? Most learning institutions and enterprises DON'T have the resources, expertise or budgets to continually defend.

Adding all the above up, it requires a new, global, independent, learning non-profit to keep secure the learning assessment solution framework. That's what this cost centre addresses.

Learning Assessment Privacy/Security Threat Subcomponent Costs:

Costs will be borne by the Learning Non-Profit - 24x7x365 Threat Assessment Costs section of this document.

Learning Assessments Learner Data Vault Requirements Subcomponent Cost Centre:

Background:

All learning assessment data must flow into the learner's LDV (Learner Data Vault). Thus, the design of the LDV must be done to accommodate learning assessment data. That's what this cost centre addresses.

Learning Assessments Learner Data Vault Requirements Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages LDV (Learner Data Vault) Standards Subcomponent Cost sections of this document.

Learning Assessments Governance/Ethics Subcomponent Cost Centre:

Background:

The emerging potential use of neurodata in learning assessments, prompted me, not quite two years ago to quote Divya Chander, a noted neuro expert, in "**Kids, Digital Learning Twins, Neural Biometrics, Their Data, Privacy & Liabilities**":

She's told me rapid advances in the neural sciences:

- Enable us to read and write to the brain
- Connections to computers outside the brain can even enable one to surf the internet
- Brain waves can uniquely identify you, i.e. a "brain print"
- Brain waves and your body can be hacked
- An emerging wide number of neural indicators are increasingly being used to assist companies et al predict our behavior

At which point, even me, a visionary guy, was overwhelmed by the sheer pace and scope of developments. She's working on new rights for all of this, as well as defining standards.

With her permission, she stated in one doc she shared with me about new ethics required:

"**If you believe that these things are true:**

• Each human being has the right to mental privacy;

• Each human being has the right to own and control their brain's data and identifying features;

• Each human being has the right to freedom from mental manipulation (their free will);

• A person's brain, mind, psyche, and memories are part of one's very Selfhood, and neural rights

can be considered human rights…

…then we should be arguing for a new code of ethics surrounding neural data and define human rights' principles that will safeguard them. Those principles should be drafted and reinforced by governments the international community and followed by independent adjudicators. They should also be willingly undertaken by companies in the private sector, especially as there really are no geographic boundaries any longer within which companies operate."

All the above is easy to say and darned hard to do. Which is one of the main reasons I created this subcomponent cost centre.

Learning Assessments Governance/Ethics Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for learning assessment governance/ethics
    - The team should include the following types of people:
      - Governance experts
      - Law experts
      - Ethics experts
      - Learning assessment experts
      - Neuro experts
      - Biometric and behavior experts
      - ADHD/ASD experts
      - Security/red team experts
      - Learning non-profit experts
      - Co-design experts
      - Police/enforcement experts
      - Lesson learnt expert
- Start with:
  - Creating use cases for learning assessment governance and ethics
  - Identify high level requirements
  - Then drill down to crawling steps, determining costs, resources, and requirements to achieve results
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale
- As I see it, one of its tasks will be to:
  - Create a guiding set of ethics principles for learners
    - Skim "**Revised Principles of Identity**" to see a set of guiding principles I created for identity
    - I'm NOT a learning expert and thus want this team to create and update a guiding set of ethics learning principles

Rethinking Learning IEP – Individualized Education Plan Subcomponent Cost Centre:

Background:

The IEP was introduced in schools in 1975:

> "The IEP describes how the student learns, how the student best demonstrates that learning, and what teachers and service providers will do to help the student learn more effectively. Developing an IEP requires the team to evaluate the student in all areas of suspected disability, consider the student's ability to access the general education curriculum, consider how the disability affects the student's learning, and choose a federal placement for the student." - https://eric.ed.gov/?id=EJ1013681 .

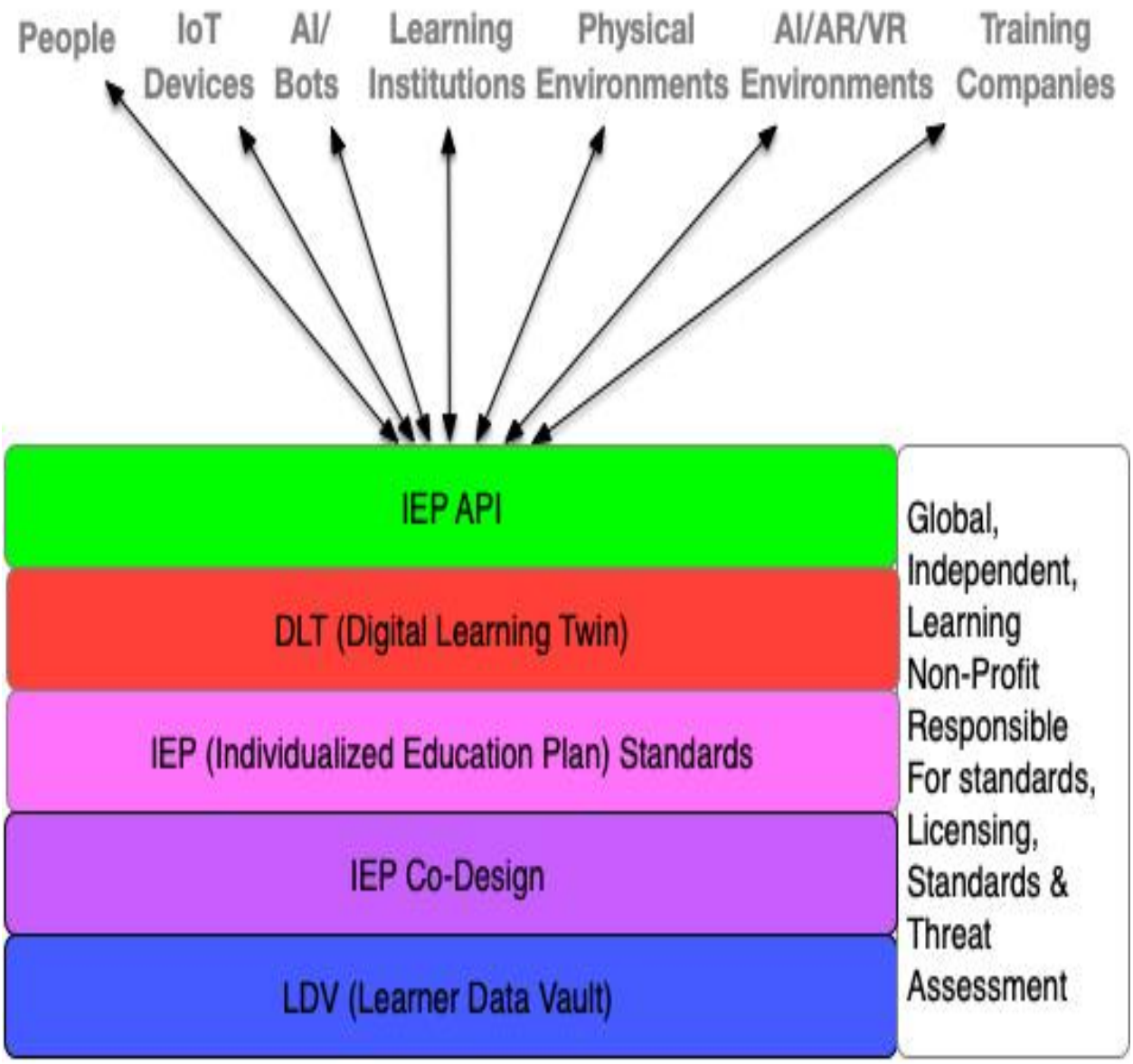
My vision is to give each student on the planet, regardless of their learning abilities, an IEP highly tailored for them. It's continually updated from an increasing rich array of resources i.e., learning assistant bots, teaching assistant bots, humans, and a wide variety of different sensors and assessment devices.

I was told by a winner of the Teaching Award of Canada, that often for ADHD/ASD students the diagnosis is to do one on one instruction. However, since school districts can't afford this, they're often put into small groups, which may or may not work well for the learner.

If one scans current IEP standards (which vary around the planet), you'll find them requiring extensive human input, since currently, there's not lots of different sources of learning data, continually available, to draw upon. My point is I don't want to reduce human interaction, but I want to rethink when humans are used, based on each person's learning needs and learning deliverables required. **AI systems and bots, both physical and virtual, plus a wide variety of sensors, can fill this need. Thus, it's time to rethink IEP's leveraging this.**

However, as noted throughout this document, achieving a vision required crawling steps to then get to walking and running to achieve the vision. Thus, what are the initial crawling steps and costs associated with this?

IEP Subcomponent Cost Centres:



IEP – LDV (Learner Data Vault) Subcomponent Cost Centre:

Background:

All IEP's will be stored within the LDV (Learner Data Vault). Thus, LDV design must take this into consideration.

IEP – LDV (Learner Data Vault) subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages LDV (Learner Data Vault) Standards section of this document.

IEP – Co-Design Subcomponent Cost Centre:

Background:

All learners on the planet, regardless of their abilities or disabilities MUST be able to:

- Understand what an IEP is
- Receive an IEP tailored to their abilities and/or disabilities
- Have it continually updated
- With all learning data stored in their LDV

Thus, co-design is mission critical in delivering this. That's what this cost centre focusses on.

IEP Co-Design Subcomponent Costs:

Costs will be borne by the Co-Design - IEP (Individualized Education Plan) Subcomponent Cost Centre section of this document.

IEP – IEP (individualized Education Plan) Standards Subcomponent Cost Centre:

Background:

Today, around the planet, there's a higgledy-piggledy set of jurisdictional IEP standards. This architecture requires:

- Local/global IEP standards
- Able to give every learner on the planet they're own IEP
- Which can be understood by learning specialists (be they human or AI system/bots) to leverage

Each learner on the planet will have their own IEP, continually updated by their DLT. It's my view the IEP MUST BE DYNAMIC AND CONSTANTLY UPDATED BASED ON THE LEARNER AND THEIR DESIRED LEARNING OUTCOMES. Which is why the cost centre diagram shows bi-directional arrows between the IEP, the learner and other third parties.

All I can see is a rapid rate of change with not only the IEP's but also desired learning outcomes. Why? The introduction of AI leveraged digital identities. Skim "**AI Leveraged Smart Digital Identities of Us**". Thus, what we do, who we do it with, how we learn, how we use the knowledge, etc. will all likely rapidly change over the next 5-10 years.

Bottom line: Each learner's IEP's will also change as learning outcomes rapidly change.

That's what this cost centre delivers.

IEP – IEP (individualized Education Plan) Standards Subcomponent Costs:

Costs will be borne by the Learning Non-Profit Manages IEP (Individualized Education Plan) Standards Subcomponent Cost Centre section of this document.

IEP – DLT (Digital Learning Twin) Subcomponent Cost Centre:

Background:

The DLT is the AI based logic that creates the learner's IEP learning plan and then continuously updates it. The IEP is the output of the DLT.

What's the AI logic that creates the IEP? That's the question this cost centre answers. I'm NOT A LEARNING EXPERT. I expect the DLT/IEP design teams to:

- Identify the learner data points requires to create IEP's
- Determine from the IEP if it's working or not, and then
- Modify the IEP based on this
- All leveraging the IEP standards

IEP – DLT (Digital Learning Twin) Subcomponent Costs:

The costs will be borne by the Learning Non-Profit Manages DLT (Digital Learning Twin) Standards Subcomponent Cost Centre section of this document.

IEP API (Application Programming Interface) Subcomponent Cost Centre:

Background:

The learner's IEP will likely be accessed by MANY third parties, constantly, over their lifespan. The API used to do this is thus the electronic front door to the learner's IEP. How the IEP is accessed thus becomes a critical security and privacy concern.

Look at this diagram. It hypothetically means each hour, new attack vectors are being created against the IEP API. Thus, as in the legal identity architecture, a new, global, independent non-profit is used to do 24x7x365 threat analysis and keep the APIs constantly secure.

Cost Centres Dependent Upon This Cost Centre:

- Learning Non-Profit – Manages Learning API Standards Subcomponent Costs

IEP API (Application Programming Interface) Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Rethinking Learning -Learning API's (Application Programming Interface) Cost Centre:

Background:

A major performance and security question is how to securely access:

- LDV (Learner Data Vault)?
- DLT (Digital Learning Twin) access to the LDV?
- IEP?
- Third party consent agreements about accessing, inputting, and retrieving LDV data (which will be sent to the learner's SOLICT (Source of Legal Identity & Credential Truth)?

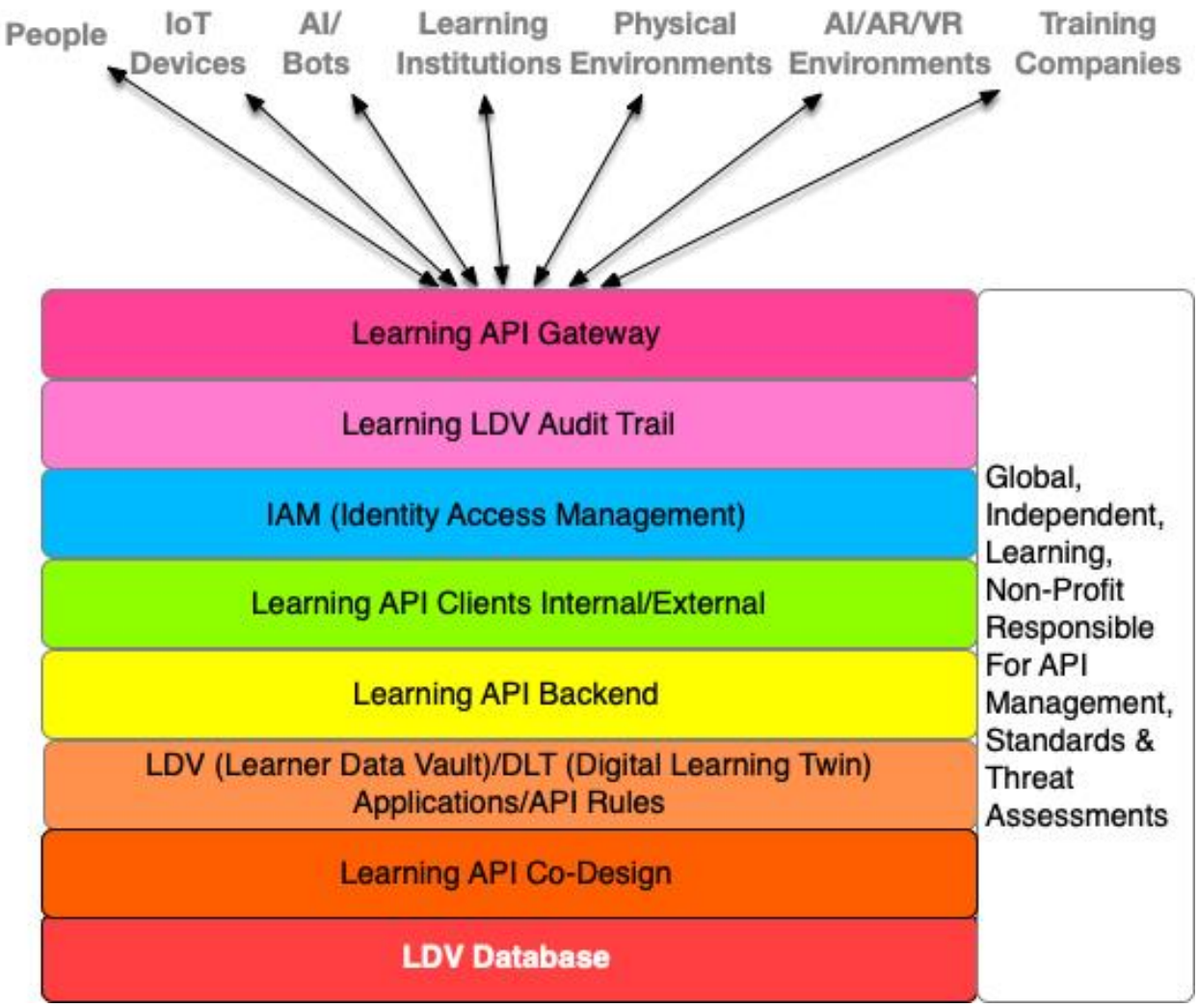
Answer - Create standard API's (Application Programming Interface).

It addresses the problems of how to query billions of learners' LDVs. So, I've included this in the architecture to get discussion and debate going on how this will be addressed.

Add to the above complexity the rapid attack new attack vectors being created against the legal identity framework from this curve. The API is the electronic front door. Which is why the architecture has the new, global, independent, well-funded, non-profit. One of its tasks is to do 24x7x365 threat analysis and produce rated threats and threat responses. Thus, the API's created will likely be very frequently updated.

I'M NOT AN API EXPERT. Thus, what follows is only my best guess at the API cost centres. I'm sure API experts will likely change them.

Learning API Subcomponent Cost Centres:



Note:

The suggested strategy is to do the work in the above cost centres and then transfer over to the learning non-profit API's cost centre to do fast upgrades as required by the threat analysis.

Learning API – LDV (Learner Data Vault) Databases Subcomponent Cost Centre:

Background:

The LDV system in this architecture will become standardized. Thus, from the perspective of creating standardized API's, it can be used with all LDV systems. So, the first place to start with the API is with the underlying LDV database. It's possible to use a data API gateway to access LDV data stored within the database.

All of this must be measured against security and performance.

Learning API – LDV Databases Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning API – Co-Design Subcomponent Cost Centre:

Background:

As API's are developed, it is essential they're extremely well tested. Thus, the API's must be tested with learners all different abilities and disabilities. This is where co-design is critical.

Other Cost Centres Dependent Upon This Cost Centre:

- Co-Design - Learning API Subcomponent Cost Centre

Learning API – LDV Databases Subcomponent Costs:

Costs will be borne by the Co-Design - Learning API Subcomponent Cost Centre section of this document.

Learning API – Applications/API Rules Subcomponent Cost Centre:

Background:

These are the following applications APIs should be designed for:

- LDV
- DLT
- PIAM
- Sending learning consent agreements to the learner's SOLICT via:
    - TODA – skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**"
    - Kantara UMA – skim Kantara UMA Working Group

API – Applications/API Rule Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning API - Backend Subcomponent Cost Centre:

Background:

The API calls will likely be translated into actions leveraging tech like Enterprise Service Bus (ESB), a database, another cloud service, a microservice, application, or web server. Thus, these must be specified, designed for, tested, and kept up to date from a security perspective.

Learning API - Backend Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning API – Clients Internal/External Subcomponent Cost Centre:

Background:

The client is a set of development tools to test and debug API's. These need to be carefully selected and use for internal and external clients.

Learning API – Clients Internal/External Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning API – IAM (Identity Access Management) Subcomponent Cost Centre:

Background:

When IAM came into being in the late 90's, it was built on authoritative identity sources feeding an LDAP (Lightweight Directory Access Protocol) on top of which the IAM system functioned. This model isn't going to work well anymore. Why?

Fast changing legal identity entity relationships. As explained throughout this document, hive relationships can be one to one, one to many, and many to many with fast changing relationships. LDAP is a poor choice for this, while graphs are likely much better.

Then there's the speed at which new entities can be created. An AI system, in one jurisdiction, can create digital bots at speeds of thousands to millions per second, which in the next second can be operating in all other jurisdictions on the planet. If these require registration showing hive relationships, then I'm not sure if graphs can work at such speeds.

Add to this the ability to confirm a CRVS legal identity entity data transfer occurred on X date, at Y time, containing a file Z, at transactional speeds. This requires use of TODA which isn't used today in IAM systems.

For information on graphs and TODA skim, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

Then there's the arrival of PIAM (Personal Identity Access Management) systems. This creates a very decentralized IM system. As noted in the PIAM Cost Centre section of this doc, it will likely become a very fast-moving standard, with lots of changes. **The PIAM will be used by the learner to grant consents to access their LDV data.**

Finally, add to this the security effects of this curve. That's where the new, global, independent non-profit comes into play with 24x7x365 threat analysis against end-to-end legal identity framework.

My point? OUR OLD IAM ARCHITECTURE ISN'T GOING TO WORK. DESIGNERS TAKE NOTE.

Learner API – IAM (Identity Access Management) Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning API – Audit Trail Subcomponent Cost Centre:

Background:

The audit trail is an essential component to the security and legal functioning of the:

- LDV
- DLT
- PIAM
- Consent agreements stored within the learner's SOLICT

TODA is a critical part of this because it can confirm on X date, at Y time, a file Z, was sent between two endpoints. Skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools for a New Age**".

A SECURE AUDIT API MUST BE DESIGNED AND IMPLEMENTED ALLOWING ADMINISTRATORS FAST ACCESS TO THE AUDIT LOGS/APPLICATIONS.

Learning API – Audit Trail Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Learning API – API Gateway Subcomponent Cost Centre:

Background:

The gateway provides the visible URL for a learning API, applies rules for use of the learning API, and then directs the learning API call to the back-end implementation. Rules include:

- Authentication and authorization
- Certificate management, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) termination and Mutual TLS
- Rate limiting and throttling
- Payload inspection (including payload size and the means to validate that the payload is structurally correct)
- Intelligent routing (routing based on the header or payload content)
- As importantly, from a security perspective, is the endpoint configuration, DNS standards, encryption, etc. to which API rules must be designed for

Learning API – API Gateway Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Costs section of this document.

Rethinking Learning - Learning Environments Subcomponent Cost Centre:

Background

The world of learning is changing. With the advent of tech like AI, AR, VR, and a whole slew of devices able to detect, record and leverage a person's biometrics and behavioral data, it changes where and how a learner learns. It's now no longer mainly confined to classrooms in schools.

As an example, my wife works with high school kids and employers arranging for them work-experience programs that line up with their interest's post-secondary. This involves arranging contracts between the student, the employer, and the school district. My point?

As wearable teach infiltrates workplaces, homes, and schools, suddenly contracts in the future will need to specify what data can be collected, how it will be used, stored, archived, and terminated. Additionally, competencies the student gains outside of the traditional school environment can be measured, and assigned to the student, to new global standards.

Soon, as John Doe, in school district X, in Jurisdiction Y, is doing a virtual work experience using AI/AR/VR with an employer in Jurisdiction Z, means contracts now need to be able to function across many different jurisdictions. Thus, I believe there are fundamental components of these types of contracts, which will be the same across many jurisdictions.

Yes, it's complicated. No, we shouldn't try to solve the planets legal contract problems with students et al, all at once. Instead, to be successful, we must learn to crawl first, then walk and run.

Thus, in the cost section, you'll see it suggesting:

- Finding 1-3 jurisdictions with education systems wanting to work with
- Find willing businesses/employers to work with who can offer students work experiences, etc.
- Leverage co-design to enable students with different abilities and disabilities to work in the workplaces
- Leverage the SOLICT/LSSI infrastructure to generate contracts with people
- The contracts for a learner/employer/etc./ should be stored in the learner's SOLICT
- Developing global standards for learning contracts & competencies the learner gains out in the real world

Other Cost Centres Dependent Upon This Cost Centre:

- Co-Design - Learning Environments Subcomponent Cost Centre

Learning Environments Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning Environment Projects Subcomponent Cost Centre section of this document.

Rethinking Learning - LMS (Learning Management Systems) Subcomponent Cost Centre:

Background:

Since the late 80's, standards have been developed for learning management systems:

- 1988 – **AICC** (Aviation Industry Computer-based Training Committee) -
- 2001 – **SCORM** (shareable Content Object Reference Model)
- 2010 – **LTI** (Learning Tools Interoperability)
- 2011 – **LRS** (Learning Reference Store) - https://adlnet.gov/publications/2016/05/Choosing-a-Learning-Record-Store-LRS/
- 2013 – **xAPI**
- 2015 – **cmi5**
- **Open LMS**

A good overview of LMS can be found in "**Chapter 4 - All About the LMS Standards and Specifications by Colleen Griffiths**".

Here's my main points:

- The advent of the DLT (digital learning twin)
- Coupled with highly customized IEP (Individualized Education Plan)
- With individual learner data vaults (LDV)
- With the emergence of learning assistant bots/teaching assistant bots
- And the beginnings of standardized contracts which are stored in either the person's SOLICT or their education data vault
- Changes the underlying LMS landscape
- **It puts the learner front and centre in controlling their own learning rather than being "taught" by a school, school district, post-secondary or enterprise training system, with their learning data stored beyond their control**.

Having said this, it's not going to happen overnight. Thus, this cost centre focuses on crawl, walk and then run stages.

I can also see how LMS systems will need to be able to create interfaces to all learners on the planet, regardless of their abilities or disabilities. This is where co-design is mission critical.

Other Cost Centres Dependent Upon This Cost Centre:

- Co-Design - LMS (Learning Management System) Subcomponent Cost Centre

Learning Management Systems Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages LMS Standards Subcomponent Cost Centre section of this document.

Rethinking Learning - Learning Competencies/Credentials Subcomponent Cost Centre:

Background:

Bad news - around the planet, proving you've had a secondary or post-secondary credential is difficult digitally. Why? There are few global standards for education credentials.

Good news – Since 2012, and established as a foundation in 2016, the Groningen Declaration Network (GDN), is a global non-profit dedicated to creating standards for digital learner data portability.

Today students can learn via AI/AR/VR environments and traditional on-line learning, along with an increasing ability to digitally apply for jobs, post-secondary enrollment, trades, professions etc. Thus, not having global standards presents problems for not only students, but also governments, institutions and businesses trying to confirm the learner's credentials.

SOLICT/LSSI/PIAM offers a new solution for the learner being in control of their learning credentials. HOWEVER, it requires education institutions around the planet to be able to do the following:

- Write an education credential to global standards
    - i.e., Groningen type standards
- Be able to digitally sign the credential, proving the learner received it from a credible education institution
- Leverage the same API to securely export the credential out of the education institution to a learner's SOLICT, via a TODA file i.e., on X date, at Y time, credential Z was sent from the educational institution to Jane Doe's SOLICT file
    - By leveraging the same API which the global, independent non-profit for legal identity constantly does threat assessments against, ensures the long-term security of the educational institutions end point

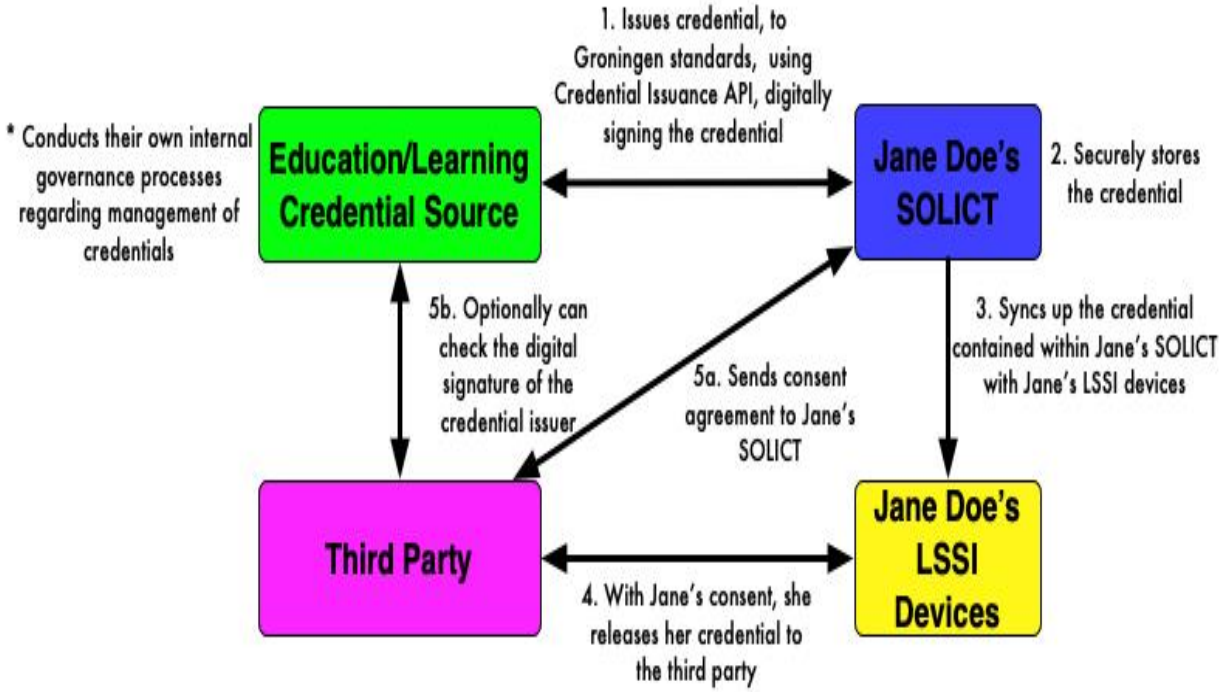
Note: The strategy this document suggests for processes for issuing the education credential is the same as the one suggested in "Cost Centre: Authoritative Credentials Source section of this document.

Additionally, all students around the planet, regardless of their abilities or disabilities, MUST be able to:

- Understand what a learning competency/credential is
- Know what learning competency/credentials they have
- Be able to choose what learning competency/credentials they want to release to a third party
- Have their LSSI devices and/or PIAM instantly, securely execute this

This is where co-design is critical.

Learning Credential Vision:



Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning – Outside the Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre
- Co-Design – Learning Competencies/Credentials Subcomponent Cost Centre
- Learning Non-Profit Learning Competencies/Credentials Subcomponent Cost Centre

Learning Competencies/Credentials Exported to SOLICT by the Authoritative Government Source to Global Standards Costs:

Costs will be borne by the Cost Centre: Authoritative Credentials Source and by Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) sections of this document.

Rethinking Learning - Learning Competencies/Credentials Subcomponent Costs:

Costs will be borne by the Learning Non-Profit Learning Competencies/Credentials Subcomponent Cost Centre section of this document.

Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre:

Background:

Six decades ago, when I was young child. I was dyslexic. My parents hired a private teacher to work with me. Luckily, I quickly learnt to scan from left to right. However, as noted in "**My Learning Journey**, this experience made me closely watch as others learnt. I watched many of my fellow classmates fall off the learning conveyor belt described in "**Sir Ken Robinson - You Nailed It!**" It led me to do lots of change management in the education system as a volunteer.

The reason I tell you this is 8 years ago I wanted to rethink learning from the learner on up, starting when they're a toddler. I realized I couldn't create a new learning architecture without first rethinking a legal identity architecture for humans, AI systems and bots. 8 years later, all the prior 439 pages of this cost centre document is required to get to this cost centre i.e. thinking outside the box from the learner's perspective.

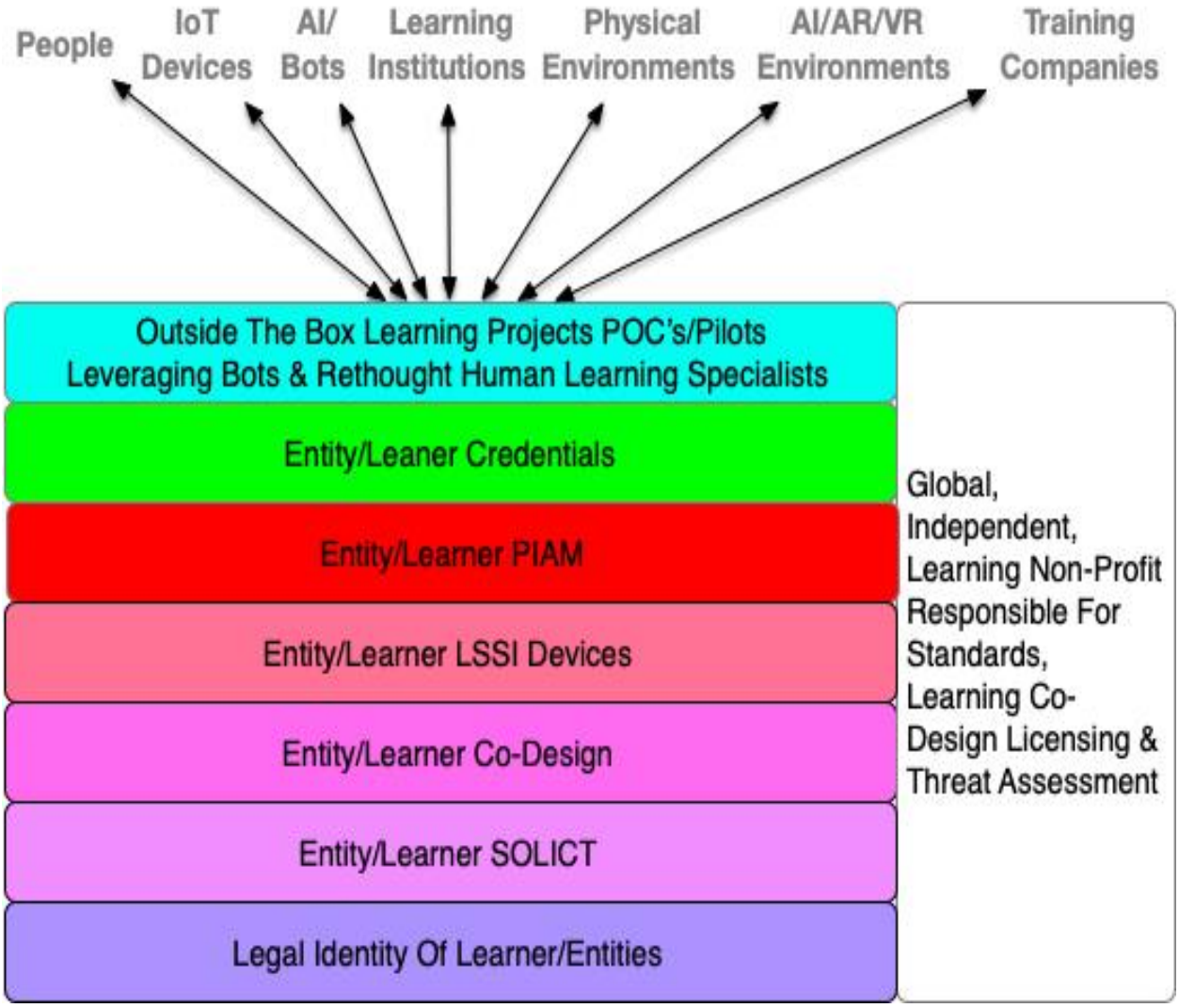
I can see leveraging:

- DLT leveraging all sorts of new data points about the leaner e.g. neural and biometric data, behavioural data, etc.
- Producing continually customized IEPs for each learner
- Different types of physical and digital bots to acts as learning assistants or specialized teaching assistants
- Rethought teachers (which I call human learning specialists)
- Many different types of learning/training environments including AI/AR/VR, workplace environments, etc.
- Rethought learning assessments
- Etc.

It will likely take a year to implement all the components this document focusses on. I can see in years two and three, all sort of outside the box learning projects spinning up.

Do I know what they are? No. However, I've allocated funds for 30 outside the box learning projects, which leverage the architectures, to rethink learning, for all learners, regardless of their abilities or disabilities. It's time to dream a new learning future.

Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Diagram:



Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre
- Cost Centre – SOLICT (Source of Legal Identity & Credential Truth)
- Co-Design - Outside The Box Learning POC's & Pilots Subcomponent Cost Centre
- Non-Profit – Manages LSSI Standards Subcomponent Cost Centre
- Non-Profit – Manages PIAM Standards Subcomponent Cost Centre
- Rethinking Learning – Learning Competencies/Credentials Subcomponent Cost Centre
- Learning Non-Profit – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre

Legal Identities Of Both Humans and AI Systems/Bots Cost:

Costs or determining legal identities of both humans and AI systems/bots will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre section of this document.

Entity SOLICT Costs:

Entity SOLICT costs will be borne by the Cost Centre – SOLICT (Source of Legal Identity & Credential Truth) section of this document.

Co-Design Costs:

Co-design costs will be borne by the Co-Design - Outside The Box Learning POC's & Pilots Subcomponent Cost Centre section of this document.

Entity LSSI Devices Costs:

Entity LSSI Devices costs will be borne by the Non-Profit – Manages LSSI Standards Subcomponent Cost Centre section of this document.

Entity PIAM Costs:

Entity PIAM costs will be borne by the Non-Profit – Manages PIAM Standards Subcomponent Cost Centre section of this document

Entity Credential Costs:

Credential costs will be borne by the Rethinking Learning – Learning Competencies/Credentials Subcomponent Cost Centre section of this document.

Outside The Box Learning Projects POC's/Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre:

Background:

As just stated, the vision is to spin up 30 outside the box learning projects leveraging the architecture this document addresses. Do I know what they should be? No. That will be something for the learning non-profit folks, and especially the co-design experts, to dream up innovative approaches for all learners, regardless of their abilities or disabilities.

In the spreadsheet most of the costing for the 30 projects begins in year two. Why? It will likely take a year to spin up all the other cost centres this document addresses, getting them to pilot and production systems.

I can see a core team of people who oversee and manage the 30 projects. Some of their team might be involved in some of the projects. This team can be spun up in the second half of the first year.

This is what the outside the box learning projects then leverages. It's time to create new learning systems from when the learner is a toddler until they're old.

Outside The Box Learning POC's/Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre:

Costs will be borne by the Learning Non-Profit – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre section of this document.

Rethinking Learning - Making Learning Vision Work in Remote, Poor Areas Subcomponent

Background:

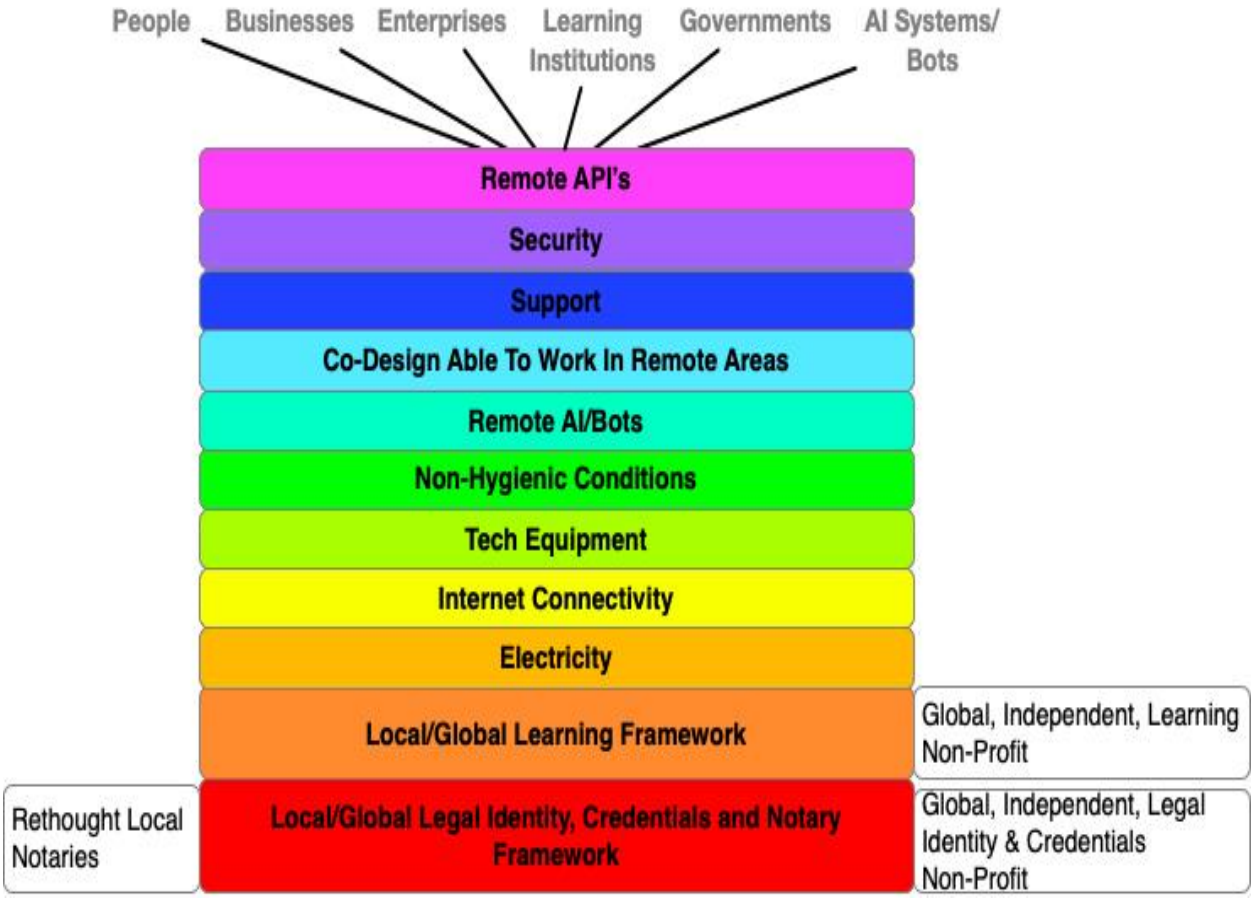
To see a vision story about leaving no learner behind on the planet who lives in remote areas, skim "**Learning Journey of Two Young Kids In A Remote Village**". There are many challenges associated with this idea, including but not limited to:

- Lack of electricity
- Lack of cheap, reliable internet connectivity
- Criminals who might want to steal the bots used in small villages
- Lack of local support facilities for things like AI/AR/VR environments
- Etc.

It's what I call in my head a "whopper challenge". So, what are the potential cost centres associated with this?

Making Learning Vision Work in Remote, Poor Areas Cost Centres Diagram:

I'M NOT AN EXPERT IS ANY OF THESE AREAS, so experts may have better ideas on the cost centres.



Local/Global Legal Identity, Credentials and Notary Framework Subcomponent Cost Centre:

Background:

This is the learner's:

- Legal identity provided by the CRVS and the learner's SOLICT, LSSI devices and PIAM
- Legal relationships
- Legal authorization rights/hives
- Credentials the learner has acquired
- Ability to work with a local notary to verify legal identity and/or credentials if required
- The learner's LDV, DLT and IEP

Cost Centres Dependent Upon This Cost Centre:

- Cost Centre: Rethought CRVS (Civil Registration Vital Statistics)
- Cost Centre: Authoritative Credentials Source
- Cost Centre – Legal Identity & Hive Relationships
- Cost Centre – Legal Authorization Rights
- Cost Centre – SOLICT (Source of Legal Identity & Credential Truth)
- LSSI Devices Cost Centre
- Cost Centre - PIAM (Personal Identity Access Management) System
- Cost Centre: API (Application Programming Interface)
- Cost Centre: Rethought Notaries
- Cost Centre - Global, Independent Legal Identity & Credential Non-Profit
- Rethinking Learning – Co-Design Cost Centre
- Rethinking Learning DLT – Digital Learning Twin (DLT) Cost Centre
- Rethinking Learning LDV - Learner Data Vault Subcomponent Cost Centre
- Rethinking Learning - Continual Learning Assessment Subcomponent Cost Centre
- Rethinking Learning IEP – Individualized Education Plan Subcomponent Cost Centre
- Rethinking Learning -Learning API's (Application Programming Interface) Cost Centre
- Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre
- Rethinking Learning - Learning Environments Subcomponent Cost Centre
- Rethinking Learning - LMS (Learning Management Systems) Subcomponent Cost Centre
- Rethinking Learning - Learning Competencies/Credentials Subcomponent Cost Centre
- Rethinking Learning - Global, Independent, Learning Non-Profit Component Cost Centre
- Co-Design Making Learning Work In Remote Areas Subcomponent Cost Centre

Local/Global Legal Identity, Credentials and Notary Framework Subcomponent Costs:

Costs will be borne by the Non-Profit - Manages Legal Identity Standards for Humans/AI Systems/Bots Subcomponent Cost Centre, the Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre and the Non-Profit - Manages Notary Standards For Legal Identity & Credentials Subcomponent Cost Centre section of this document.

Local/Global Learning Framework Subcomponent Cost Centre:

Background:

This is the learner's:

- LDV
- DLT
- IEP
- Continual Learning Assessment
- Learning API
- Learning Environment
- LMS
- Learning Competencies/Credentials

Local/Global Learning Framework Subcomponent Costs:

The costs will be borne by the Rethinking Learning - Global, Independent, Learning Non-Profit Component Cost Centre section of this document.

Remote Electricity Subcomponent Cost Centre:

Background:

Around the planet, there's several different types of off-grid renewable energy programs including but not limited to:

- **Africa** – World Bank – "**Lighting Up Africa: Bringing Renewable, Off-Grid Energy to Communities**"
- **Southeast Asia** – "**PLN Achieving 100% Electrification: The Role of Distributed Energy**"
- **Central Asia** – "**The Energy Situation in Central Asia: A Comprehensive Energy Review Focusing on Rural Areas**"
- **South America** – "**Options for Resilient and Flexible Power Systems in Select South American Economies**"
- **North America**
  - **Canada** – "**Market Snapshot: Overcoming the challenges of powering Canada's off-grid communities**"
  - **US (Alaska)** – "**Renewable electricity generation for off grid remote communities; Life Cycle Assessment Study in Alaska, USA**"
- **Europe** – "**Remote areas can now access low-emission, highly efficient off-grid electricity and heat**"
- **South Pacific** – "**Pacific Energy Update 2020**"
- **Australia/NZ** –
  - **Australia** – "**Off grid - Australian Renewable Energy Agency (ARENA)**"
  - **NZ –** "**The People in Remote Area are Starting to Experience Electricity**"
- **China** – "**MICROGRIDS FOR ELECTRICITY GENERATION IN CHINA**"

Note: The location of the remote pilot sites will drive a localized solution. However, it's important to do lessons learnt to then assist in rapidly scaling in other pilots having similar electricity generation requirements.

Remote Electricity Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - Remote electrical generation experts
            - Remote internet connectivity experts
            - Learning experts
            - Legal experts
            - Privacy experts
            - Security/red team experts
            - Standards experts
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Network/connectivity experts
            - Identity experts
            - Lesson learnt experts
- Start with determining potential energy consumption requirements from:
    - Rethought learning environment for the pilot site
    - Other localized energy consumption requirements
- Identify high-level requirements
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above
- Pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar electrical grid requirements

Costs for this cost centre are TBD (To Be Decided) by the experts and the initial funding country.

Remote Internet Connectivity Pilot Subcomponent Cost Centre:

Background:

Bottom Line: "Two thirds of the world's school-age children have no internet access at home, new UNICEF-ITU report says". So, the strategy is to use a rethought learning architecture and infrastructure, to drive this into place, starting with small pilots in 1-3 jurisdictions. There are several innovative internet connectivity projects including but not limited to:

- **Africa** – "**The Digital Moonshot: Bringing Universal Internet Access in Africa**"
- **Southeast Asia** – "**Development in Southeast Asia: Opportunities for donor collaboration**"
- **Asia** – "**How Central Asia can ensure it doesn't miss out on a digital future**"
- **South America** – "**Closing the digital gap to end poverty in Latin America and the Caribbean**"
- **North America:**
  - US:
    - "**5 steps to get the internet to all Americans - Brookings Institution**"
    - "**PCI - The Tribal Resource Center: Digital Opportunities Through Tribal Broadband**"
  - **Canada**: - "**Broadband Fund: Closing the digital divide in Canada**"
  - **Mexico -** "Mexico wants internet access for all. Getting everyone online could reduce poverty, too"
- **South Pacific – "Broadband Connectivity in Pacific Island Countries**"
- **Europe** – "**The Digital divide in Europe - Towards meaningful connectivity**"
- **Australia/NZ**:
  - **Australia** – "**Digital divide': 2.5 million Australians with no internet connection**"
  - **NZ** – "**Digital inclusion and wellbeing in New Zealand**"

Remote Internet Connectivity Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - Remote internet connectivity experts
            - Learning experts
            - Legal experts
            - Privacy experts
            - Security/red team experts
            - Standards experts
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Network experts
            - Identity experts
            - Lesson learnt experts
- Start with determining the most cost-effective internet connectivity requirements for the pilot sites:
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above
- Pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar internet connectivity requirements

Costs for this cost centre are TBD (To Be Decided) by the experts and the initial funding country.

Remote Tech Equipment Subcomponent Cost Centre:

Background:

Throughout the rethought learning cost centre, it refers to leveraging emerging tech such as AI/AR/VR et al to then rethink assessments, take the data into a DLT, create customized IEP's for each child, and then continually refine the IEP's leveraging assessments, biometric/behavioral data, et al. My dumb question to funders who want to do this in poor, remote locations on the planet is, "How will we make this work in challenging operating conditions?"

As mentioned in the Remote AI/Bots Cost Centres section, the devices will have to perform in a wide range of different operating conditions. Further, it's also highly likely criminals will want to take the tech for themselves by forcibly stealing it.

Then there's the price points of the tech to consider i.e., we're piloting this in very poor parts of the planet. Finally, there's the support to consider i.e.., the local support centre might be a VERY LONG WAYS AWAY. Add it all up, and it's another significant challenge, which is why I've made it a separate cost centre.

As stated in the other remote pilot cost sections, rather than trying to solve all the planet's remote tech challenges, I suggest the design requirements come out of the 1-3 pilots we're going to first do. See what didn't work, what worked, learn from it and then rapidly apply it to sites with similar operating characteristics.

Remote Tech Equipment Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - AI/AR/VR tech experts/vendors
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Bot experts with experience designing bots to operate in challenging conditions
            - Bot experts with experience designing bots to operate in potentially hostile environments where malicious people might want to effectively kidnap the bot, take it away and use it for their own purposes
            - Remote internet connectivity experts
            - Remote location experts
            - Learning experts
            - Legal experts
            - Privacy experts
            - Security/red team experts
            - Standards experts
            - Network/connectivity experts
            - Identity experts
            - Co-design experts
            - Lesson learnt experts
- Start with determining the bot requirements for the pilot sites
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above
- Pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar bot operating requirements

Remote Non-Hygienic Conditions Subcomponent Cost Centre:

Background:

I've been in many poor villages around the planet. Many of them aren't hygienic. It's not inconceivable that bots and tech equipment can be dropped into pools of urine, shit, mud, etc. Thus, this reality must be addressed to in any rethought learning pilots in remote, poor locations.

I'M NOT AN EXPERT IN THIS. Thus, what follows is simply my best guess at a cost-centre. It's likely experts who work constantly in such remote locations will amend what follows. My strategy, as repeatedly stated throughout the remote cost section, is to let the 1-3 pilots drive requirements for devices etc.

I've broken this out as a separate section, since there should likely be resources assigned to just focus on this. I can see lessons learnt people on the team, documenting what didn't work, what worked and then, based on this, adjusting future roll-our strategies.

Remote Non-Hygienic Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - Non-hygienic experts
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Bot experts with experience designing bots to operate in challenging conditions
            - Remote internet connectivity experts
            - Learning experts
            - Legal experts
            - Co-design experts
            - Privacy experts
            - Security/red team experts
            - Standards experts
            - Network/connectivity experts
            - Identity experts
            - Lesson learnt experts
- Start with determining non-hygienic requirements for the pilot sites
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above and pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar bot operating requirements

Remote AI/Bots Subcomponent Cost Centre:

Background:

It's one thing to talk of leveraging bots in urban areas to do learning assessments, teaching assistant, and learning assistance, but it's completely another challenge when one think of using this in remote parts of the planet. As per some of the other cost centres in this section, there are major challenges with electricity, connectivity, non-hygienic conditions, security, sensor input devices (e.g., AI/AR/VR, etc.) and support challenges. Depending on where the pilot sites are located there also may be extremely dry, cold, wet, sand, etc. conditions to also deal with.

Then there's the security issues to also consider. In my head, I can see a criminal gang walking into the pilot village and forcibly taking the bots with them to use as and where they see fit. This is yet another design challenge most people likely aren't even thinking of.

Add it all up, and therefore I've created this as a separate cost centre. There's lots of problems to solve which likely require significant investment of very skilled resources and research to drive a successful design and implementation into place.

Depending on the connectivity available for a pilot site, the design team must also decide how much of the assessment, DLT and IP update processing to do within the bots rather than having it done by a cloud system. If this is the case, then periodic updating to a master system in the cloud can be scheduled.

I'M NOT AN AI BOT EXPERT, NOR AM I AN EXPERT IN HANDLING VERY CHALLENGING OPERATING ENVIRONMENTS. Thus, what follows is only my best guess to identifying cost centres. I'm sure, real experts will recommend a more detailed and accurate approach.

My strategy is to again not try to solve all the planet's bot operating challenges. Instead, I'm recommending focusing down on 1-3 pilots, in remote locations, carefully selected by experts to do the initial pilots in. Learn from what didn't work, what worked, and then rapidly scale to other similar sites.

Regarding bots:

- Look at the Spot video which shows bot development for operating in tough conditions
- Then look at QT Robot, a learning assistant bot
- Watch Boston Dynamics bots doing a parkour course

My goal is to take this kind of tech, mesh it up with Spot type tech, and create the beginnings of a remote learning bot infrastructure.

Remote AI/Bots Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Bot experts with experience designing bots to operate in challenging conditions
            - Bot experts with experience designing bots to operate in potentially hostile environments where malicious people might want to effectively kidnap the bot, take it away and use it for their own purposes
            - Remote internet connectivity experts
            - Learning experts
            - Legal experts
            - Privacy experts
            - Co-design experts
            - Security/red team experts
            - Standards experts
            - Network/connectivity experts
            - Identity experts
            - Lesson learnt experts
- Start with determining the bot requirements for the pilot sites
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above
- Pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar bot operating requirements

Co-Design Able To Work in Remote Areas Subcomponent Cost Centre:

Background:

Because of remote locations, it's highly likely there will be unexpected challenges with learners having different learning abilities and disabilities. This cost centre focusses on this.

Note: It leverages the Learning Non-Profit's Co-Design Team and cost centres.

Co-Design Able To Work in Remote Areas Subcomponent Cost:

Costs will be borne by the Co-Design Making Learning Work In Remote Areas Subcomponent Cost Centre section of this document.

Remote Support Subcomponent Cost Centre:

Background:

Remote locations bring with it additional challenges in providing support. The location might be a very long way from support centres, the communication might not always be reliable, etc. Thus, different ways of providing support must be considered in the design, implementation, and maintenance phases of the pilots. That's why I've created this as a separate cost centre.

I'M NOT AN EXPERT IN REMOTE SUPPORT. Thus, I'm sure experts who are, will amend my best guesses below.

Remote Support Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - Tech support experts with lots of remote experience
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Bot experts with experience designing bots to operate in challenging conditions
            - AI/AR/VR support experts
            - Tech infrastructure experts
            - Remote internet connectivity experts
            - Learning experts
            - Legal experts
            - Co-design experts
            - Privacy experts
            - Security/red team experts
            - Standards experts
            - Network/connectivity experts
            - Identity experts
            - Lesson learnt experts
- Start with determining support requirements for the pilot sites
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above and pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar support operating requirements

Remote Security Subcomponent Cost Centre:

Background:

As stated throughout the pilot cost centre section of this document, there are additional security concerns. Remote locations often have remote security challenges with criminals, etc. forcibly operating and taking away things they want to use. Add to this, criminals wanting to hack into the rethought learning infrastructure to either use the connectivity et al for their own purposes or, to obtain villagers ID's et al to then masquerade as them. Yes, it's complicated, which is why I've created this as a separate cost centre.

I'M NOT AN EXPERT IN REMOTE SECURITY. Therefore, what follows is only my best guess. Remote security experts will likely want to amend what follows.

Remote Security Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 pilot sites within jurisdictions to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for a rethought global, independent non-profit
        - The team should include the following types of people:
            - Remote physical and digital security experts
            - Security/red team experts
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Bot experts with experience designing bots to operate in challenging conditions
            - Tech infrastructure experts
            - Remote internet connectivity experts
            - Learning experts
            - Legal experts
            - Co-design experts
            - Privacy experts
            - Standards experts
            - Network/connectivity experts
            - Identity experts
            - Lesson learnt experts
- Start with determining security requirements for the pilot sites
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above and pilot this
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale in other locations having similar security operating requirements

Remote API's Subcomponent Cost Centre:

Background:

Dependent upon location, connectivity, and tech used, it may or may not affect the way that APIs are used. Thus, I created this cost centre to potentially focus on this as conditions arise.

Remote API's Subcomponent Costs:

Costs will be borne by the Learning Non-Profit – Manages Learning API Standards Subcomponent Cost Centre section of this document.

Rethinking Learning - Global, Independent, Learning Non-Profit Component Cost Centre

Background:

This curve frequently referred to in this document created problems that Albert Einstein was quoted as saying, "**We can't solve problems by using the same kind of thinking we used when we created them.**" Change happens faster and faster, potentially creating new attack vectors each hour.

Our old learning and legal identity systems weren't built for this. **The curve requires out of the box thinking for out of the box times.** Which is why this architecture models what the legal identity architecture specified i.e. creation of a global, independent non-profit, but a sperate one for the learning solution framework. Its job is to do the following:

- Establish and maintain new LDV (Learner Data Vault) standards
- Establish and maintain new DLT (Digital Learning Twin) standards
- Establish and maintain Learning Assessment standards
- Establish and manage IEP (Individualized Education Plan) standards
- Manages LDV databases
- License LDV/DLT to jurisdictions & training companies
- Does 24x7x365 threat analysis against not only the tech used in learning solution framework, but also the governance, business processes and end users, issuing rated threat assessments, which people, IoT devices, AI systems/bots, learning institutions & training companies respond, within certain time periods, based on threat levels
- Manages learning API standards
- Manage learning co-design standards

The actual learning participants legal identities and their education/learning credentials can be protected by the proposed global, independent non-profit proposed throughout the global, independent legal identity non-profit. However, it can't, and shouldn't be responsible for learning system protection and standards. That's why I've included in the architecture, a separate global, independent learning body to do this. They'll handle the learning systems, DLT, IEP, assessment, learner data vaults, API's et al.

The non-profit will exist in 3 different physical locations, 8 time zones apart. It begs the question, who'll pay for it?

My strategy is to use a similar funding model that's proposed for the SOLICT/LSSI/PIAM/API legal identity non-profit. I'm proposing each educational jurisdiction around the planet pay an annual small license fee per student, to a maximum yearly amount. This would fund the non-profit.

Why should a jurisdiction license the above? It will reduce their costs. How? From the moment a learner shows up at their door, they'll be able to access their LDV's and IEP's. It will allow for

streamlining the traditional yearly class structure by being able to leverage tech to aid a learner to learn, faster, cheaper and better.

For example, consider the West Vancouver School District where I live. The district, or the provincial ministry of education, would pay a fee per each of their students enrolled in the school district to the global non-profit. In return they can leverage the standards for the DLT, IEP, learner data vault, LMS et al as part of the products they buy, subscribe to, or build themselves. As importantly, they'd also continually receive rated threat assessments 24x7x365.

As part of the license agreement, they'd agree to respond accordingly. So, a very low risk might take months or longer to address, while a very high risk would be responded to within hours. This is bringing current industry best practices to the new emerging world of learning.

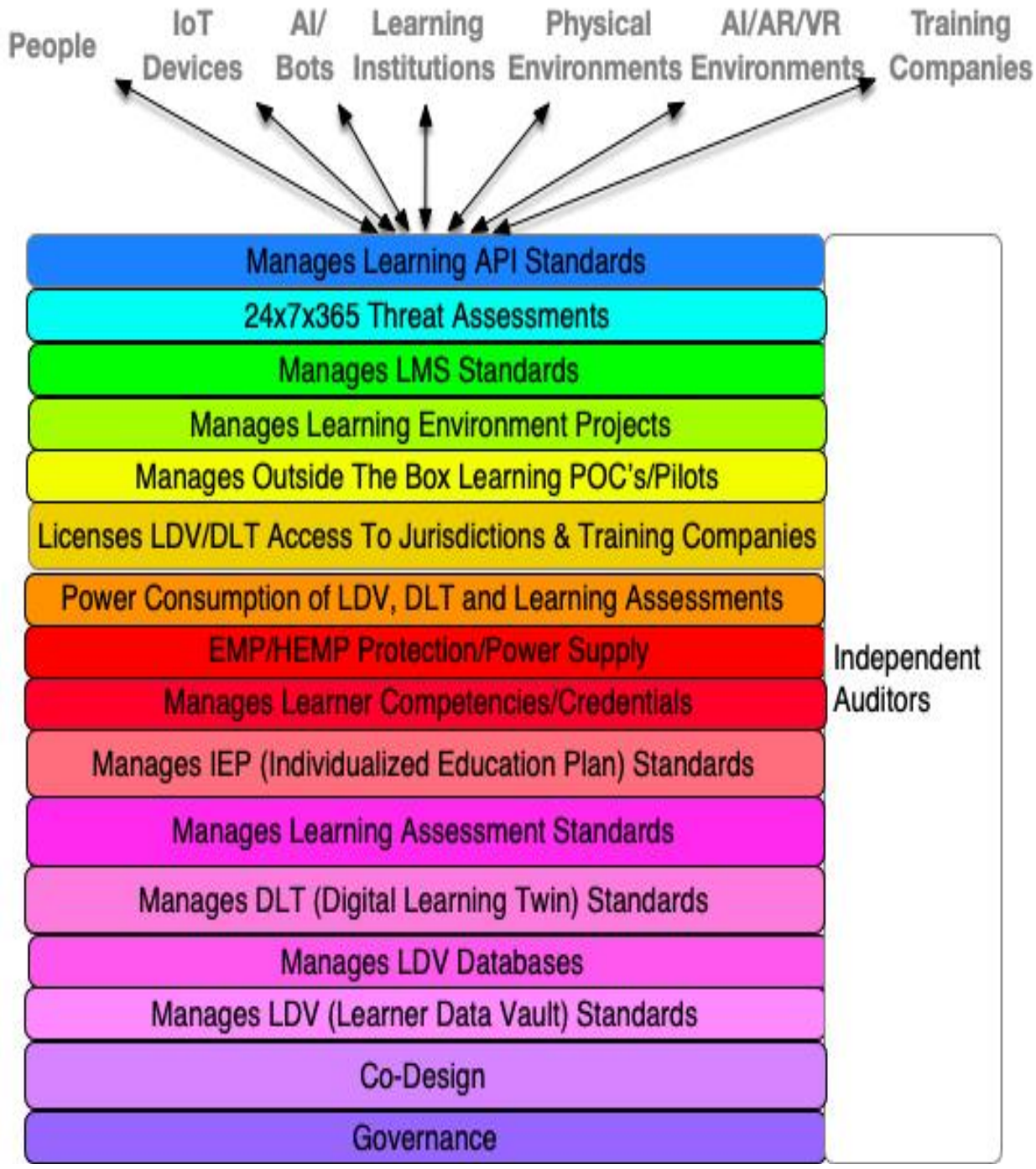
It also applies to the vendors. For example, a learning assist bot vendor would pay a small fee to leverage the global learning standards and incorporate them into their products/services. They'd agree to respond in a similar manner to threat assessments.

The fees must be low per student and per vendor, to ensure wide adoption and continued use of the standards and threat assessment response framework. It must encourage innovation caused by the curve, while at the same time rapidly adopting security frameworks for new threats.

Finally, I again note this is a visionary architecture document. It will take time to be deployed in 1-3 educational jurisdictions around the planet with vendors participating. Using the crawl, walk and run strategy.

That's what this cost centre delivers. It's out of the box thinking for out of the box times.

Global, Independent, Learning Non-Profit Subcomponent Cost Centres Diagram:



Learning Non-Profit - Governance Subcomponent Cost Centre:

Background:

The non-profit, who's operating in a VERY political world, must not be political. How can this be done? I suggest the following membership by type of representatives:

- Other global standards bodies
- Global non-profits
- UN
- Universities
- Industry

I suggest the representative numbers chosen must ensure that to fundamentally change the global non-profit requires 66% of the members to support a change. This stops quick movements to take control of the board, yet it doesn't stop change from occurring to the non-profit.

I can see the body's headquarters being in a country well respected for being independent and stable. However, having said this, the actual operational piece of the global non-profit should be in three separate locations, roughly 8 time zones apart. Why?

Its job is to do 24x7x365 threat assessments as the planet turns. Further, if some type of disaster occurs in one or more locations, the non-profit keeps operating. So, this needs to be baked into the cost structure.

Governance costs also include management, HR, accounting, finance, payroll et al.

While a lot of the work of the non-profit will be done via the threat assessment part of it, an equally vital part is the legal team the non-profit has. Its work will cross over all jurisdictions, laws and regulations around the planet. Thus, it's very important to have a well-respected legal team, with LOTS of connections around the planet. Their job is to navigate potentially politically treacherous waters. I feel this non-profit must be created rather than assigning its functions to an existing non-profit body. It must be "politically squeaky clean" from the beginning.

The non-profit will likely manage standards for LDV, DLT, and IEPs. This too is very political. Thus, very careful political consideration must be given to representation on the various standards bodies.

The licensing aspect of the global non-profit is equally important from a governance perspective. Very careful political thought must be paid to how this is perceived around the planet.

Also, there's the LDV operations component, which also has a very political component to it as well. How the data is stored, where it's stored, how it's accessed all can quickly become political footballs. Thus, very careful political attention also needs to be given to this.

At a minimum, LDV systems must be available at 5 9's availability (99.999% uptime is required) i.e., 5.26 minutes downtime per year. It would be desirable if it was 6 9's (99.9999%) i.e., 31.56 seconds downtime per year.

Finally, management of the global, independent, non-profit must be done by a well-respected team. It's the heart of setting standards and protecting learners and their data around the world. Thus, the management team must be of trusted people who can act independently, despite lots of political pressure from various groups.

Learning Non-Profit Governance Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

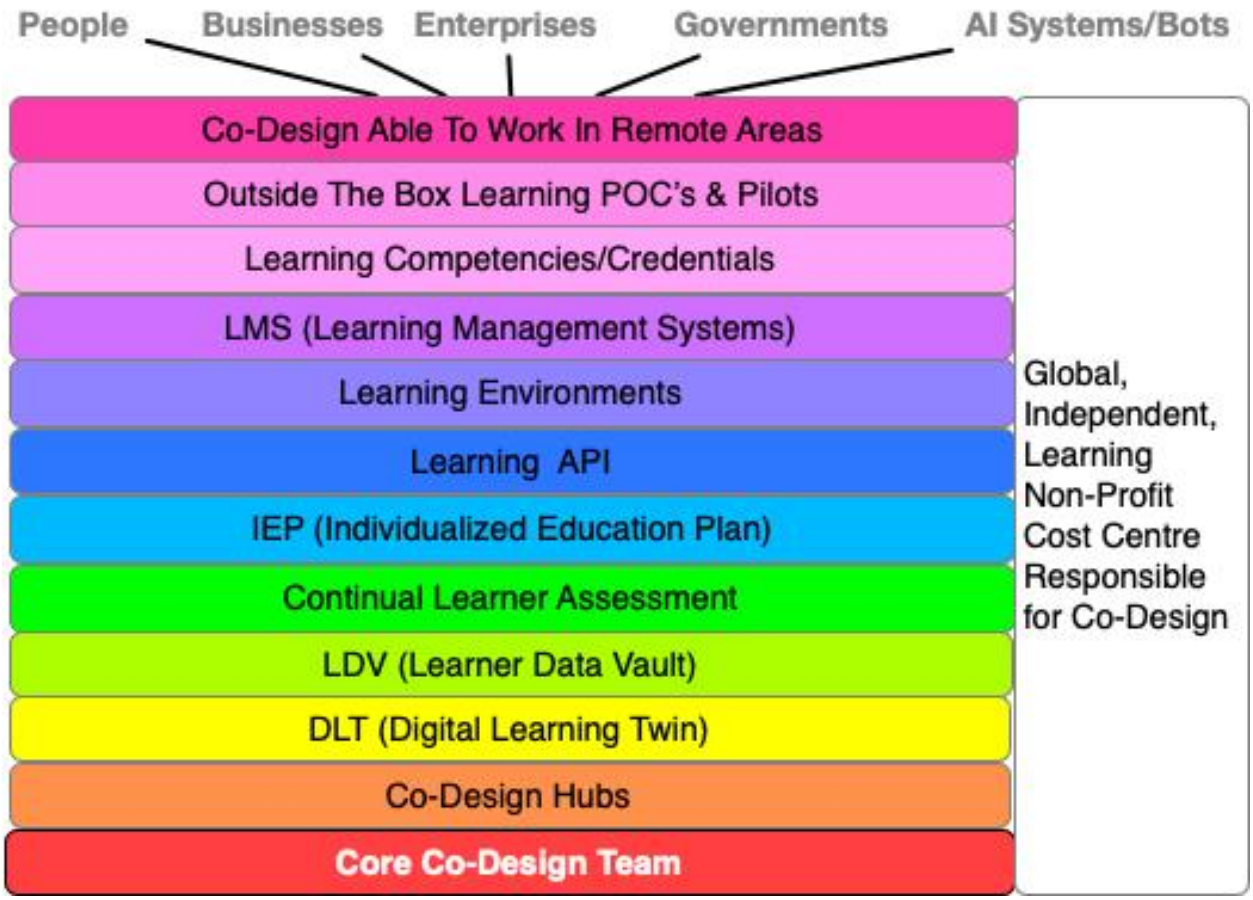
- Fund and create a small team composed of:
  - Global, independent non-profit experts
  - Legal experts
  - Political experts
  - LDV experts
  - IEP experts
  - DLT experts
  - Licensing experts
  - Database experts
  - AI systems, physical and virtual bot experts
  - Smart digital identities experts
  - Learning institutions
  - Training companies
  - Business process experts
  - Co-design experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Data centre/cloud experts
  - Lesson learnt experts
- Create high level governance requirements, use cases, and cost estimates
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground

Learning Non-Profit – Co-Design Subcomponent Cost Centre:

Background:

As stated in "Vision – Co-Design 'Nothing About Us Without Us' and throughout this doc, co-design is mission critical in enabling people to understand and use the legal identity, credential and learning architecture. As importantly, the section "Us "contains very useful lessons for the team managing this cost centre to learn from.

Learning Non-Profit – Co-Design Subcomponent Cost Centres Diagram:



Other Cost Centres Dependent Upon This Cost Centre:

- Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Subcomponent Cost Centre
- Rethinking Learning – Co-Design Cost Centre
- DLT – Co-Design Subcomponent Cost Centre
- LDV Co-Design Subcomponent Cost Centre
- Learning Assessment Co-Design Subcomponent Cost Centre
- IEP – Co-Design Subcomponent Cost Centre

- Learning API – Co-Design Subcomponent Cost Centre
- Rethinking Learning - Learning Environments Subcomponent Cost Centre
- Rethinking Learning - LMS (Learning Management Systems) Subcomponent Cost Centre
- Rethinking Learning - Learning Competencies/Credentials Subcomponent Cost Centre
- Rethinking Learning – Outside The Box POC's & Pilots Subcomponent Cost Centre

VERY IMPORTANT NOTE:

As stated throughout this document I'm NOT a co-design expert. Given this, here are my thoughts:

The learning architecture is built on top of the legal identity and credential architecture. Thus, in the beginning, the learning co-design team will be heavily reliant upon the legal identity and credential co-design team.

Therefore, I'm suggesting that in the early days, the learning co-design team become part of the legal identity and credential co-design team. While the learning co-design team focusses on "learning", I think that there will be lots of initial cross-over between the two teams. Both teams can leverage the same co-design hubs. When the time is right, the two teams can separate.

If co-design experts agree with this suggestion, then it complicates the budgeting and governance structures. Why? The two teams in the end will reside in separate non-profits. Thus, it requires an initial flexible approach in governance and budgeting until the two teams decide it's time to separate.

Note: For this version of the Excel spreadsheet, I've left separate the two non-profit's co-design teams.

Core Co-Design - Team Subcomponent Cost Centre:

Background:

Note: I'M NOT A CODESIGN EXPERT. THUS, WHAT'S WRITTEN BELOW WILL LIKELY BE EDITED AND ADJUSTED BY PEOPLE THAT ARE.

The core co-design team is composed of many different types of people including:

- People with a wide variety of disabilities
- People of different genders
- People of different ages
- People of different first nations
- Experienced psychologists, psychiatrists and physiotherapists who work with people having learning/training disabilities
- VERY experienced co-design team leaders who've already successfully implemented co-design projects
- Legal experts who are experienced in learning/training laws and regs pertaining to people with disabilities having access to learning/training systems
- Business process experts who are experienced in delivering learning/training services to people with disabilities
- Governance experts who are experienced in delivering learning/training citizen facing governance solutions involving co-design
- Security experts who are experienced in delivering learning/training citizen facing security solutions involving co-design
- Etc.

I suggest that a core team of co-design people be created which will be used for all the co-design subcomponent cost centres depicted in the pic at the beginning of this section. Where specific subcomponent cost centres require additional expertise or different types of people with disabilities, then the team will be expanded to include them.

Non-Profit Core Co-Design Team Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - People with a wide variety of disabilities
  - People of different genders
  - People of different first nations
  - People with a wide variety of ages
  - Experienced psychologists, psychiatrists and physiotherapists who work with people having disabilities
  - VERY experienced co-design team leaders who've already successfully implemented learning co-design projects
  - Legal experts who are experienced in learning/training laws and regs pertaining to people with disabilities having access to learning/training systems
  - Business process experts who are experienced in delivering learning/training services to people with disabilities
  - Governance experts who are experienced in delivering learning/training citizen facing governance solutions involving co-design
  - Security experts who are experienced in delivering learning/training citizen facing security solutions involving co-design
  - Notary experts experienced in learning /training credentials
  - Lesson learnt experts
  - Etc.
- Create high level requirements, use cases, and cost estimates for:
  - Annually running the core co-design team in one country and their local state/provinces jurisdictions for the following subcomponent cost centres:
    - Co-Design Hubs
    - DLT (Digital Learning Twin)
    - LDV (Learner Data Vault)
    - Continual Learning Assessment
    - IEP (Individualized Education Plan)
    - Learning API
    - Technology Learning Assistant Bots/Human Learning Specialists
    - Learning Environments
    - LMS (Learning Management Systems)
    - Learning Competencies/Credentials
    - Making Learning Work in Remote Areas
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work, and then adjust the core team accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - Hubs Subcomponent Cost Centre:

Background:

Note: I'M NOT A CODESIGN EXPERT. THUS, WHAT'S WRITTEN BELOW WILL LIKELY BE EDITED AND ADJUSTED BY PEOPLE THAT ARE.

While reading Marie Johnson's excellent book, **Nadia – Politics, Bigotry, Artificial Intelligence",** I was educated about why co-design hubs are critical for enabling people with disabilities to participate in co-design. Thus, I've created this cost centre embracing this.

Depending on the country that initially funds, the number of co-design hubs required will likely vary. To create my first high-level cost guesstimate, I've used the number of 30 co-design hubs to begin with. Whatever the final number, my advice to the team responsible for this subcomponent cost centre is drive out a budget cost per co-design hub which can be used within the initial country to calculate total guesstimated costs for all the hubs.

Non-Profit Co-Design Hubs Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - People who've created co-design hubs before
- Create high level requirements, use cases, and cost estimates for:
  - Cost guesstimates to create each co-design hub
  - Total number of co-design hubs required
  - Annual costs for running the
  - Annually running the co-design hubs in one country and their local state/provinces jurisdictions for the following subcomponent cost centres:
    - DLT (Digital Learning Twin)
    - LDV (Learner Data Vault)
    - Continual Learning Assessment
    - IEP (Individualized Education Plan)
    - Learning API
    - Teaching/Learning Assistant Bots/Human Learning Specialists
    - Learning Environments
    - LMS (Learning Management Systems)
    - Learning Competencies/Credentials
    - Making Learning Work In Remote Areas
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design hubs, and then adjust the hubs accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - DLT (Digital Learning Twins) Subcomponent Cost Centre:

Background:

The DLT is all about leveraging co-design to create learning for people of all abilities and disabilities. As importantly, a learner, regardless of their abilities or disabilities should be able to understand:

- What they're DLT is
- What it can do for them
- How it works

That's what this co-design centre addresses. Thus, it's mission critical that the co-design team responsible for the DLT be part of the design, testing, implementation and maintenance process from the beginning.

Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning DLT – Digital Learning Twin (DLT) Cost Centre
- DLT – Co-Design Subcomponent Cost Centre

Co-Design - DLT (Digital Learning Twins) Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - LDV (Learner Data Vault) Subcomponent Cost Centre:

Background:

Every learner on the planet, regardless of their abilities or disabilities MUST know:

- What their LDV is
- What's stored in it
- What they can and can't do with the data stored within it
- How they can use their LSSI devices and PIAM to release portions of their learning data, with their consent, to third parties

That's what this cost centre delivers.

Cost Centres Dependent Upon This Cost Centre:

- LDV Co-Design Subcomponent Cost Centre

Co-Design - LDV (Learner Data Vault) Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - Continual Learning Assessment Subcomponent Cost Centre:

Background:

Each learner on the planet, regardless of their abilities or disabilities, MUST be able to:

- Understand what learning assessments are
- Know what type of learning assessments are being used with them
- Give their approval (or their parents/legal guardians do) to use their DLT and LDV data as part of the assessment via their LSSI devices and/or PIAM
- Have the assessment occur which is tailored to their learning style and abilities/disabilities
- With the resulting data stored within their LDV

Thus, co-design is mission critical in achieving this. That's what this cost centre is focused on.

Other Cost Centres Dependent Upon This Cost Centre:

- Learning Assessment Co-Design Subcomponent Cost Centre

Co-Design - Continual Learning Assessment Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - IEP (Individualized Education Plan) Subcomponent Cost Centre:

Background:

All learners on the planet, regardless of their abilities or disabilities, MUST be able to:

- Understand what an IEP is
- Receive an IEP tailored to their abilities and/or disabilities
- Have it continually updated
- With all learning data stored in their LDV

Thus, co-design is mission critical in delivering this. That's what this cost centre focusses on.

Other Cost Centres Dependent Upon This Cost Centre:

- IEP – Co-Design Subcomponent Cost Centre

Co-Design - IEP (Individualized Education Plan) Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - Learning API Subcomponent Cost Centre:

Background:

As API's are developed, it is essential they're extremely well tested. Thus, the API's must be tested with learners all different abilities and disabilities. This is where co-design is critical.

Other Cost Centres Dependent Upon This Cost Centre:

- Learning API – Co-Design Subcomponent Cost Centre

Co-Design - Learning API Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - Learning Environments Subcomponent Cost Centre:

Background:

In Rethinking Learning - Learning Environments Subcomponent Cost Centre section of this document it states:

- Finding 1-3 jurisdictions with education systems wanting to work with
- Find willing businesses/employers to work with who can offer students work experiences, etc.
- Leverage co-design to enable students with different abilities and disabilities to work in the workplaces

Co-design is thus required in meeting this.

Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning - Learning Environments Subcomponent Cost Centre

Co-Design - Learning Environments Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - LMS (Learning Management System) Subcomponent Cost Centre:

Background:

In the "Rethinking Learning - LMS (Learning Management Systems) Subcomponent Cost Centre" section of this document it states:

> "I can also see how LMS systems will need to be able to create interfaces to all learners on the planet, regardless of their abilities or disabilities. This is where co-design is mission critical. "

Thus, that's why I created this subcomponent section to focus on it.

Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning - LMS (Learning Management Systems) Subcomponent Cost Centre

Co-Design LMS (Learning Management System) Subcomponent Costs:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design – Learning Competencies/Credentials Subcomponent Cost Centre:

Background:

The Rethinking Learning - Learning Competencies/Credentials Subcomponent Cost Centre section of this document states:

> Additionally, all students around the planet, regardless of their abilities or disabilities, MUST be able to:
>
> - Understand what a learning competency/credential is
> - Know what learning competency/credentials they have
> - Be able to choose what learning competency/credentials they want to release to a third party
> - Have their LSSI devices and/or PIAM instantly, securely execute this

This is where co-design is critical.

Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning - Learning Competencies/Credentials Subcomponent Cost Centre

Co-Design – Learning Competencies/Credentials Subcomponent Costs:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design - Outside The Box Learning POC's & Pilots Projects Subcomponent Cost Centre:

Background:

As stated in Rethinking Learning – Outside The Box POC's & Pilots Subcomponent Cost Centre section of this document, co-design is a critical component in creating outside the box learning POC's and pilots. That's what this cost centre focusses on.

Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning – Outside The Box POC's & Pilots Subcomponent Cost Centre

Co-Design - Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centres above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Co-Design Making Learning Work In Remote Areas Subcomponent Cost Centre:

Background:

As noted in Co-Design Able To Work in Remote Areas Subcomponent Cost Centre:

> "Because of remote locations, it's highly likely there will be unexpected challenges with learners having different learning abilities and disabilities. This cost centre focusses on this."

Cost Centres Dependent Upon This Cost Centre:

- Co-Design Able To Work in Remote Areas Subcomponent Cost Centre

Co-Design – Making Learning Work In Remote Areas Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Determine any additional personnel requirements that the core co-design team doesn't have and budget for them
- Create high level requirements, use cases, and cost estimates for the co-design team re noted subcomponent cost centre above
- As the above subcomponent cost centres begin, learn what works, and more importantly what doesn't work re co-design members and resources, and then adjust accordingly
- Next, prepare to adjust this cost centre as other countries and their local jurisdictions adopt the new legal identity, credential and learning architectures
- Rapidly scale around the planet

Learning Non-Profit – Manages LDV (Learner Data Vault) Standards Subcomponent Cost Centre:

Background:

The LDV - Learner Data Vault Subcomponent Cost Centre section of this document lays out the complexity of providing each entity they're own LDV. As one can see, it's very, very complicated. Thus:

- THE ACTUAL SOLICT STANDARD MUST BE BASED ON A WIDE VARIETY OF USE CASES
- AS MUST BUSINESS PROCESS AND SECURITY STANDARDS RE LDV MUST BE BASED ON A WIDE VARIETY OF USE CASES

On a slightly related note:

Not quite two years ago, I wrote "A Database Per Entity on the Planet - A Deeper Dive on SOLICT". I haven't found time to update it re legal hive relationships and authorization rights for humans, AI systems and bots. While the SOLICT and LDV are quite different, the operational complexity is very similar. So, with this caveat, it's an excellent background read for the LDV standards team.

Other Cost Centres Dependent Upon This Cost Centre:

- LDV Data Standards Subcomponent Cost Centre
- Learning Assessments Learner Data Vault Requirements Subcomponent Cost Centre
- IEP – LDV (Learner Data Vault) Subcomponent Cost Centre

Learning Non-Profit Manages LDV (Learner Data Vault) Standards Subcomponent Costs:

Note: It's highly likely this standards group should also be part of the LDV Data Standards Subcomponent Cost Centre. For this version of the document, I've left it separate.

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
    - The team should include the following types of people:
      - Learning data experts
      - Learning experts
      - Co-design experts
      - IoT device experts
      - AI system/bot experts
      - Learning institution experts
      - Training company experts
      - AI/AR/VR experts
      - Business process experts
      - Database experts
      - Red team experts
      - Smart digital identity experts
      - Global, learning non-profit experts
      - SOLICT consent experts
      - Lesson learnt expert
  - Create LDV data standards use cases
  - Do small, controlled POC's and pilots to see what LDV data standards works and what doesn't work
  - Learn from it, and then rapidly scale

Learning Non-Profit Manages LDV Databases Subcomponent Cost Centre:

Background:

When creating the new legal identity framework, I wanted to architect it such that a malicious state couldn't delete all identity records for an identity. When Scott David, University of Washington, gave me the idea of creating, for each person, a separate database, which they can control, that exists in the cloud, outside of a jurisdiction's reach, I realized this was the solution I'd been looking for. I then applied it as well to a learner's data by creating the LDV.

YET, THERE'S A BIG BUT WHICH COMES WITH IT. WHO PAYS FOR, RUNS AND SECURELY MANAGES THE LIKELY TRILLIONS OF SOLICT DATABASES?

I figured out a way for the global, independent, non-profit to fund it via licensing. It's the performance and security which most concerns me:

Security Challenges – Performance & Security

SOLICT and LDV will become key to a learner wanting to write learning consents to their SOLICT with immediate interactions with their LDV.

Performance:

I can see, as LDV's become used by billions of people, demand on the cloud-based databases will become very high. Thus, this must be built into the design.

Security:

I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks, leveraging digital bots and AI systems against the learning systems via their LDV API's. They could effectively "drown the LDV" with lots of either read or write requests. The Evil Inc's will effectively want to shut down learning within a jurisdiction demanding ransom requests. Thus, this must be addressed in design use cases.

Updating:

I could also see the business process problems of keeping track of billions of LDV's. It requires high availability of the end-to-end SOLICT system. Updates must be made live with little or no downtime i.e. 5'9's or 6'9's (99.999-99.9999% availability).

All of the above must be addressed in design use cases.

Then there's the issue of the actual underlying database. As described in "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**", I can see the possibility of graph databases being used to map the many, fast changing, learning device relationships to a learner. **Yet, a question in my mind is can graphs perform at these very fast, very high-volume speeds and loads? TODA can but I'm not sure of graphs.**

Add to this the overall security framework for the graph databases. **How can say Jane Doe be sure her LDV data isn't being seen or worse, modified by the global, non-profit's analysts, AI systems, bot or management?**

Finally, the SOLICT is the key architectural performance linchpin for an entity operating second-by-second in today's world. **How will the underlying data centres, clouds, etc. be managed to be available at a minimum of 5 9's (99.999%) or even 6 9's (99.9999%)? (5 9's is a downtime of 5.26 minutes per year, while 6 9's is a downtime of 31.56 seconds per year).**

Other Cost Centres Dependent Upon This Cost Centre:

- LDV Data Centre Subcomponent Cost Centre
- LDV Database Application Subcomponent Cost Centre
- LDV Infrastructure Updating Subcomponent Cost Centre
- Legal Identity Non-Profit – Manages SOLICT Databases Subcomponent Cost Centre

VERY IMPORTANT NOTE:

This cost centre will be responsible for billions of LDV databases. In the Legal Identity Non-Profit, it will be responsible for billions of LDV databases. Thus, here's my suggestion…

Rather than initially have each non-profit figuring out how to cost effectively and securely operate billions of databases, it makes much more sense, in the early days, for the two non-profits to leverage resources, expertise and costs, by creating them together. As lessons are learnt, then after 2-3 years, the two non-profits may decide to split operation of the two or, continue on.

Thus, costs for this centre are borne by the SOLICT database cost centres.

Learning Non-Profit Manages LDV Databases Subcomponent Costs:

Costs will be borne by the Legal Identity Non-Profit – Manages SOLICT Databases Subcomponent Cost Centre

Learning Non-Profit Manages DLT (Digital Learning Twin) Standards Subcomponent Cost Centre:

Background:

All I can see in my head is this curve occurring. It means increasingly rapid tech change, which in turn means rapid changes to AI. AI is the heart of the DLT. Thus, as the tech changes, so to must the DLT. Which is why I created the DLT Standards subcomponent cost centre in the DLT section of this document.

Its job is to continually update the DLT standards. Since it's likely billions of people will use the DLT over their lifetimes, keeping the DLT up to date is paramount. The curve also creates new attack vectors against the DLT. Thus, from a security perspective, it too must be constantly kept up to date.

This cost centre MUST also focus on the power consumption of each DLT. There will literally be billions of these on the planet, each consuming energy. Thus, the individual DLT net power consumption cost must be kept very low. Skim "**Decentralized AI – Risks, Legal Identity, Consent & Privacy**" to see one possible solution.

The new, global, independent, learning non-profit will administer the DLT standards. As well, it will also conduct 24x7x365 threat analysis, constantly updating the DLT as and when required.

Other Cost Centres Dependent Upon This Cost Centre:

- DLT – DLT (Digital Learning Twin) Standards Subcomponent Cost Centre
- IEP – DLT (Digital Learning Twin) Subcomponent Cost Centre

Learning Non-Profit Manages DLT (Digital Learning Twin) Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for DLT standards
        - The team should include the following types of people:
            - Standards experts
            - Learning experts
            - ADHD/ASD experts
            - AI experts
            - Bot experts
            - Computing chip experts
            - Security/red team experts
            - Standards experts
            - Network experts
            - Co-design experts
            - Lesson learnt expert
            - AI power consumption experts
            - Global power consumption experts
- Start with:
    - Creating use cases for DLT standards and also for DLT power consumption
    - Identify high level requirements
    - Then drill down to crawling steps, determining costs, resources, and requirements to achieve the DLT
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale

Learning Non-Profit – Managed Learning Assessment Standards Subcomponent Cost Centre:

Background:

As stated in the Learning Assessment Standardizing/Automating Traditional Learning Assessments Subcomponent Cost Centre section of this document:

Traditional assessments typically include:

- Written assessments
- Performance assessments
- Portfolio assessments

My points:

- The planet's a higgledy-piggledy mess re assessment standards
  - With globalization and digitization, it's time to create global learning assessment standards
- The arrival of technology potentially offers ways to automate sections of the learning assessment

This subcomponent cost centre's tasks are to:

1. Identify traditional learning assessments
2. Create new global learning assessment standards
3. Determine ways to automate some of them to reduce time and costs of conducting the learning assessments
4. Then to track new assessment techniques and create standards for them (like neuro brain reading/writing)

Other Cost Centres Dependent Upon This Cost Centre:

- Standardizing/Automating Traditional Learning Assessments Subcomponent Cost Centre

Learning Non-Profit Managing Learning Assessments Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases for automating traditional learning assessments
    - The team should include the following types of people:
      - Traditional learning assessment experts
      - ADHD/ASD experts
      - Data experts
      - Network experts
      - Security/red team experts
      - API experts
      - Co-design experts
      - Learning non-profit experts
      - Lesson learnt expert
- Start with:
  - Determining today's best practices/standards for doing ADHS/ASD assessments
    - ADHD assessment review should include but not be limited to:
      - "**2020 Canadian ADHD Practice Guidelines**"
      - American Psychiatric Association "**Diagnostic and Statistical Manual of Mental Disorders (DSM–5)**"
      - 2018 German "**Long version of the interdisciplinary evidence- and consensus-based (S3) guideline "Attention-Deficit/Hyperactivity Disorder (ADHD) in children, adolescents and adults**"
      - 2018 National Institute for Health and Care Excellence (NICE) – "**Attention deficit hyperactivity disorder: diagnosis and management**"
      - 2017 Spanish "**Guía de Práctica Clínica sobre las Intervenciones Terapéuticas en el Trastorno por Déficit de Atención con Hiperactividad (TDAH)**"
    - ASD assessment review should include but not be limited to:
      - Canadian Pediatric Society – "**Standards of diagnostic assessment for autism spectrum disorde**r"
      - "**Standards of diagnostic assessment for autism spectrum disorder**"
      - American Psychiatric Association "**Diagnostic and Statistical Manual of Mental Disorders (DSM–5)**"
      - **European Autism International Guidelines** and "**Some elements about the prevalence of Autism Spectrum Disorders (ASD) in the European Union**"
  - Then move on to other traditional learning assessments
  - Determine if there's any automated assessments practices today
  - Determine if there's any use of behavioral/biometric data used in ADHD/ASD assessment today
  - Review use of bots in doing any ADHD/ASD assessments

    - Identify gaps in current assessment best practices
    - Then stand back and create the initial draft strategic plan for approaching standardizing learning assessments
    - It's highly likely some section of this work will spin off into other sub-project teams
    - Then lay out a comprehensive budget and plan for creating more data-based assessment standards
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve results
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale

Learning Non-Profit Manages IEP (Individualized Education Plan) Standards Subcomponent Cost Centre:

Background:

As stated in the IEP (individualized Education Plan) Standards Subcomponent Cost Centre section of this document:

> "Today, around the planet, there's a higgledy-piggledy set of jurisdictional IEP standards. This architecture requires:
>
> - Local/global IEP standards
> - Able to give every learner on the planet they're own IEP
> - Which can be understood by learning specialists (be they human or AI system/bots)

Other Cost Centres Dependent Upon This Cost Centre:

- DLT – IEP (Individualized Education Plan) Subcomponent Cost Centre
- IEP – IEP (individualized Education Plan) Standards Subcomponent Cost Centre

Learning Non-Profit Manages IEP (Individualized Education Plan) Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
        - The team should include the following types of people:
            - IEP experts
            - Learning specialists
            - ADHD/ASD experts
            - AI and bot (physical and digital) experts
            - Security/red team experts
            - Standards experts
            - Behavioral/biometric experts
            - Neuro experts
            - Co-design experts
            - Network experts
            - Identity experts
            - Global, learning non-profit experts
            - Lesson learnt expert
- Start with:
    - Doing an assessment of current IEP standards and best practices around the planet
        - E.g., **A Guide to the Individualized Education Program**
    - Creating use cases for IEP's for this architecture
    - Identify high level requirements
    - Then drill down to crawling steps, determining costs, resources, and requirements to achieve the IEP
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale

Note: My advice to the team it to create rapid iterations of the IEP's. Start with what already exists in the ADHD/ASD education world. Then rapidly move on. Don't try to boil the ocean. **You need to create a flexible IEP language which can rapidly be changed and grown**.

Learning Non-Profit Learning Competencies/Credentials Subcomponent Cost Centre:

Background:

As stated in "Rethinking Learning - Learning Competencies/Credentials Subcomponent Cost Centre", the goal of this cost section it to:

- Write an education credential to global standards i.e., Groningen type standards
- Be able to digitally sign the credential, proving the learner received it from a credible education institution
- Leverage the same API to securely export the credential out of the education institution to a learner's SOLICT, via a TODA file

That's the goal of this cost section.

Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre

VERY IMPORTANT NOTE:

The work this team does strongly overlaps the work being done by the Legal Identity & Credential Non-Profit's Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre. Thus, it makes sense to leverage resources and expertise while minimizing bugets to run the costs out of the above cost centre.

Learning Non-Profit Learning Competencies/Credentials Subcomponent Costs:

Costs will be borne by the Legal Identity & Credential Non-Profit's Non-Profit – Manages Credential Issuance Standards Subcomponent Cost Centre section of this document.

Learning Non-Profit EMP/HEMP Protection/Power Supply Subcomponent Costs:

Background:

Over my business life as an identity architect, I've led many leading edge, visionary, identity projects. They were often the first within an enterprise requiring high availability i.e., 99.999%. Thus, my teams would work on things like:

- Being able to continually update software without taking down all servers
- Highly available data centres
- Cloud

All of this was in the back of my mind while architecting a new legal identity trust framework and also contemplating the LDV data centers. As the planet madly digitizes, I realized the digital legal identity trust and LDV framework I was proposing had a very big potential weakness. It required electricity to run 24x7x365.

So, I asked myself this dumb question – "What could bring all of this down?" I strongly suggest readers read "**When Our Digital Legal Identity Trust Goes Poof!**". **There's a 1 in 8 chance this decade our electrical grids could go down!**

IT WON'T BE POLITICALLY POPULAR TO ADDRESS. Why? It requires governments and industry to invest lots of money reengineering their electrical grid networks. Industry won't want to voluntarily do this in short time frames. Governments won't want to invest since it takes money away from other high-profile budgets. I sum it up in one word – YIKES!!!!!

Couple this with the fact AI systems are on track to consume most of the planet's energy by the 2040's (skim Figure 1 in "**AI Power Consumption Exploding**").

Then add in the fact that the new age CRVS, SOLICT and LDV systems must be available at 5 9's 99.999%_ or even 6 9" s availability (99.9999%). **(5 9's is a downtime of 5.26 minutes per year, while 6 9's is a downtime of 31.56 seconds per year).**

Which is why I've created a separate subcomponent cost centre to draw attention to all the above.

My strategy is to leverage the desire for governments to create a new legal identity and learning framework, by raising the red flag about electricity. I can see in my head governments acknowledging this, by incrementally funding changes to their existing grid networks.

The place to start is by ensuring government data centres holding vital legal data, like the CRVS/SOLICT, and learning data, like the LDV, are fully protected from EMP/HEMP events and have sustainable power supplies. I can also see how CRVS and learning licensing agreements can raise these issues as part of the licensing discussions/agreements.

Other Cost Centres Dependent Upon This Cost Centre:

- LDV Data Centre Subcomponent Cost Centre

Very Important Note:

The Legal Identity & Credential non-profit has a very similar cost section Non-Profit – EMP/HEMP Protection/Power Supply Subcomponent Cost Centre. It makes sense to have both non-profits separately working together on this from a resources, budget and expertise perspective. That's why I've combined them. Thus, this cost centre will be borne by the Legal Identity non-profit one.

Learning Non-Profit - EMP/HEMP Protection/Power Supply Subcomponent Costs:

Costs will be borne by the Legal Identity & Credential Non-Profit – EMP/HEMP Protection/Power Supply Subcomponent Cost Centre.

Learning Non-Profit – Power Consumption Of LDV, DLT and Learning Assessments Subcomponent Cost Centre:

Background:

There are four trends I see affecting this architecture's learning power consumption:

1. Global warming affecting cheap availability of power
2. This AI power consumption curve depicted in Figure 1 of "AI Power Consumption Exploding" which shows by 2040-ish AI will be consuming most of the planet's power
3. Every legal entity on the planet leveraging their DLT which will consume power
4. Every person on the planet leveraging their LDV databases which will consume power

Thus, that's why I've broken it out as a separate cost centre which the non-profit keeps focussing on creating power friendly ways of delivering the architecture for:

- LDV
- DLT
- Learning Assessment

Other Cost Centres Dependent Upon This Cost Centre:

- LDV Power Consumption Subcomponent Cost Centre
- DLT – Power Consumption Subcomponent Cost Centre

Very Important Note:

A similar exercise is occurring in the Legal Identity and Credential Non-Profit re power consumption of SOLICT, LSSI devices and PIAM. Thus, my suggestion, in the early days, is to combine both cost centres as one and leverage the expertise and resources. Over time, the two cost centres can operate independently within their own non-profit. Which is why this cost centre is borne by the legal identity non-profit cost centre.

Non-Profit – Power Consumption Of LDV, DLT and Learning Assessments Subcomponent Costs

Costs will be borne by the Legal Identity Non-Profit – Power Consumption Of CRVS Data Centres, SOLICT Databases, LSSI Devices & PIAM Subcomponent Cost Centre section of this document.

Learning Non-Profit – Licenses LDV/DLT/IEP Access to Jurisdictions & Training Companies Subcomponent Cost Centre:

Background:

THE NON-PROFIT MUST BE CONTINUALLY WELL-FUNDED TO FUND THE 24X7X365 THREAT ASSESSMENT, ETC. HOW CAN THIS BE DONE?

The architecture solution framework proposes licensing the LDV/DLT/IEP framework to jurisdictions based on a very small charge per learner up to a yearly maximum amount. Along with the learning assessment standards the non-profit will also offer, it enables jurisdictions to lower their cost per student leveraging tech,

IT'S VERY POLITICAL. It requires great tactful political skill in creating the first licensing agreements.

Non-Profit – Licenses LDV/DLT/IEP Access to Jurisdictions & Training Companies Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Fund and create a small team composed of:
  - Finance experts
  - Legal experts
  - Political experts
  - LDV experts
  - DLT experts
  - IEP experts
  - AI systems and bots experts
  - Co-design experts
  - Business process experts
  - Red team experts
  - Standards experts
  - Network/connectivity experts
  - Lesson learnt experts
- Create high level requirements, use cases, and cost estimates for:
  - License agreements with jurisdictions
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale around the planet

Learning Non-Profit – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre:

Background:

The vision is to spin up 30 outside the box learning projects leveraging the architecture this document addresses. Do I know what they should be? No. That will be something for the learning non-profit folks, and especially the co-design experts, to dream and come up with innovative approaches for all learners, regardless of their abilities or disabilities.

In the spreadsheet most of the costing for the 30 projects begins in year two. Why? It will likely take a year to spin up all the other cost centres this document addresses, getting them to pilot and production systems.

I can see a core team of people who oversee and manage the 30 projects. Some of their team might be involved in some of the projects. This team can be spun up in the second half of the first year.

This is what the outside the box learning projects then leverages. It's time to create new learning systems from when the learner is a toddler until they're old, which works for everyone, regardless of their abilities or disabilities.

Other Cost Centres Dependent Upon This Cost Centre:

- Rethinking Learning – Outside The Box Learning POC's & Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre

Outside The Box Learning POC's/Pilots Leveraging AI Systems, Bots & Rethought Human Learning Specialists Subcomponent Cost Centre:

- Create core outside the box program management team to oversee and manage the 30 projects:
    - The team should include the following types of people:
        - Learning experts
        - Co-design learning experts
        - Disability experts
        - AI system experts
        - Learning assistant/teaching assistant AI systems and bots vendors/experts
        - Physical and digital bot specialists
        - Behavioral/biometric/neurological experts
        - Experts in leveraging AI to literally read our minds
        - Assessment experts
        - LMS experts
        - Legal experts
        - Privacy experts
        - Security/red team experts
        - Standards experts
        - Network experts
        - Identity experts
        - Lesson learnt experts
    - This team can be spun up in the second half of the first year
- The core management team and the global, independent learning non-profit's first goals should be:
    - To create three high level types of programs
        - One is for rapid, iterative learning development programs with good short-term deliverables i.e., one year
        - Another is for rapid, iterative learning development programs with good medium-term deliverables i.e., two years
        - The third is what I call in my head "blue sky type projects. These are what might seem off the wall ideas
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above
- Learn from the short and mid-term projects
    - Determine what works and more importantly, what doesn't work
    - Based on results, repilot and/or rapidly scale around the planet
- If any of the off the wall type projects work, then begin to consider how to rapidly scale them around the planet

Learning Non-Profit – Manages Learning Environment Projects Subcomponent Cost Centre:

Background:

As described in Rethinking Learning - Learning Environments Subcomponent Cost Centre crawl, walk and then run. That's what this cost centre does.

Learning Non-Profit – Manages Learning Environment Projects Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 jurisdictions and businesses/employers to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
        - The team should include the following types of people:
            - Legal experts
            - Learning experts
            - Privacy experts
            - Consent experts
            - LDV experts
            - Security/red team experts
            - Education credentials standards experts
            - Behavioral/biometric experts
            - Network experts
            - Identity experts
            - Global, independent, learning non-profit experts
            - Co-design experts
            - Lesson learnt experts
- Start with identifying high level requirements:
    - Create high level requirements for the following types of situations:
        - External learning environments involving third parties
        - Students obtaining competencies in external environments
    - Create use cases for the above
    - Determine common legal contract requirements for these which are required across multiple jurisdictions
    - Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above including use of co-design
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- Amend based on results, repilot, and then rapidly scale
- Transfer management of any standards created, attack vectors, et al to the new global, independent learning non-profit or whatever body deemed appropriate

Learning Non-Profit – Manages LMS Standards Subcomponent Cost Centre:

Background:

As described in Rethinking Learning - LMS (Learning Management Systems) Subcomponent Cost Centre section of this document this cost centre focusses on crawl, walk and run.

Learning Non-Profit – Manages LMS Standards Subcomponent Costs:

To accurately estimate the costs, the following needs to be done:

- Find willing 1-3 jurisdictions and LMS vendors/standards bodies to work with
- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level deliverables and create the first use cases
        - The team should include the following types of people:
            - Learning experts
            - LMS experts
            - Legal experts
            - Privacy experts
            - Security/red team experts
            - Standards experts
            - Behavioral/biometric experts
            - Learning assistant/teaching assistant AI systems and bots vendors/experts
            - Network experts
            - Identity experts
            - Global, independent, learning non-profit experts
            - Co-design experts
            - Lesson learnt experts
- Start with determining global implications to LMS systems from the use of PIAM//LSSI/SOLICT DLT/IEP/LDV and co-design
- Identify new LMS high level requirements
- Create use cases for the above
- Then drill down to crawling steps, determining costs, resources, and requirements to achieve the above
- Rapidly prototype and POC to measure results, figure out what isn't working well, and redo POC
- Then do small, controlled pilots to see how it works out in the real world
- All the above MUST be done in conjunction with the other sub-project teams
- Amend based on results, repilot, and then rapidly scale
- Transfer management of any standards created, attack vectors et al to the new global, independent learning non-profit or whatever body deemed appropriate

Learning Non-Profit - 24x7x365 Threat Assessments Subcomponent Costs:

Background:

As mentioned throughout this document, this curve means a continually increasing array of attack vector threats against leaner data governance, business processes, tech used and end users. **The attacks will be against all components the different learning architectural/cost diagrams in this doc. YES, IT'S COMPLEX AND FAST CHANGING.**

To mitigate against this, threat assessments are composed of:

- People, resources, and infrastructure required to operate a global, 24x7x365 threat assessment centre, for the LDV, DLT, IEP, learning assessments and API's, covering the governance, business processes, tech infrastructure used and end users
- Communication structure for the threats including standardized threat assessments
- Licensing requirements requiring licenses of jurisdictions and training companies re API's to react to different levels of threat assessments, in different ways, within certain time periods

I note, because of the rapidly changing nature of the attack vectors, it's highly likely significant, recurring investment in new tech, like quantum computers etc. will be required i.e., it won't be cheap. The planet's trust in the learning framework rests on the backs of the threat assessment teams.

Other Cost Centres Dependent Upon This Cost Centre:

- LDV Security Subcomponent Cost Centre
- Learning Assessment Security/Privacy Subcomponent Cost Centre

Learning Non-Profit - 24x7x365 Threat Assessment Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
    - Assemble a very small group of experts to lay out high-level threat assessment deliverables and create the first use cases
    - Threat assessment team – the team should be composed of highly skilled people including but not limited to
        - Security/Red team experts
        - Learning experts
        - LDV experts
        - DLT experts
        - IEP experts
        - Learning assessment experts
        - AI Systems/bots experts
        - Networks experts
        - API experts
        - Databases experts
        - Physical and virtual security experts
        - Quantum computing experts
        - Communications experts
        - Encryption experts
        - Lessons learnt experts
        - Co-design experts
        - Etc.
- Determine a wide range of use cases for threats against the cost centres in the learning costs centres section of this document
- Drive out the suggested annual budgets, resources, and team requirements
- Then create a plan to get political buy-in from the right parties around the planet to get this off the ground
- Do rapid POC's and small, controlled pilots
- Learn what works, what doesn't work, and adjust
- Rapidly scale use of non-profit threat analysis around the planet

Learning Non-Profit – Manages Learning API Standards Subcomponent Costs:

Background:

The Learning API's (Application Programming Interface) Cost Centre raises these questions of how to access:

- LDV (Learner Data Vault)?
- DLT (Digital Learning Twin) access to the LDV?
- IEP?
- Third party consent agreements about accessing, inputting and retrieving LDV data (which will be sent to the learner's SOLICT (Source of Legal Identity & Credential Truth)?

Which is where API's standards come into play. However, there's this tech change curve to consider. As the API is the electronic front door to the learning framework described within this document, it means the Evil Inc.'s and malicious states of the planet will leverage the tech change curve to constantly create new attack vectors against the API.

Thus, the non-profit must not only do continual 24x7x365 threat analysis against the API but constantly update the API standards, as and when required. That's what this cost centre delivers.

Other Cost Centres Dependent Upon This Cost Centre:

- LDV API (Application Programming Interface) Subcomponent Cost Centre
- DLT – API (Application Programming Interface) Subcomponent Cost Centre
- Learning Assessment API's (Application Programming interface) Subcomponent Cost Centre
- IEP API (Application Programming Interface) Subcomponent Cost Centre
- Learning API – LDV (Learner Data Vault) Databases Subcomponent Cost Centre
- Learning API – Applications/API Rules Subcomponent Cost Centre
- Learning API - Backend Subcomponent Cost Centre
- Learning API – Clients Internal/External Subcomponent Cost Centre
- Learning API – IAM (Identity Access Management) Subcomponent Cost Centre
- Learning API – Audit Trail Subcomponent Cost Centre
- Learning API – API Gateway Subcomponent Cost Centre
- Remote API's Subcomponent Cost Centre

Very Important Note:

A large part of this cost centre work is threat analysis and prevention. Thus, it makes sense for this cost centre to be part of the Learning Non-Profit - 24x7x365 Threat Assessments Subcomponent Costs centre. This maximizes resources, expertise and minimizes budget costs. Thus, in the Excel spreadsheet, that's what I've done.

Learning Non-Profit – Manages Learning API Standards Subcomponent Costs:

Costs will be borne by the Learning Non-Profit - 24x7x365 Threat Assessments Subcomponent Costs section of this document.

Learning Non-Profit - Independent Auditors Subcomponent Cost Centre:

Background:

Who watches the watchers? This is a major concern in the governance and operations of the new, global, independent, non-profit. The architecture is built around having a group of independent auditors to audit the enterprise regularly.

Politics change over time. Thus, the global independent non-profit may fall to political attacks either internally within the non-profit, or externally. Thus, since the non-profit is a key centrepiece in global learning framework, a mechanism MUST be created to keep intact its "political squeaky clean" functioning.

Careful thought needs to be applied here to prevent just one auditing firm doing the analyzing – for it could lead to leveraging against the auditing firm to produce the "desired audit results". I'm not sure of the mechanism to mitigate against this – but I know it needs to be thought through by the initial funders and the initial board.

The costs of operating this independent auditing function MUST be built into the global, independent non-profit's annual operating costs.

I'M NOT AN EXPERT ON THIS. Thus, what follows is only my best guess on where to start. People with much more experience in this area will likely recommend a change to below.

Independent Auditors Costs:

To accurately estimate the costs, the following needs to be done:

- Create a preliminary budget to:
  - Assemble a group of non-profit and auditing experts including but not limited to:
    - Legal experts
    - Non-profit experts
    - Auditing experts
    - Political experts
    - Learning experts
    - Co-design experts
    - Lessons learnt analysts
    - Others?
  - Create high level requirements for how the independent auditing group could function, along with use cases and proposed annual budgets
  - Get political buy in from key groups
- Then create a plan to bring this into reality with budgets, resource requirements, et al

Summary

The visions outlined in this document are transformational. It rethinks how people, poor to rich, able or disabled, living anywhere on the planet, can legally identify themselves, from cradle to grave, both physically and digitally. Each person is in control of their legal identity, choosing how much to release of their identity and credential data, biometrics, and behavioral data. The SOLICT/LSSI/PIAM architecture significantly reduces identity friction and fraud costs for businesses, governments, and people.

The same framework also addresses legal identification of rapidly emerging smart digital versions of us, as well as AI systems and bots. As we literally create billions or more of these types of entities, many of them will require legal identification.

The learning vision leverages the rethought legal identity framework. It enables a child, anywhere on the planet, to be given the same learning opportunities, regardless of their abilities to learn. Over time, not overnight, it will force a rethink on our current education systems planet wide. My goal is no child should be left behind in this learning tech revolution we're entering.

Yes, it's complex. Yes, there's lots of potential political pitfalls which could derail it. However, this document suggests strategies to carefully crawl, walk and then run. It suggests through every cost centre, doing pilots in 1-3 jurisdictions at first i.e., don't try to solve all the planet's many legal identities and learning problems at the global stage. As the deployments become successful, design them to rapidly scale.

Lay the foundations for maintaining the CRVS/SOLICT/LSSI/PIAM/Learning Vision infrastructure, over time, both fiscally and security. That's why the two global, independent non-profits are created.

We're entering a major paradigm shift where our old ways won't work well anymore. Thus, it requires out of the box thinking for our out of the box times. It also requires out of the box funders to take the lead in funding, designing, and implementing this.

High Level Cost Reference Papers:

Readers should skim these two docs:

- **Guesstimate Cost Notes Rethinking Legal Identity & Leveraging This to Rethink Learning (Word Doc)**
- **Guesstimate Costs Rethinking Legal Identity & Leveraging This to Rethink Learning (Excel Spreadsheet)**

About the Author:

Guy Huntington is a veteran identity trail blazing architect, program and project manager who's lead as well as rescued many large identity projects with many of them involving identity federation. His past clients include Boeing, Capital One, Kaiser Permanente, WestJet, Government of Alberta's Digital Citizen Identity and Authentication Program and Alberta Blue Cross. As one of his past clients said "He is a great find, because he is able to do high quality strategic work but is also well-versed in project management and technical details, so he can traverse easily from wide to deep. With Guy, you get skills that would typically be encompassed in a small team of people."

For the last eight years, he's been thinking, writing, and searching for new pieces with which to rethink both human and AI System/Bot legal identities, as well as also rethinking learning. He now has an architecture and plans addressing this and is in discussions with a country to fund and deploy.

Guy consults on this.