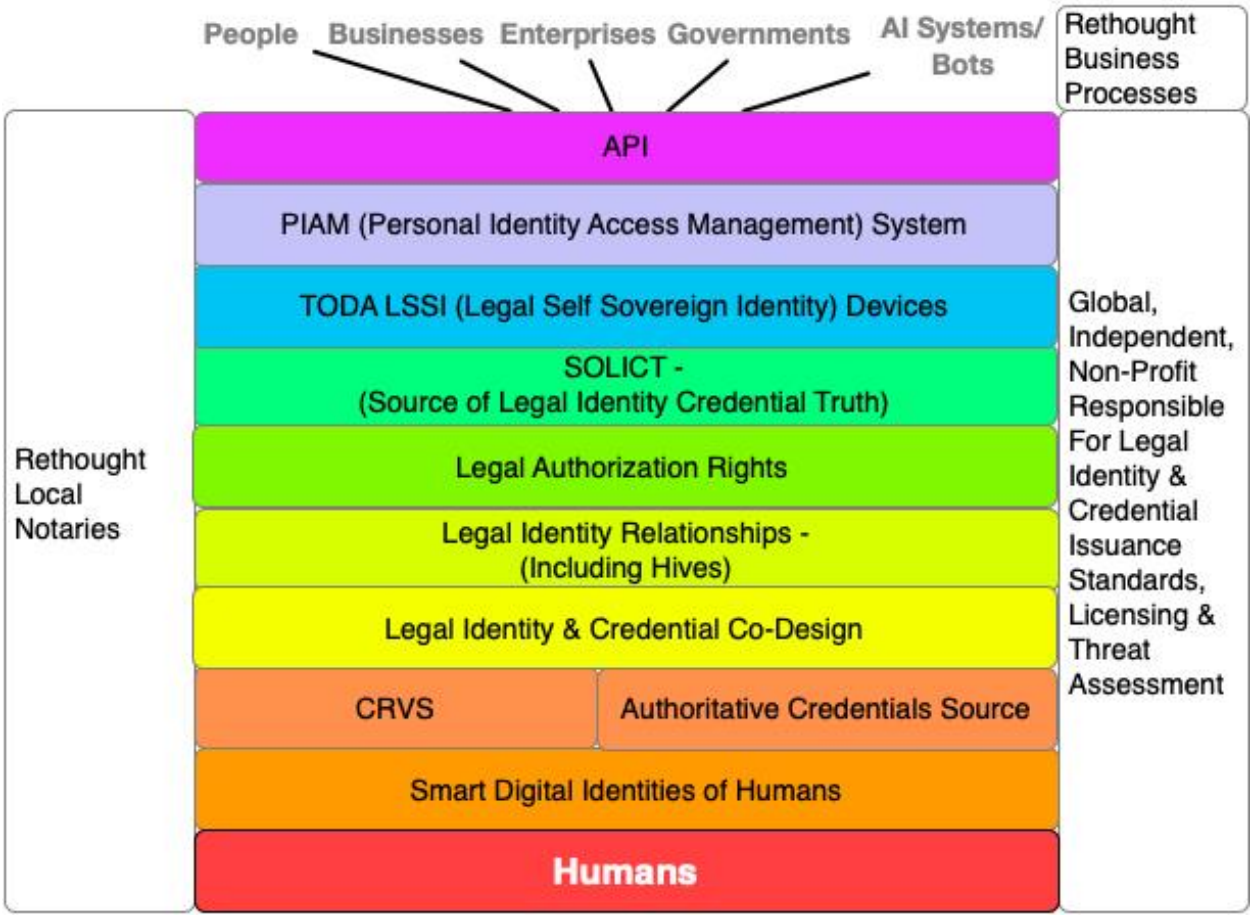
Rethinking Human Legal Identity



Author: Guy, Huntington, President, Huntington Ventures Ltd.
Original Issue Date: October 1, 2021
Updated April 19, 2024

TABLE OF CONTENTS

Executive Summary

Our current legal identity system, planet wide, is badly broken. To see why read problems 1-2 in "**Legal Identity Problem Statements**". The underlying cause is a highly fragmented **CRVS (Civil Registration Vital Statistics)** system, with no data standards, still using paper which is easily frauded.

It isn't anywhere ready for the arrival of smart digital identities of us, AI systems and bots legal identities, and human clones. Skim "**AI Leveraged Smart Digital Identities of Us**" and "**I Hate How We Use Biometrics Today**".

Add to this our emerging ability to belong to "hives". Skim "**Hives, AI, Bots & Humans - Another Whopper Sized Problem**". These might require legal registration.

Then consider increasing numbers of people fleeing where they live due to climate change. Many of them won't be carrying legal identity documents, wanting to enter your country. How can you determine who's who?

Add to this the requirement to service all citizens with a legal identity and credential framework on the planet which works for them regardless of their abilities or disabilities.

Next, **consider this this curve**. It means, each day, new attack vectors will be created against your state/provincial jurisdictions running CRVS systems. My premise? Most of them don't have the budgets, expertise, or personnel to address this. How can this be done?

Finally, consider the major political problem of most legal identity frameworks being run by laws and regs at the local state/provincial level. THEY'RE VERY TERRITORIAL. How can rapid legal identity change be managed, still leaving them in control?

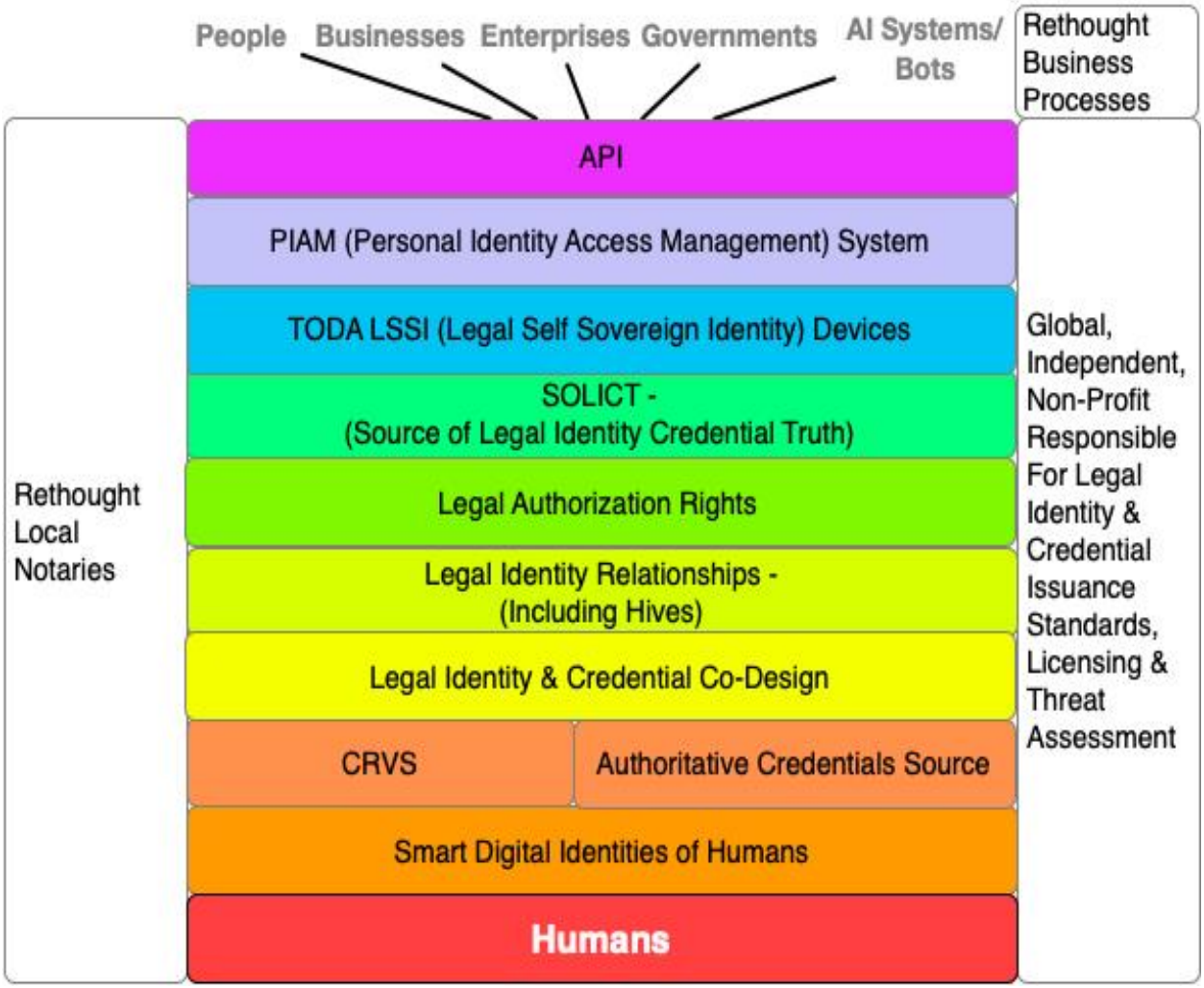
This document contains a high-level flyover of the solution architecture addressing this. It offers the ability to:

- Register all humans, in a new age CRVS system, using some of their biometrics
- Gives them the ability to register digital AI agent type identities against their legal identity
- Allows them, with their consent, to be able to instantly prove their identity ranging from anonymous through to their full level identity as well as any credentials they have
- Allows them to be able to easily prove their identity and legal identity relationships in any contract or legal hive relationship they enter
- Gives governments a way, with the citizens consent, to verify peoples' physical and digital legal identities
- Enable your businesses to gain competitive edges by being able to do things faster, cheaper, and better

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 architecture delivers.

Introduction:

This document is a high-level flyover of the major components to rethink human legal identity. It's written for senior decision makers to get a grasp of the components. It uses this diagram to illustrate the high-level components:



Within component section, it contains references to specific cost centre details, which the decision maker will likely want to direct their analysts to.

Here's how the document works:

- Component title
- Short description
- Cost centre display
- Reference links to more detailed cost centre information
- Examples using diagrams

Humans and Legal Identities

Description:

Today's legal identity world is a mess. How can I say this? Skim problems 1, 2 and 3 in "**Legal Identity Problem Statements**". Thus, underneath all this talk and protocols about "digital identity" is a crappy legal identity. Now look forward to what's coming at us…

- **Human Cloning** - skim problem #11 in "**Legal Identity Problem Statements**". Thus, any new legal identity framework and architecture must be built with being able to easily differentiate human clones both physically and digitally
- **AI Leveraged Smart Digital Identities of Us** - skim "**AI Leveraged Smart Digital Identities of Us**". We're in the early days of a whopper sized paradigm shift. As the article states it's full of risk. Thus, as the risk rises, smart digital identities of us must be legally registered. Today, on the planet, this legal identity framework doesn't exist.
- **Politics** - legal identity is frequently managed in local state/provincial jurisdictions. Each is VERY territorial wanting to keep control of their laws and regulations. **THUS, ANY NEW LEGAL IDENTITY FRAMEWORK MUST BE BUILT STILL GIVING LOCAL JURISDICTIONS CONTROL BUT INTEGRATING INTO AN INSTANTANEOUS GLOBAL FRAMEWORK**.
- Vision: skim "**Revised Principles of Identity**". It lays out guiding principles for legal identity.

Links:

- In the CRVS section, it describes how each local jurisdiction still keeps control of their CRVS systems by laws and regs, yet plugs into a new age global system able to work at warp speed
- In the credentials section it shows how we can easily prove our credentials locally and globally
- In the co-design section it shows how each citizen, regardless of their abilities or disabilities is able to use their SOLICT, LSSI devices and PIAM to release portions of their legal identity and credential information to third parties
- In the smart digital identities section, it shows how we can register one or more smart digital identities against our underlying physical legal identity
- In the legal identity relationship section, it shows how legal identities of humans, AI systems and bots will function as we enter the age of "hives"
- In the authorization rights section, it shows how we can control and delegate our authorization rights
- In the global, independent, well-funded, non-profit section, it shows a 24x7x365 security threat analysis to keep the end to end legal identity & credential governance framework secure
- In the notaries section, it shows how new age, notaries can independently verify human, AI system and bot legal identities

Smart Digital Identities of Humans

Description:

Smart digital identities of us are rapidly emerging. Skim this article, "**AI Leveraged Smart Digital Identities of Us**".

This curve means the pace of change, increase in AI, will mean over time, not overnight, dramatic changes in what these digital entities of us can do on our behalf. They'll do financial trading, buying/selling things on our behalf and even working on our behalf.

All of this comes with risk. For low-risk situations, a person can create, buy, license et al, smart digital versions of themselves calling them whatever they'd like. For medium to high-risk situations, it requires legal identity registration of these entities, in a CRVS system, against our physical legal identity. Skim this article for an example of Nurse or Doctor Jane Doe leveraging her AI leveraged, smart medical digital identity to simultaneously manage several patients while she works with someone else (skim "**Hives, AI, Bots & Humans - Another Whopper Sized Problem**")

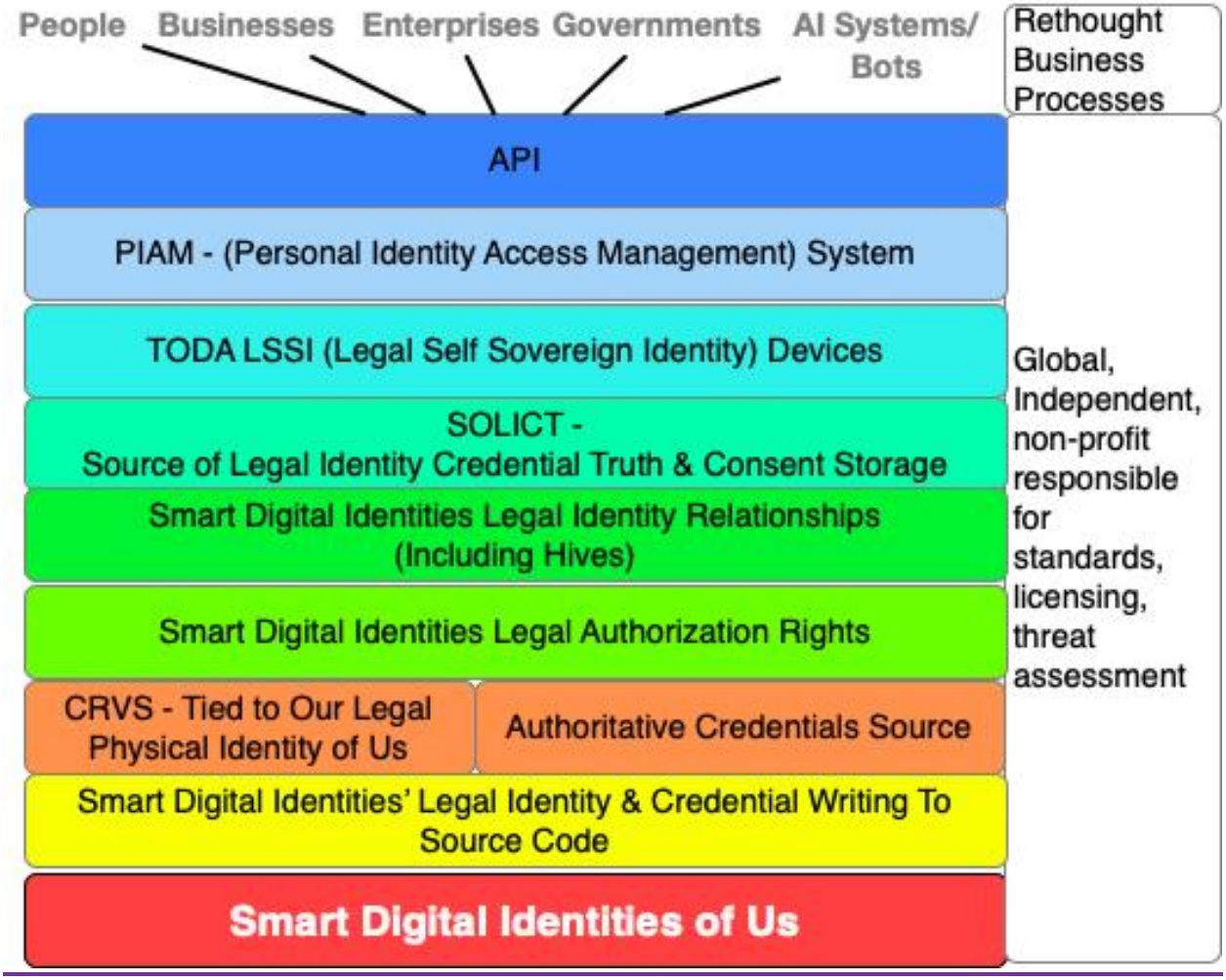
Further, the use of these types of entities also extends to kids. I strongly urge readers to skim these two articles:

- "**Kids & Digital Identities**"
- "**Sex & Identity**"

There's a big challenge in registering smart digital identities of us, which is the same challenge with legally registering AI systems and bots – "How do we legally register them in their source code?" This isn't a trivial challenge. To learn more about this, I suggest readers skim these two articles:

- **"The Challenge with AI & Bots - Determining Friend From Foe"**
- **"A Whopper Sized Problem- AI Systems/Bots Beginnings & Endings"**

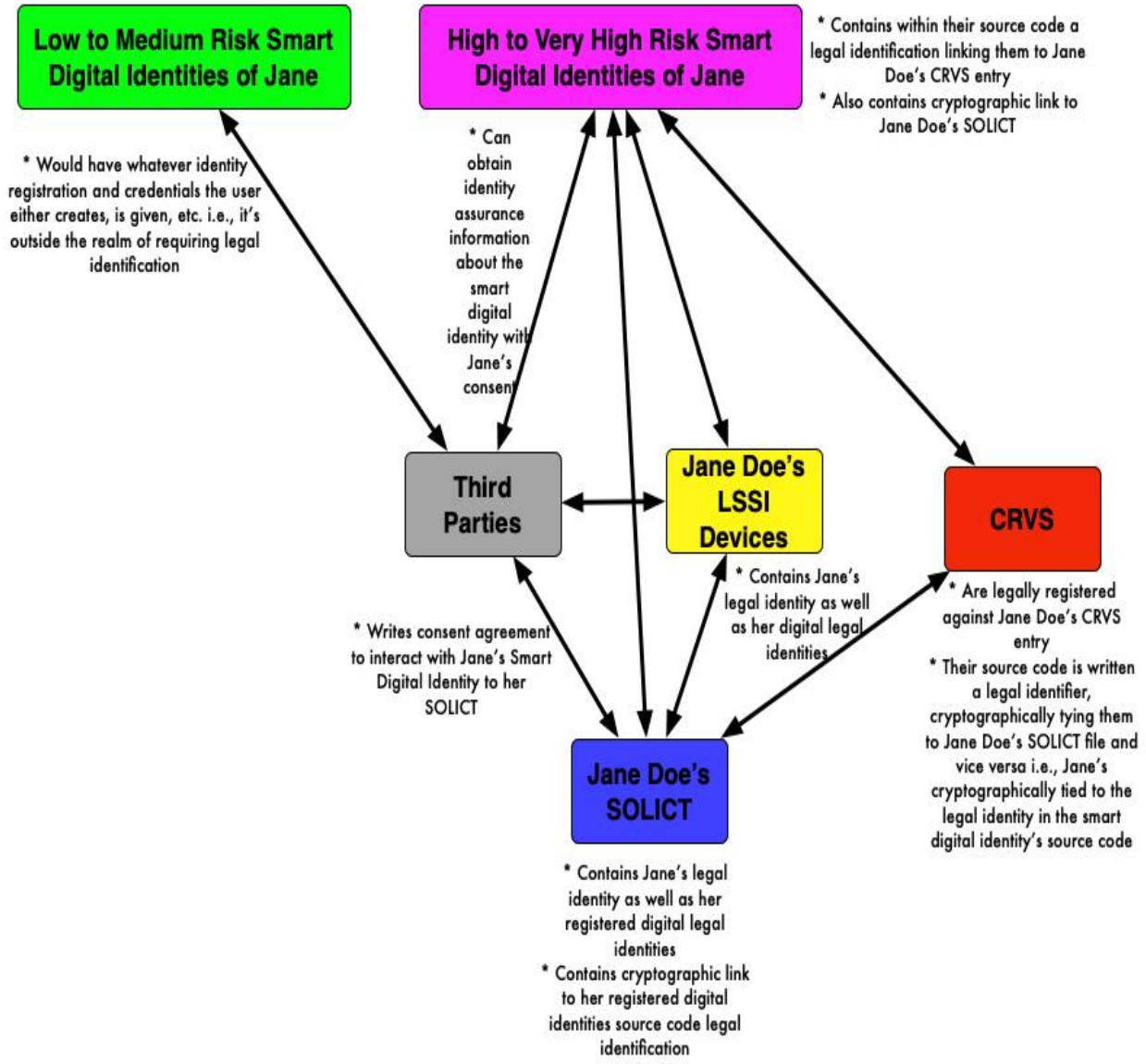
Smart Digital Identities of Humans Cost Centres:



Smart Digital Identities of Us Cost Centre Reference Links:

Read the section titled "**CRVS – Smart Digital Identities of Us Sub-Component Cost Centres**" in "**Cost Centres- Rethinking Legal Identity & Learning Vision**".

Smart Digital Identities Examples:



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.

Rethinking CRVS – Civil Registration Vital Statistics

Description:

Each jurisdiction will use the same type of CRVS system, all to a new common, global, data standard. Within the CRVS, it stores not only the person's legal identity information, but also their forensic fingerprints and iris scans, which hare stored using a proprietary algorithm and number, digitizing the results. Note: forensic biometrics are required to legally differentiate human clones when they appear.

Note: The problem with biometrics is they're not revocable and re-issuable. Thus, if they're obtained by a database hack, or obtained without our consent (like the German Defense Minister's fingerprints obtained at a distance in 2014), then we're effectively screwed for the rest of our lives.

Hypothetically, the architecture at birth of a person, the CRVS obtains from the parent/legal guardian at birth, a secret number and, using a public algorithm, creates an anonymous biometric identifier. The CRVS digitally signs and writes to the person's **SOLICT (Source of Legal Identity & Credential Truth)**. The reason for doing this is, if the biometric is compromised, the person can go to the CRVS, have them revoke the biometric and replace it with a new one. Thus, biometrics now become revocable and re-issuable. To see an example of this skim the last section titled, "**Jane's Legal Identity is Compromised**" in "**An Identity Day in the Life of Jane Doe**".

The CRVS also has agreements with all other CRVS systems around the planet to use an agreed upon search algorithm to confirm an identity of a person.

The CRVS also has a new relationship with local notaries. The notary is, with the person's consent, able to search on one specific CRVS system, taking their biometrics and legal identity information, to confirm their legal identity. The notary IS NOT ABLE TO TROLL ALL CRVS SYSTEMS AROUND THE PLANET. Thus, the role of notaries is updated.

The CRVS is also able to register, where the risk warrants it, smart digital identities of us e.g., digital twins, AI personal assistants, AI virtual selves, etc.

The CRVS system, data standards and overall security standards are managed by a new, global, independent non-profit. To fund this, each jurisdiction pays an annual license fee, per CRVS event, up to a maximum amount (see the global, non-profit section of this document).

Many existing CRVS systems around the planet have stacks of paper registrations, or use old PC networks, or use mainframes. **The non-profit will develop an automated conversion system to rapidly convert this to new data standards, offering it for free or a very low cost, to the jurisdiction as part of the licensing agreement.**

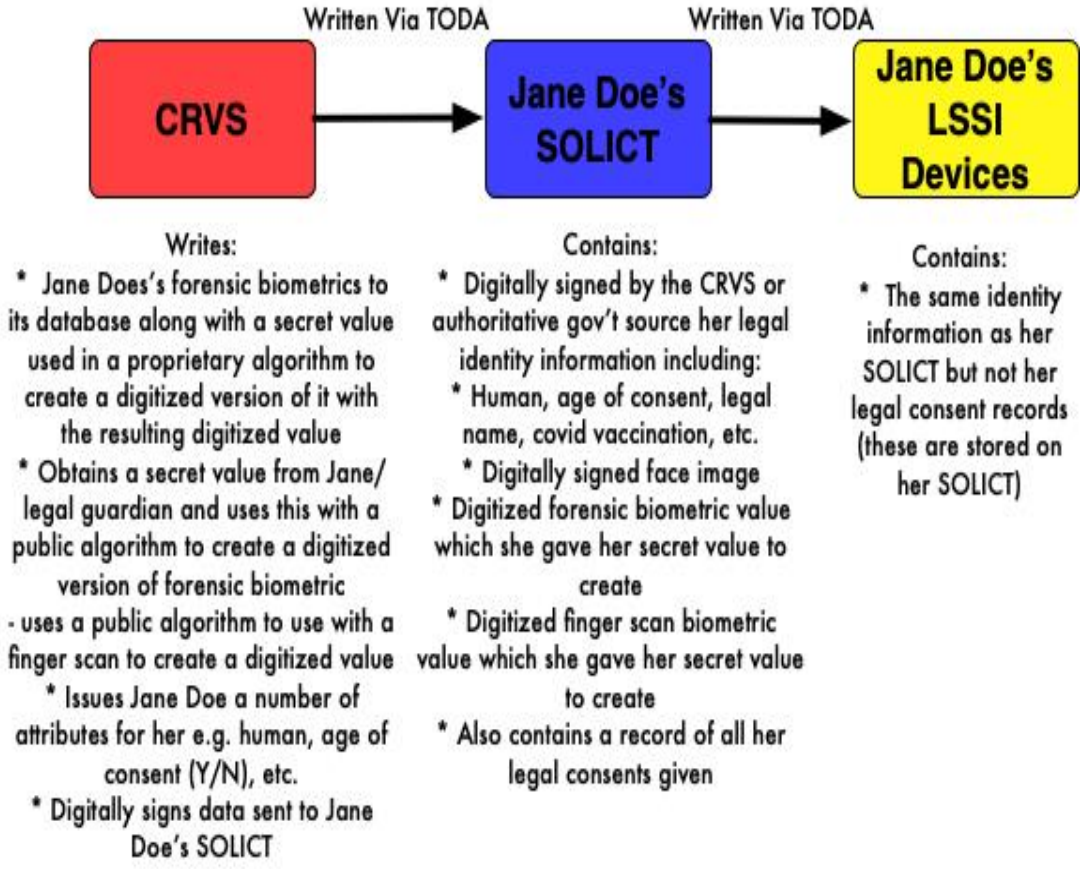
It's all out of the box thinking for the out of the box times we're living in.

CRVS Cost Centre Reference Links:

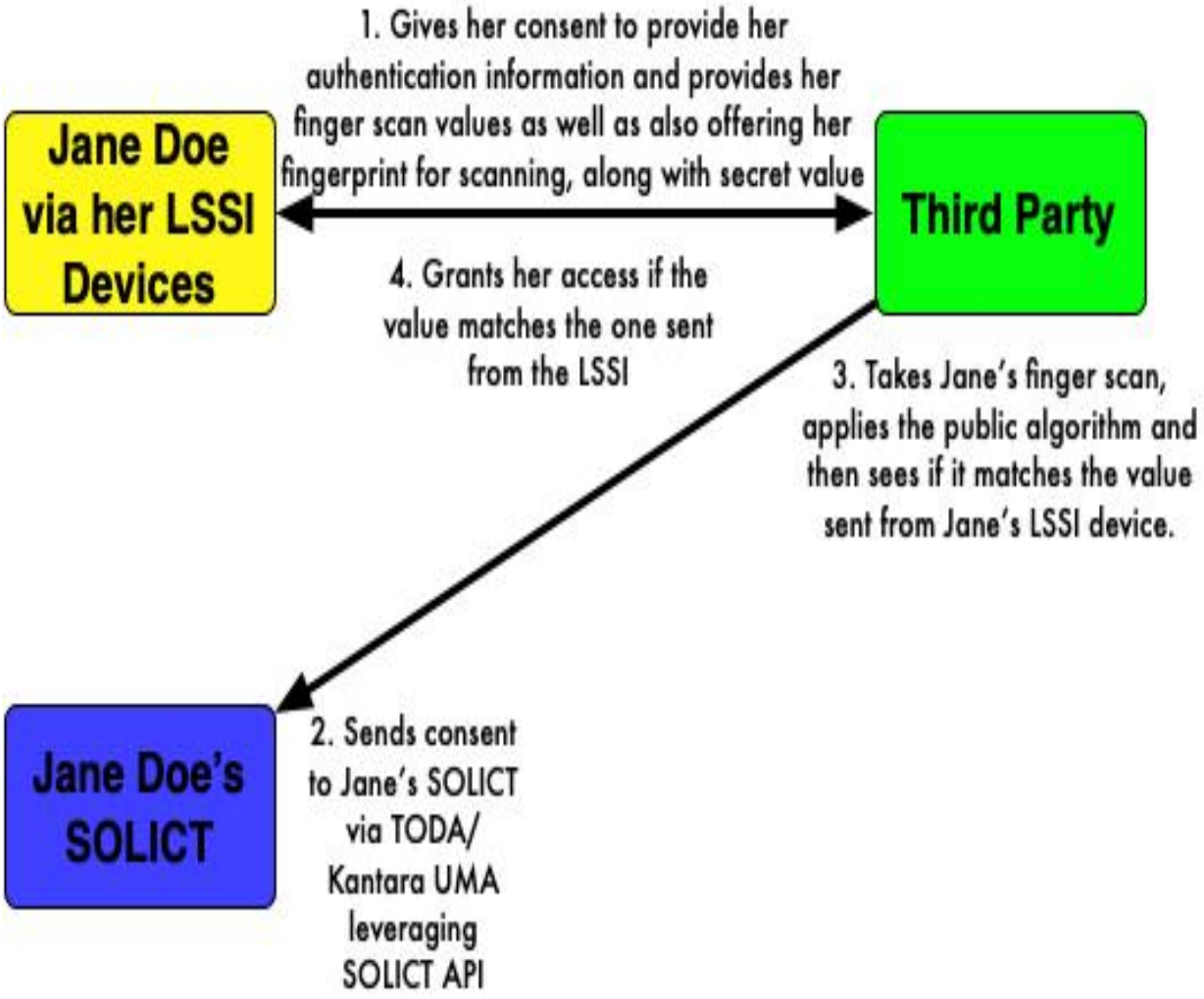
Read the section titled **Cost Centre: Rethought CRVS (Civil Registration Vital Statistics)** in "**Cost Centres Rethinking Legal Identity Learning Vision**".

CRVS Examples:

Issuance of Legal Identity Diagram



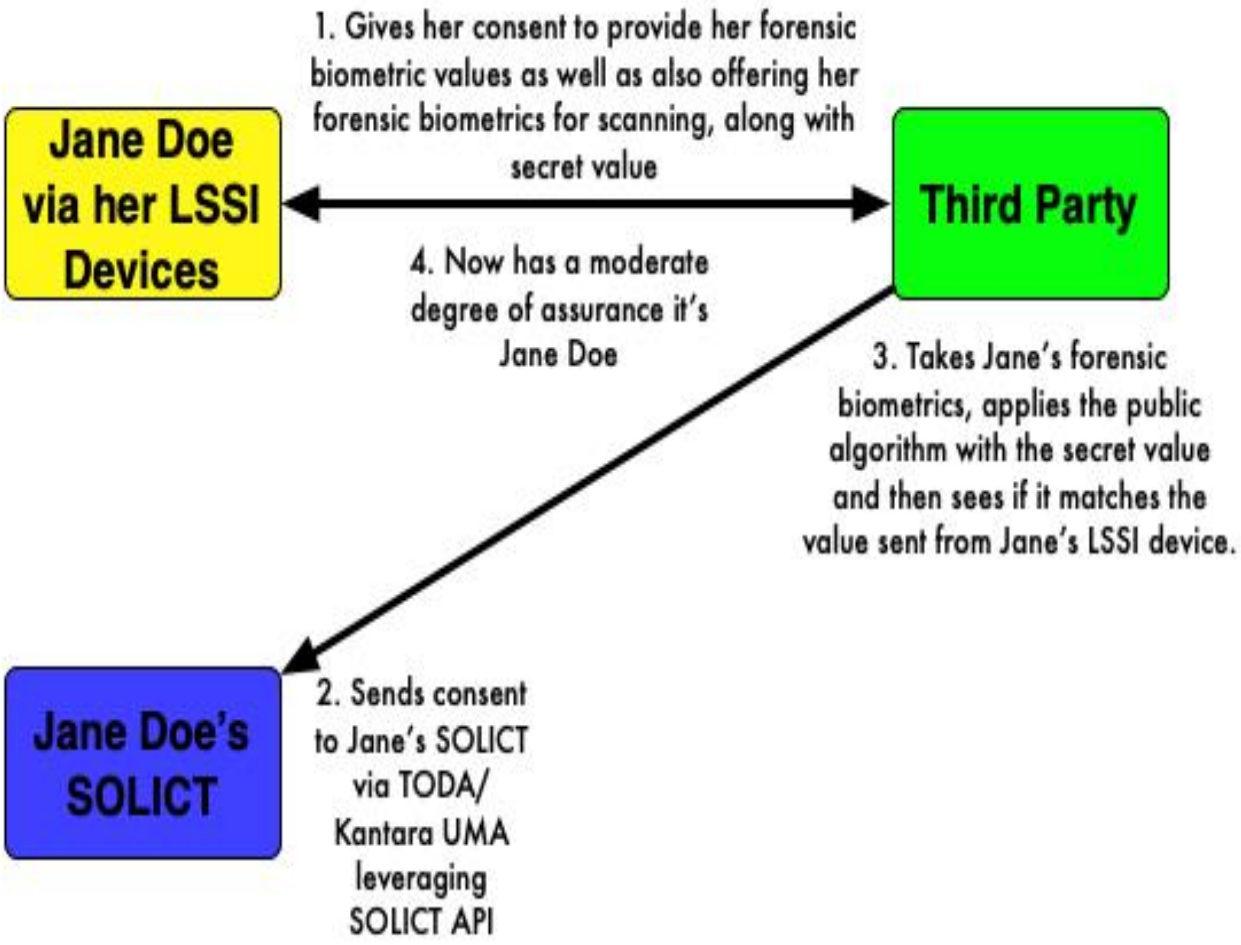
Authentication With a Third Party



Note:

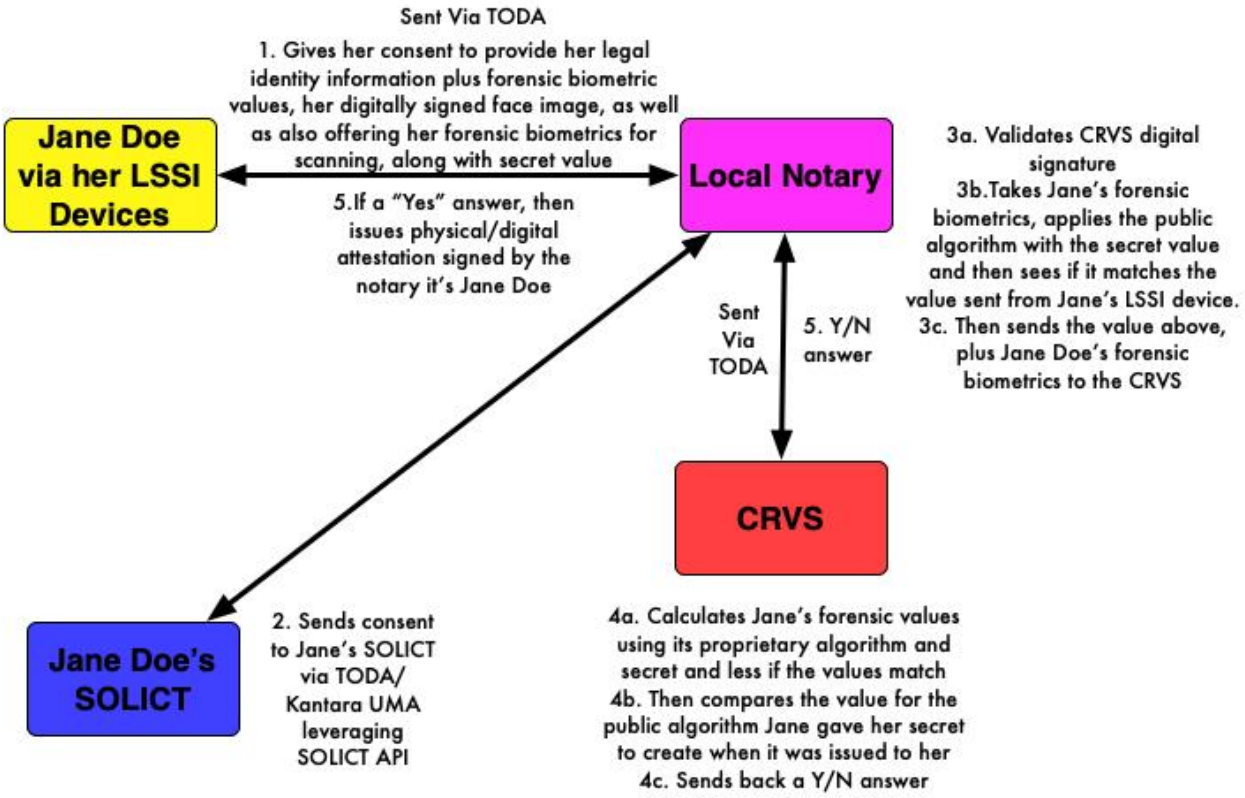
1. For the above the third party optionally could make a quick electronic trip to validate the digital signature sent by the CRVS
2. There will be a different version of this type of authentication, using an iris scan

Increased Identity Assurance

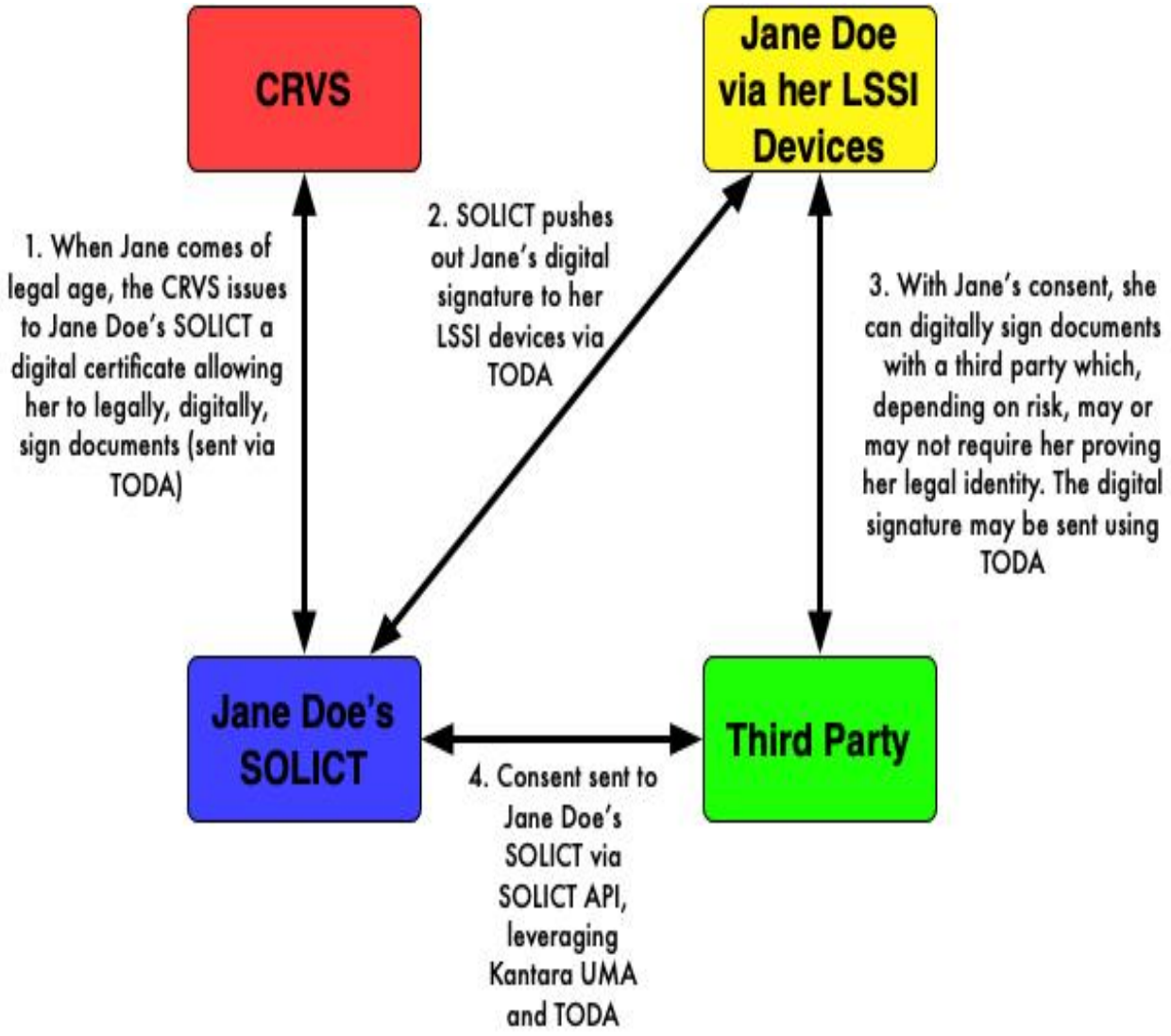


Note: For the above the third party optionally could make a quick electronic trip to validate the digital signature sent by the CRVS.

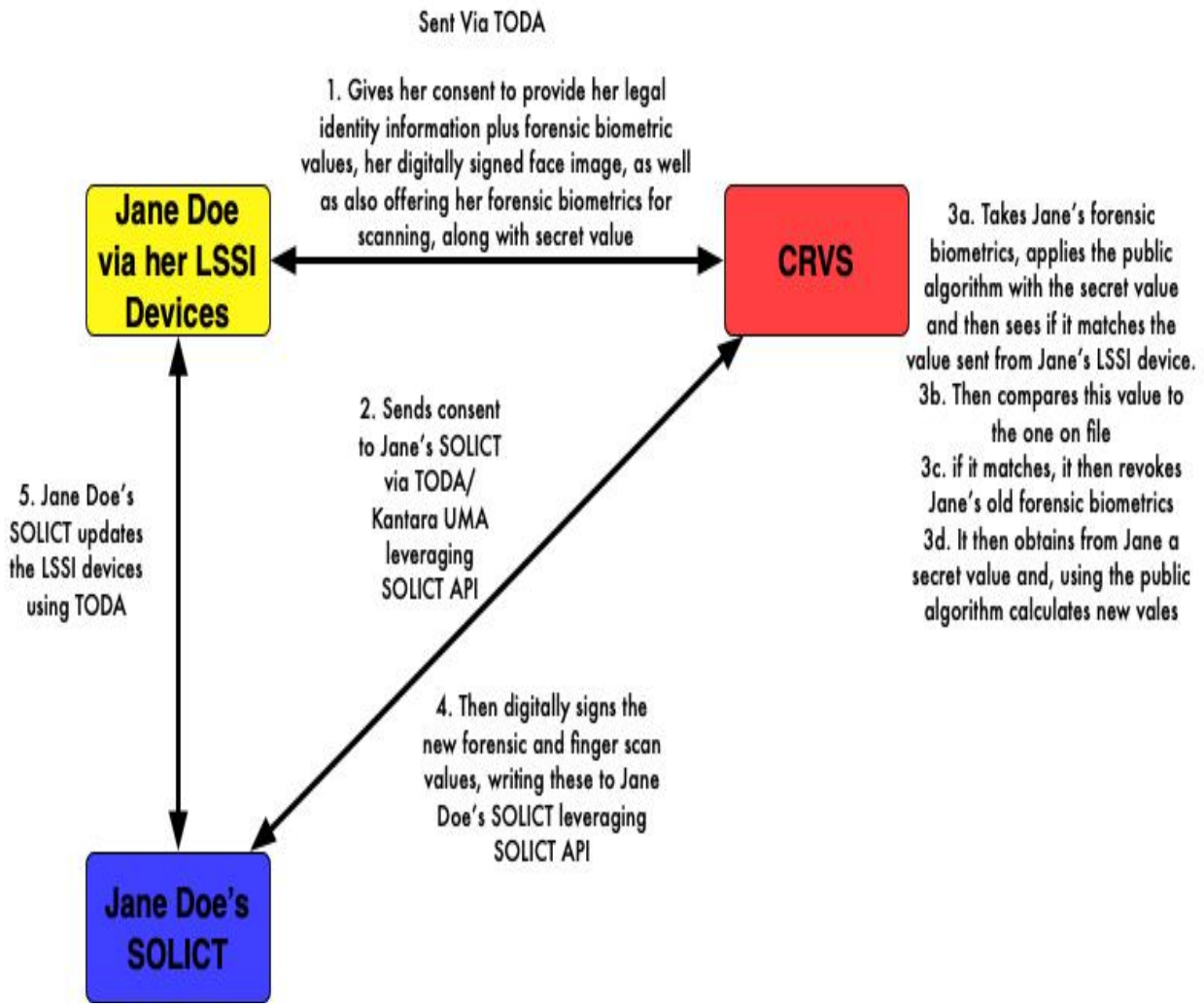
High Identity Assurance



Digitally Signing Documents

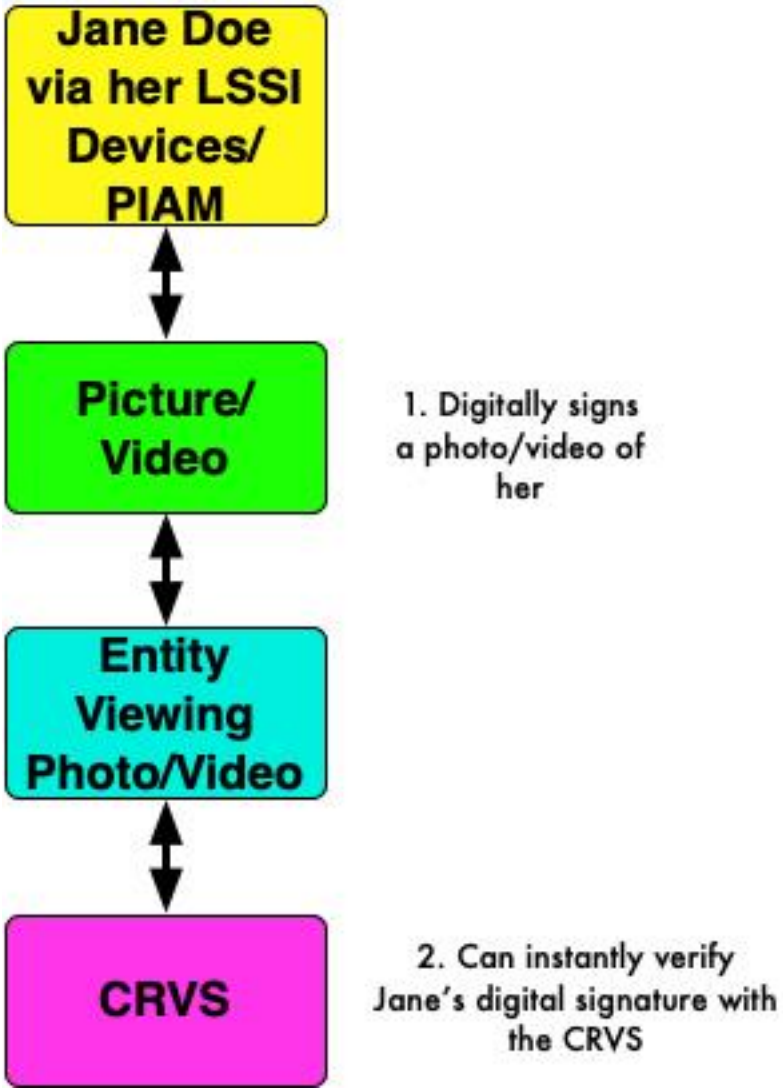


Revoking and Reissuing Biometrics



Proving A Photo of You Isn't a Deep Fake

Skim to the section titled "**Jane Defends Herself Against a Malicious Deep Fake Video**" "**An Identity Day in the Life of Jane Doe**" to see an example of what's below.



Authoritative Credentials Source

Description:

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 "**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 adapt 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.

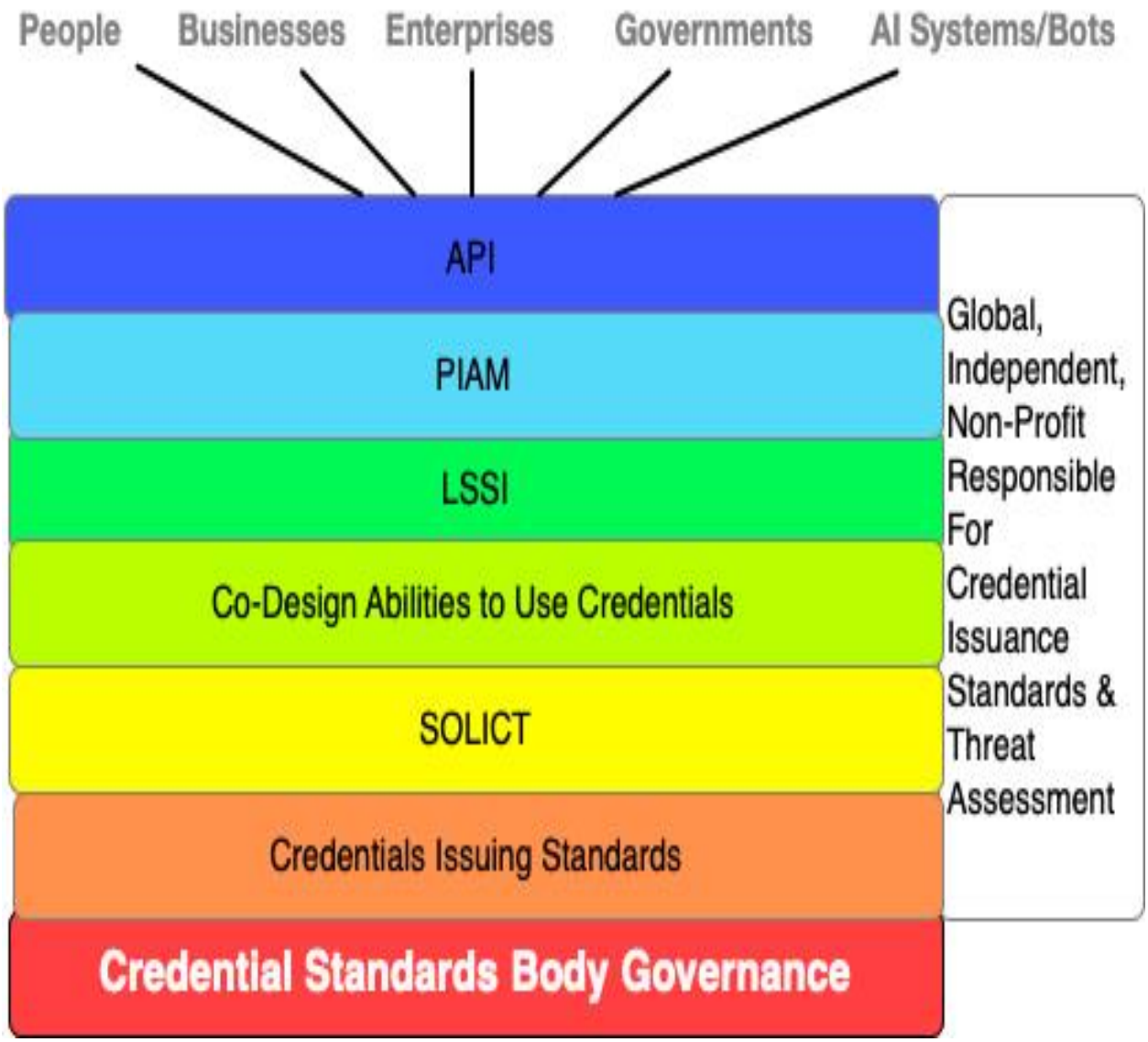
Thus, the architecture is built on a global, independent legal identity & credential non-profit responsible for credential issuance standards, which the credential standards bodies can adopt. Over time, as the non-profit detects new attack vectors against the credential issuing standards, it can automatically 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.

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

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

Authoritative Source Credentials Cost Centres Diagram:

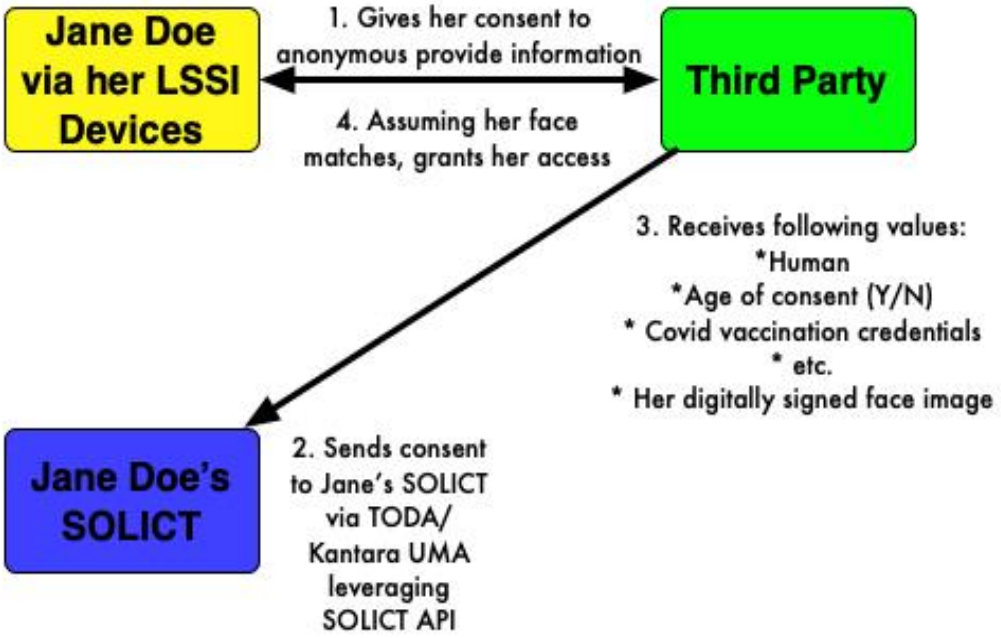


Authoritative Source Credentials Cost Centre Reference Links:

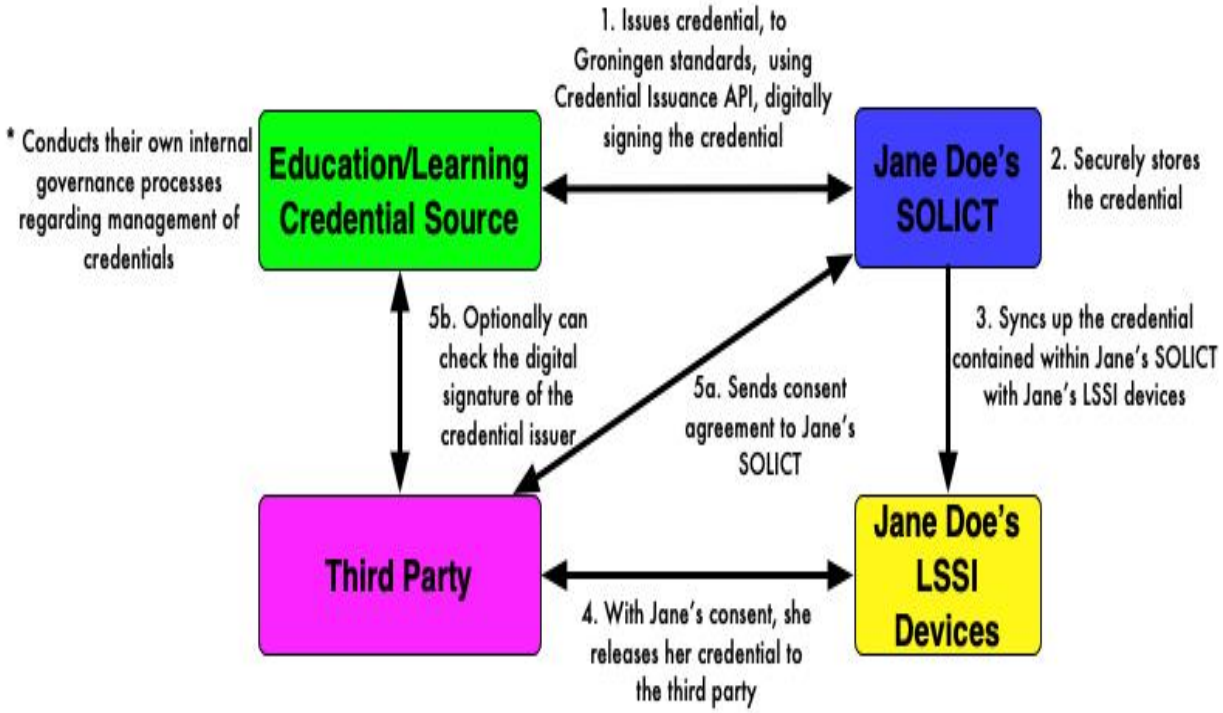
Read the section titled "**Cost Centre: Authoritative Credentials Source** " in "Cost Centres Rethinking Legal Identity Learning Vision".

Authoritative Credential Examples:

Anonymously Proving Age of Consent, Covid Vaccination, Etc.



Proving One's Education Credentials



Note: For the both 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.

Legal Identity & Credential Co-Design

Description:

I strongly suggest readers skim to the section titled, "**Vision – Co-Design 'Nothing About Us Without Us**' " starting on page 55 of this doc and read it. It states the following:

"As I see it, these architectures two most important, critical challenges are:

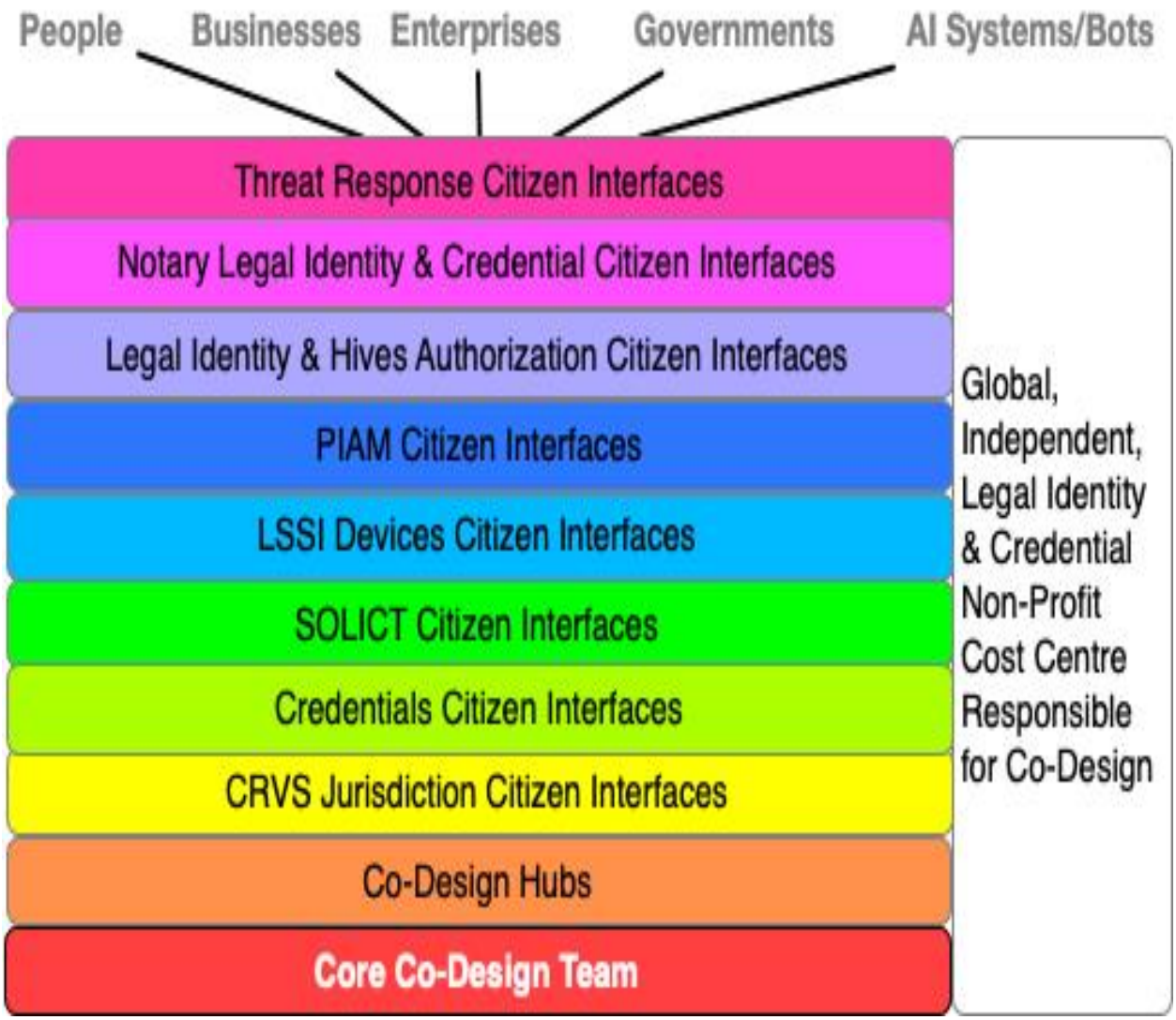
1. **Creating a continually secure architecture for registering digital entities at transactional speeds**
2. **Creating citizen interfaces, designed from the ground up, enabling all citizens, regardless of their abilities or disabilities, to understand and use their SOLICT, LSSI devices, PIAM, DLT, 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."

The vision section also contains this sub-section titled, "**Learning From Others Who've Gone Before Us**' which discusses a recent book **"Nadia – Politics, Bigotry, Artificial Intelligence"** written by a veteran architect Marie Johnson. It lays out how to screw up a co-design project. I think it's a must read for senior government analysts and policy makers.

Thus, I've taken lessons learnt from the book, and applied them to creating an architecture which will be successfully used by literally several billion people on the planet. Throughout the cost centre doc, you'll see it building in co-design teams in many of the critical cost centres from the beginning.

Legal Identity & Credential Co-Design Cost Centres:



Authoritative Source Credentials Cost Centre Reference Links:

Read the section titled "**Non-Profit – Legal Identity & Credentials Co-Design Team and Standards Sub-Component Cost Centre**" in "**Cost Centres Rethinking Legal Identity Learning Vision**".

Legal Identity & Hive Relationships

Description:

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 and there is no legal framework work able to work physically or digitally, locally and globally.

Skim "**Hives, AI, Bots & Humans - Another Whopper Sized Problem**" to see 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:

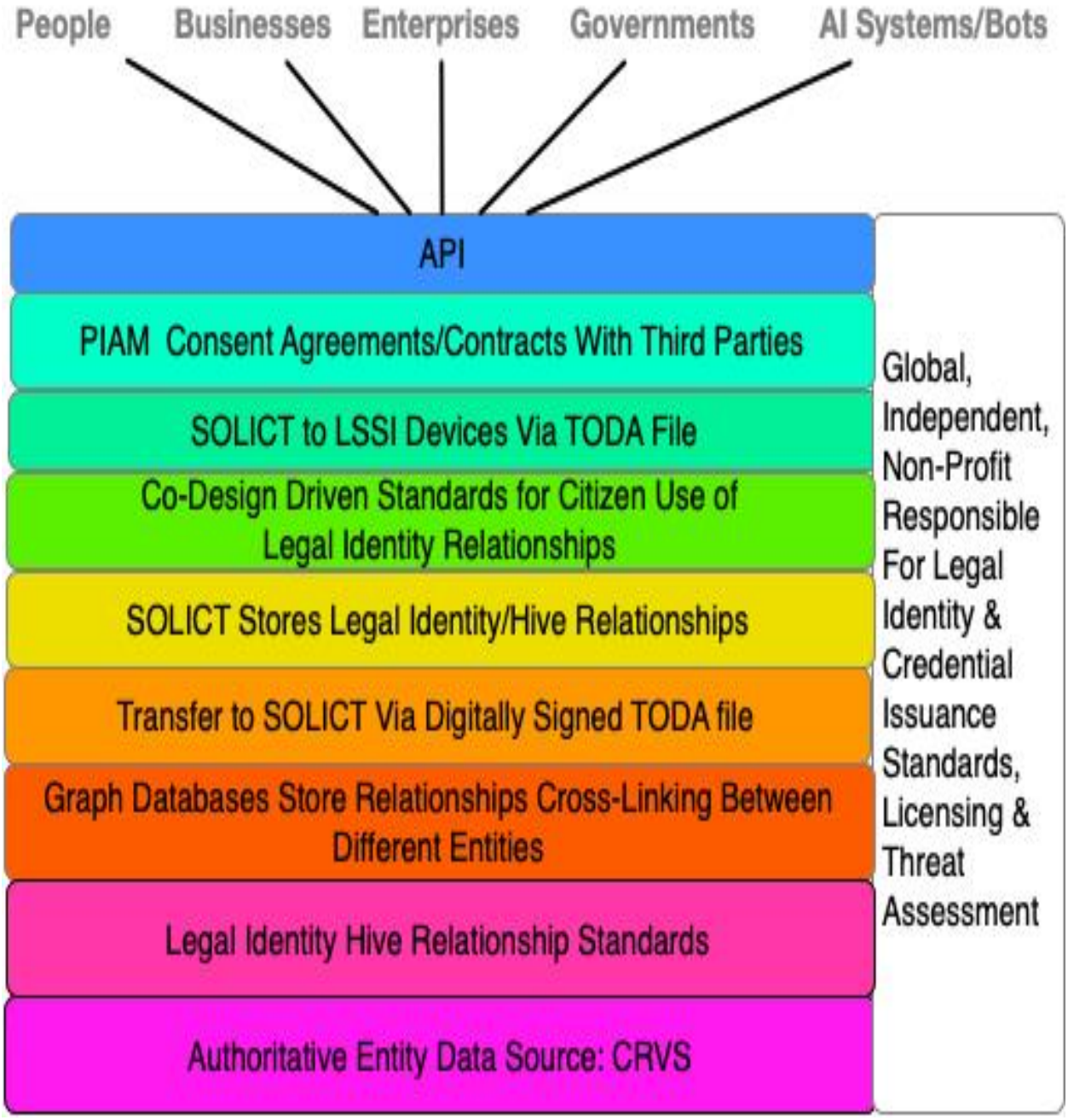
- Speed at which hive legal identity relationships can hypothetically change i.e., seconds or minutes – so the CRVS system MUST BE FAST.
- Complex relationships i.e., it can be one to many and many to many – so the CRVS needs the architecture to allow for this.
- How to cross-link between all the different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

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

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's SOLICT a digitally signed TODA file containing the legal identity relationships.

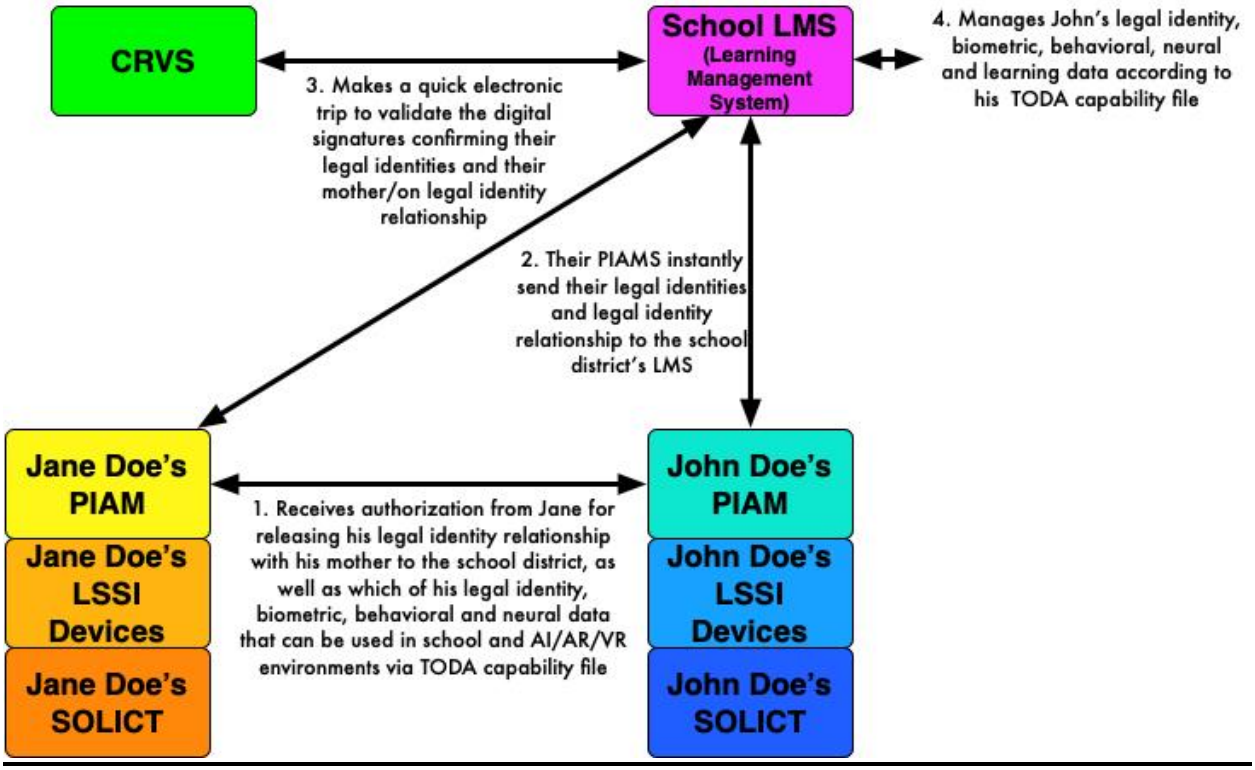
Legal Identity& Hive Cost Centres Diagram:



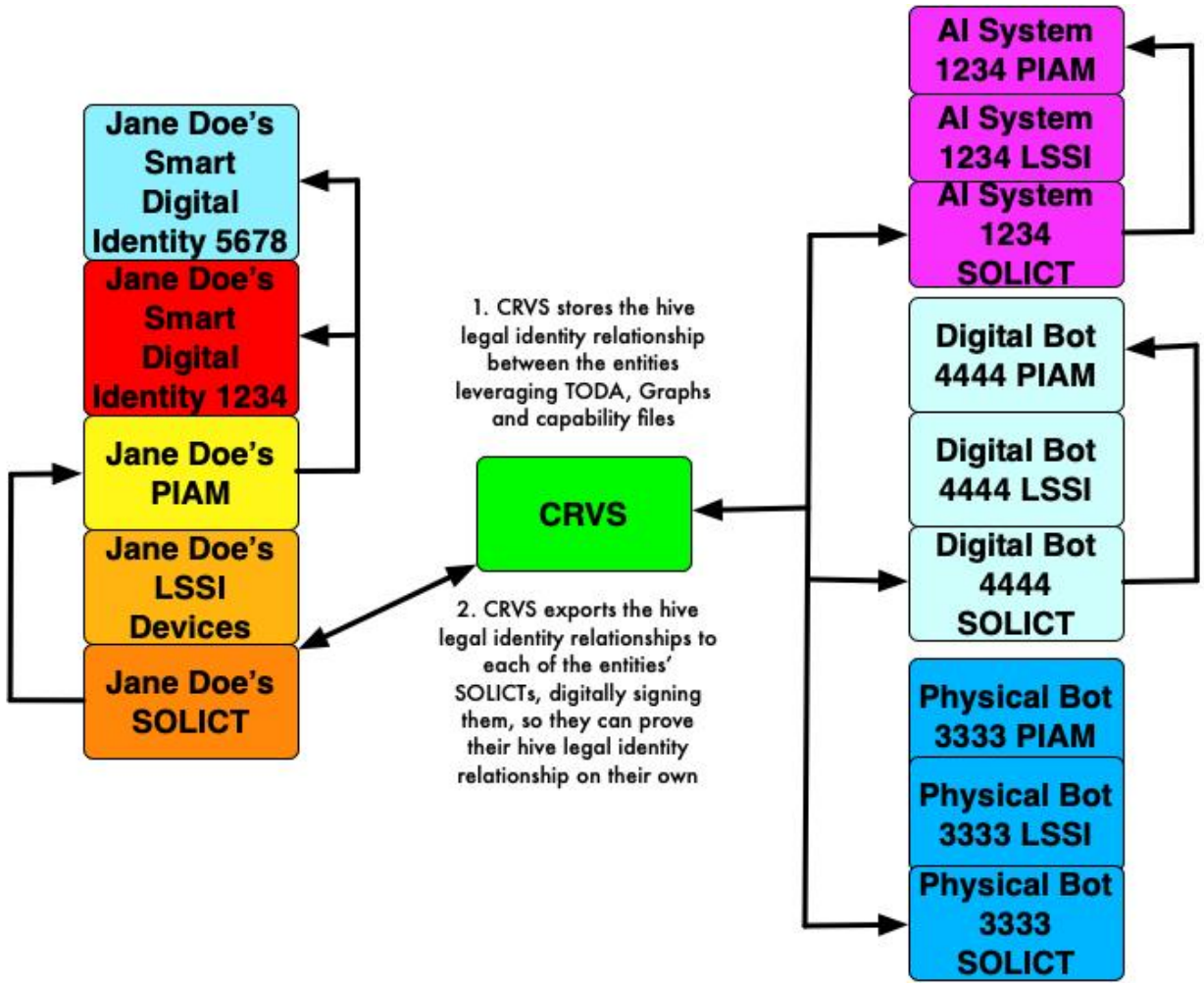
Legal Identity& Hive Relationships Cost Centre Reference Links:

Read the section titled "**Cost Centre – Legal Identity & Hive Relationships**" in "**Cost Centres Rethinking Legal Identity Learning Vision**".

Examples 1:


CRVS
School LMS
(Learning Management System)
4. Manages John's legal identity, biometric, behavioral, neural and learning data according to his TODA capability file
3. Makes a quick electronic trip to validate the digital signatures confirming their legal identities and their mother/on legal identity relationship
2. Their PIAMS instantly send their legal identities and legal identity relationship to the school district's LMS
Jane Doe's PIAM
Jane Doe's LSSI Devices
Jane Doe's SOLICT
1. Receives authorization from Jane for releasing his legal identity relationship with his mother to the school district, as well as which of his legal identity, biometric, behavioral and neural data that can be used in school and AI/AR/VR environments via TODA capability file
John Doe's PIAM
John Doe's LSSI Devices
John Doe's SOLICT

Example 2:


AI System 1234 PIAM
AI System 1234 LSSI
AI System 1234 SOLICT
Jane Doe's Smart Digital Identity 5678
Jane Doe's Smart Digital Identity 1234
Jane Doe's PIAM
Jane Doe's LSSI Devices
Jane Doe's SOLICT
1. CRVS stores the hive legal identity relationship between the entities leveraging TODA, Graphs and capability files
CRVS
2. CRVS exports the hive legal identity relationships to each of the entities' SOLICTs, digitally signing them, so they can prove their hive legal identity relationship on their own
Digital Bot 4444 PIAM
Digital Bot 4444 LSSI
Digital Bot 4444 SOLICT
Physical Bot 3333 PIAM
Physical Bot 3333 LSSI
Physical Bot 3333 SOLICT

Legal Authorization Rights

Description:

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 portions of them. Consider this example…

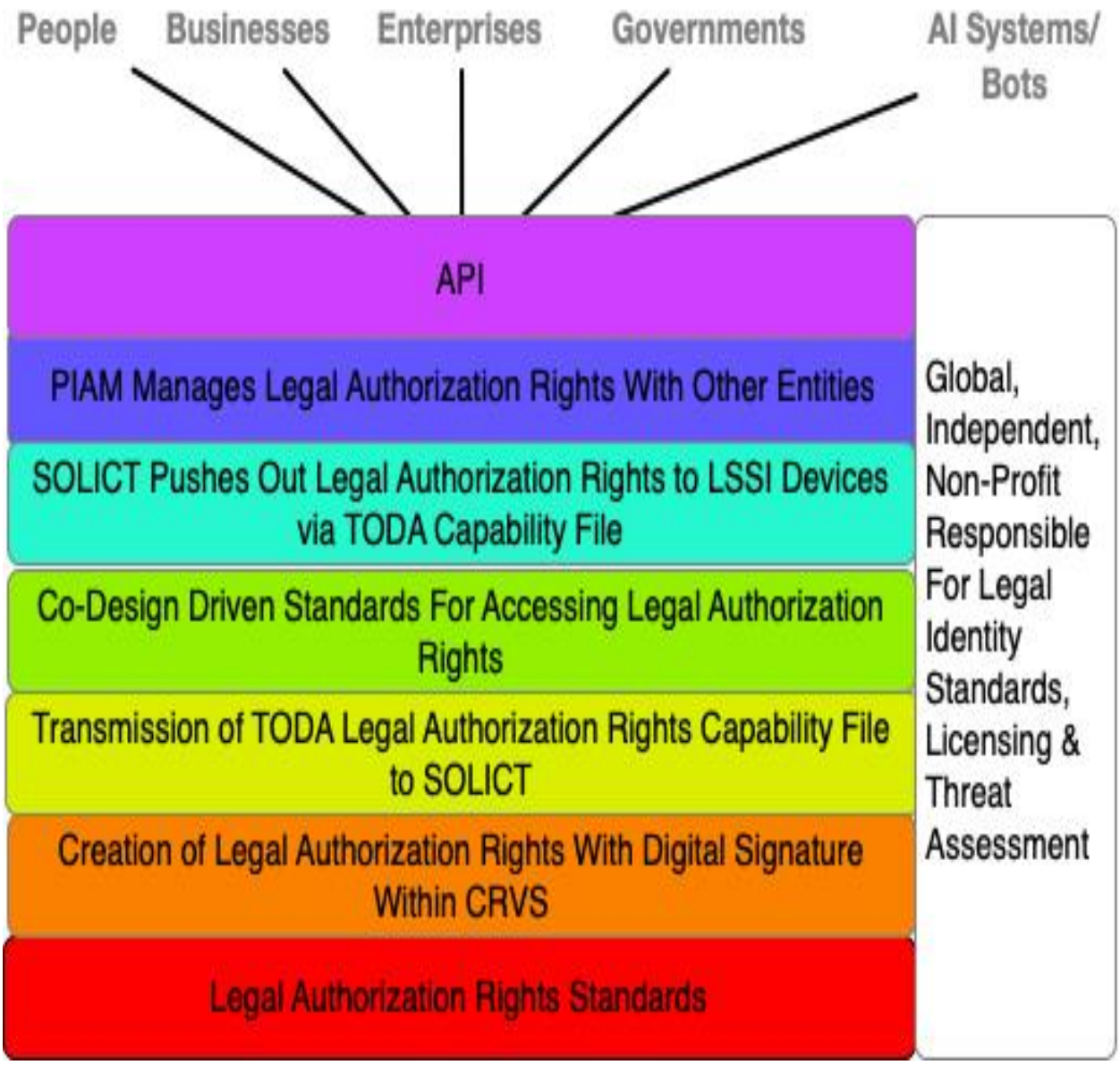
Jane Doe's son, John Doe is attending school. John has a learning assistant bot, AssistBot. How can:

- Jane delegate some of her authority, as John's mother, to the school district agreeing what portions 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.

Skim "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**" to see a new toolkit allowing for legal authorization rights to be created. They show how TODA capability files can be used to be assigned and delegate portions of an entity's authorization rights. It's out of the box thinking for out of the box times.

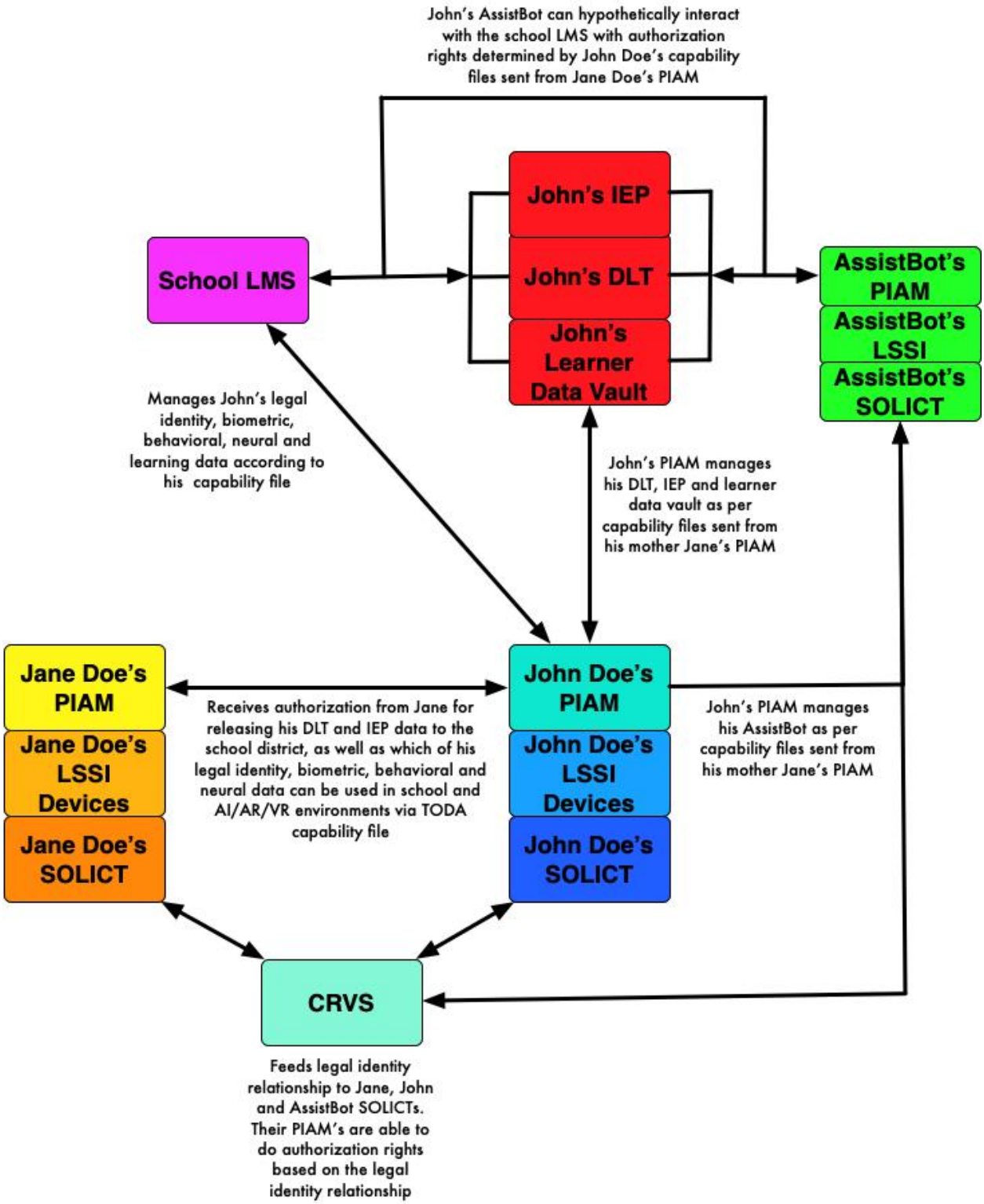
Authorization Rights Cost Centres:



Legal Authorization Rights Cost Centre Reference Links:

Read the section titled "**Cost Centre – Legal Authorization Rights"** in "**Cost Centres- Rethinking Legal Identity & Learning Vision**".

Example:


John's AssistBot can hypothetically interact with the school LMS with authorization rights determined by John Doe's capability files sent from Jane Doe's PIAM
John's IEP
John's DLT
John's Learner Data Vault
School LMS
AssistBot's PIAM
AssistBot's LSSI
AssistBot's SOLICT
Manages John's legal identity, biometric, behavioral, neural and learning data according to his capability file
John's PIAM manages his DLT, IEP and learner data vault as per capability files sent from his mother Jane's PIAM
Jane Doe's PIAM
Jane Doe's LSSI Devices
Jane Doe's SOLICT
Receives authorization from Jane for releasing his DLT and IEP data to the school district, as well as which of his legal identity, biometric, behavioral and neural data can be used in school and AI/AR/VR environments via TODA capability file
John Doe's PIAM
John Doe's LSSI Devices
John Doe's SOLICT
John's PIAM manages his AssistBot as per capability files sent from his mother Jane's PIAM
CRVS
Feeds legal identity relationship to Jane, John and AssistBot SOLICTs. Their PIAM's are able to do authorization rights based on the legal identity relationship

SOLICT - Source of Legal Identity & Credential Truth

Description:

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.

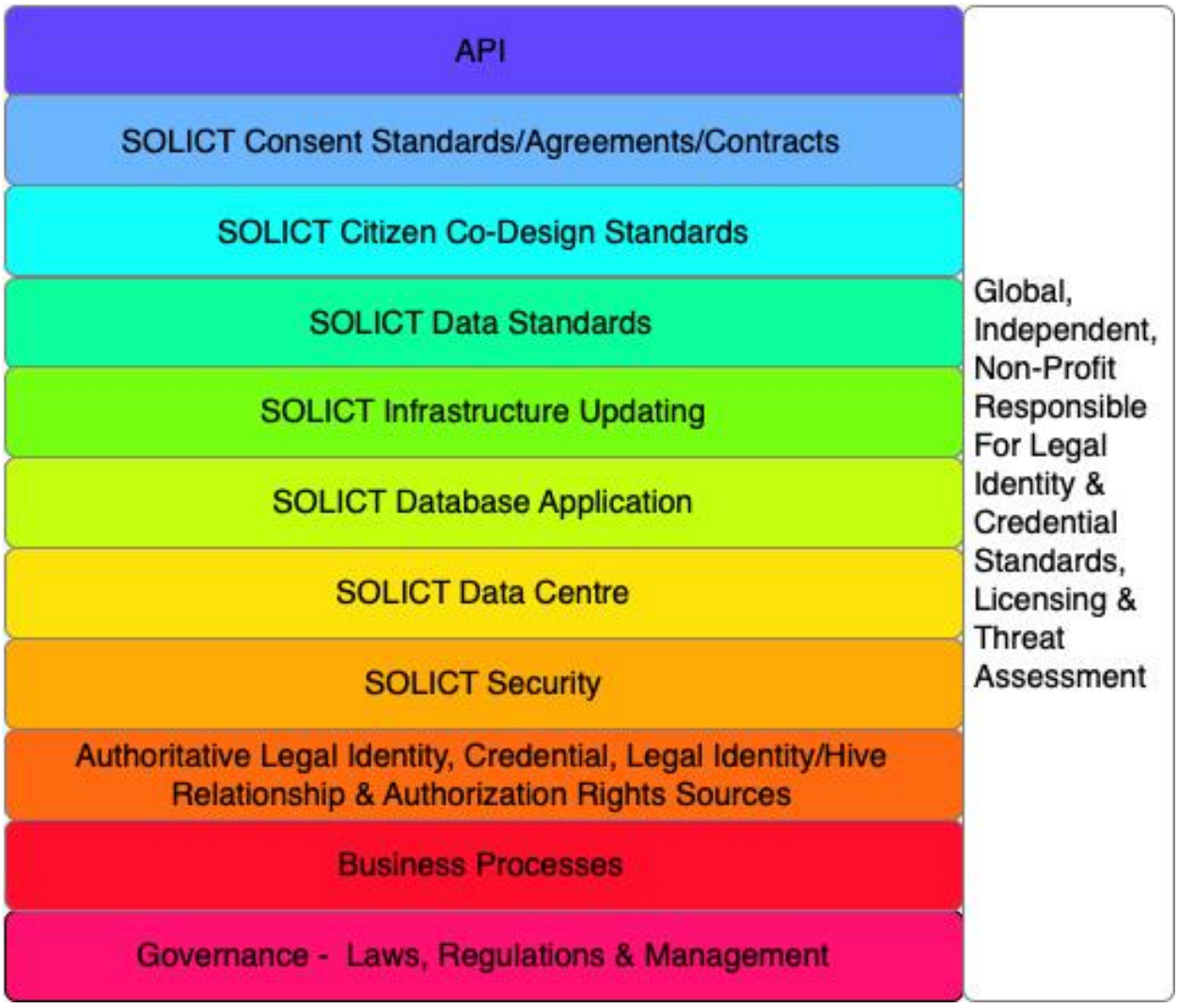
It also reduces the potential impact when a large, legal identity database is breached, with all the records of many people now hacked. By reducing the attack surface for each person, it makes it more complex and costly for criminals to do their work across many different people's legal identities.

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.

It's a new concept, creating new tools for a new age. This brings with it new challenges. It will become the front door to entities wanting to write to the SOLICT, interactions with a person's LSSI (legal self-sovereign identity) devices and their PIAM (personal identity access management) system. Thus, the cost centre document acknowledges this, looking to start small, by doing several crawling steps to get it going.

SOLICT Cost Centre Diagram



SOLICT Cost Centre Reference Links:

Refer to the section titled "**Cost Centre – SOLICT (Source of Legal Identity & Credential Truth)** " in **"**Cost Centres – Rethinking Legal Identity & Learning Vision**"**.

SOLICT Examples:

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

LSSI Devices

Description:

Legal Self-Sovereign Identity (LSSI) devices are a way for a person or entity to prove, with their consent, portions of their legal identity and credentials. It's fed by the person's entity's SOLICT (Source of Legal Identity & Credential Truth), which in turn is fed by authoritative government and/or credential bodies for their legal identity and credentials.

Note:

1. Once the government issues the identity and credential information to an entity's SOLICT/LSSI, the entity is now in control of when, where and how they release their information to
2. All consents given by a entity to a third party to use their legal identity and credential information is written to the entity's SOLICT

There are five potential sources for an LSSI device:

- **Physical legal identity card**
- **Physical wristband biometrically tied to the person**
- **Digital legal identity application**
- **A chip inserted into the person**
- **LSSI information written to the entity's source code**

The biometrically tied wristband is an idea to enable very poor people without access to technology or, people like my mom who's rapidly losing her mental abilities, to be able to function in our modern world. It requires funding to prove it out.

All LSSI devices in the future might be lost or compromised. Thus, they can be revoked and reissued by the entity's SOLICT.

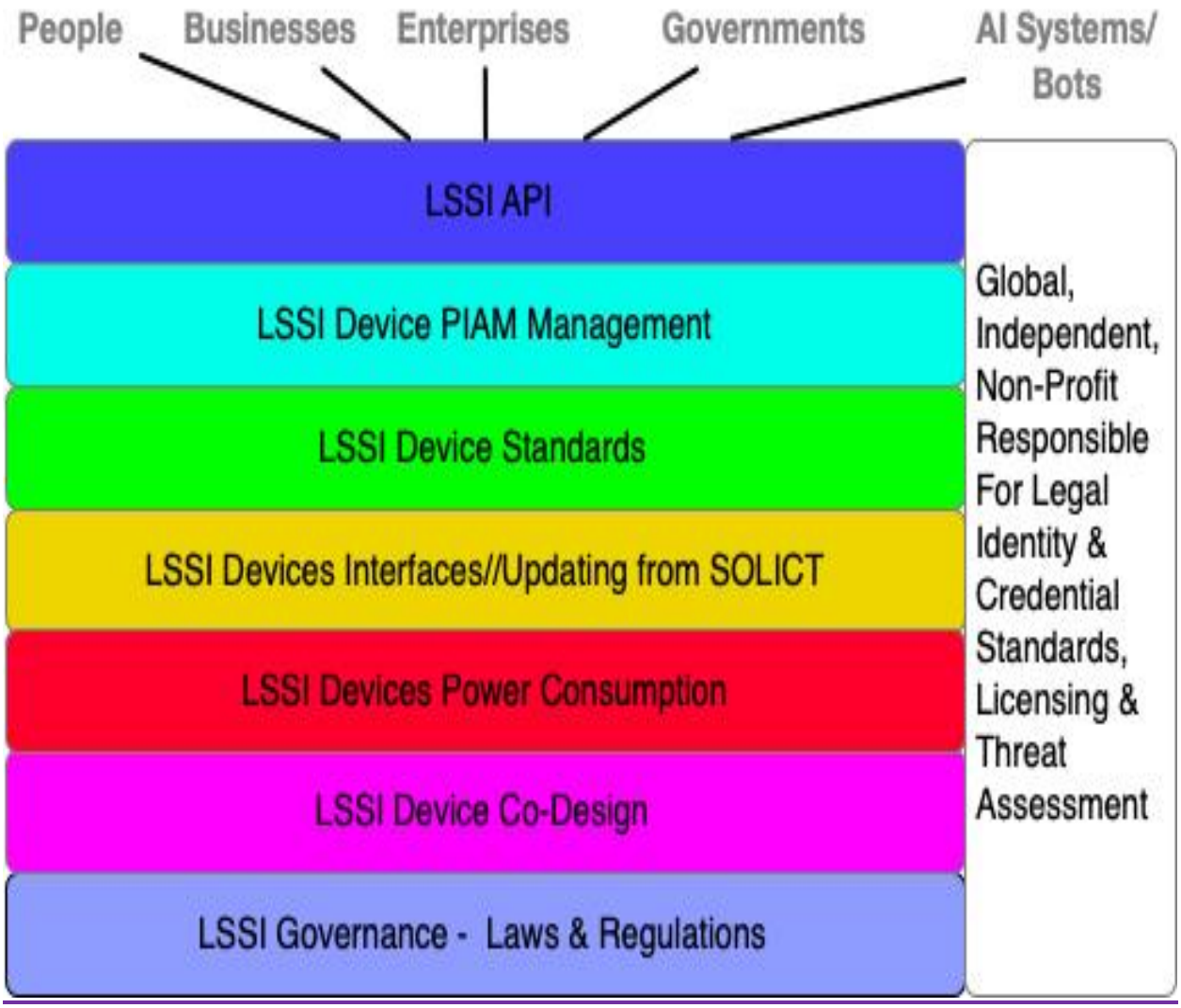
Not all identity and credential information must be on an entity's LSSI device. The choice is up to each entity as to which information to transfer from their SOLICT to their LSSI device.

Further, all citizens on the planet must be able, regardless of their abilities or disabilities to:

- Understand what their LSSI devices are
- Know how to release portions of their legal identity & credential information to third parties
- Make decisions on their own
- Then have their LSSI devices and/or PIAM securely and instantly execute it
- This is where co-design is mission critical

Accessing the LSSI information is via a proposed LSSI API. This will likely come under attack by criminal groups. Thus, the global, independent non-profit, as part of its mandate, establishes standards for the LSSI devices as well as continually looking for new attack vectors. When a attack vector is found, it's rated based on threats and entities will be notified if the threat risk is high to very high. Very high threats must be responded to within hours.

LSSI Devices Cost Centre Diagram



Examples:

Review CRVS examples, Credential examples, and Legal Identity Relationship & Hive examples to see how LSSI works.

LSSI Device Cost Centre Reference Links:

Read the section titled "**LSSI Devices Cost Centre**" in "**Cost Centres- Rethinking Legal Identity & Learning Vision**".

PIAM (Personal Identity Access Management)

Description:

As **Jane Doe walks down a street, wearing AI/AR glasses/contact lenses, she'll be 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.

Further, all citizens on the planet must be able, regardless of their abilities or disabilities to:

- Understand what their PIAM is
- Know how to release portions of their legal identity & credential information to third parties
- Make decisions on their own
- Then have their LSSI devices and/or PIAM securely and instantly execute it

This is where co-design is mission critical

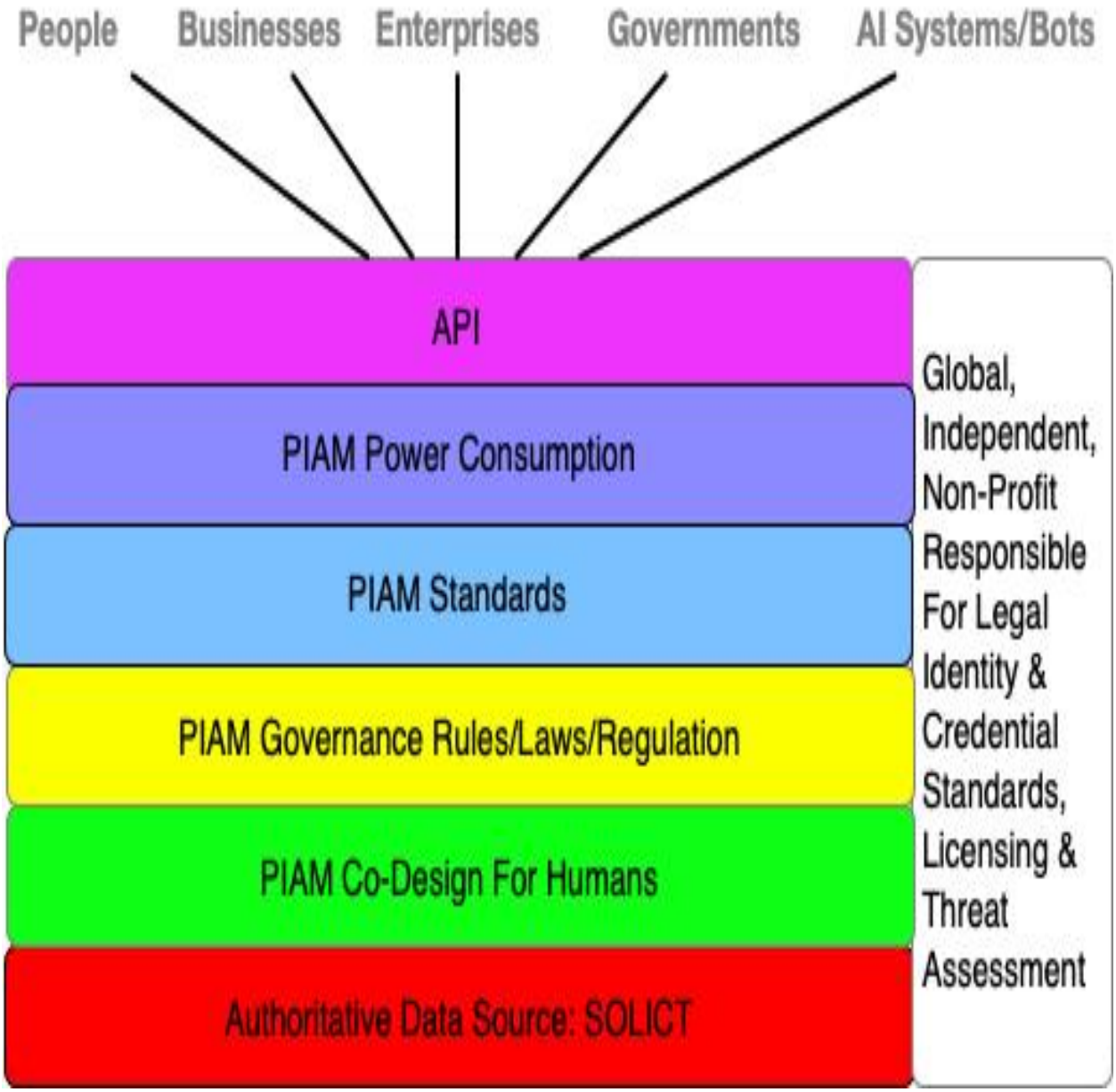
Now making this vision become a reality requires security standards, since the PIAM will become a prime point of attack by criminals. Further, given this curve, it means today's best security standards can quickly become tomorrow's turd. Which is why the architecture calls out for PIAM standards to be 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. 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

PIAM Cost Centre Diagram:

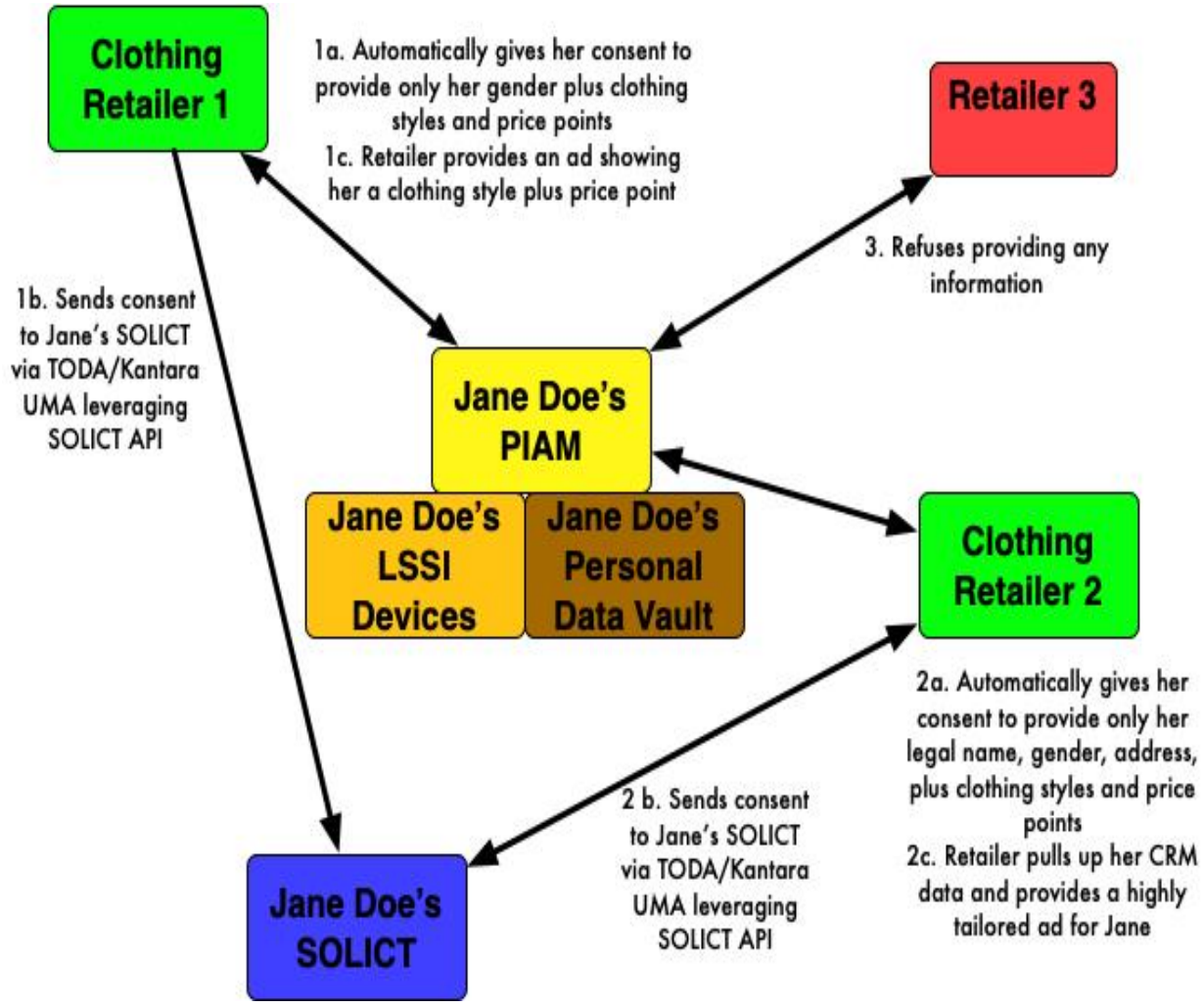


PIAM Cost Centre Reference Links:

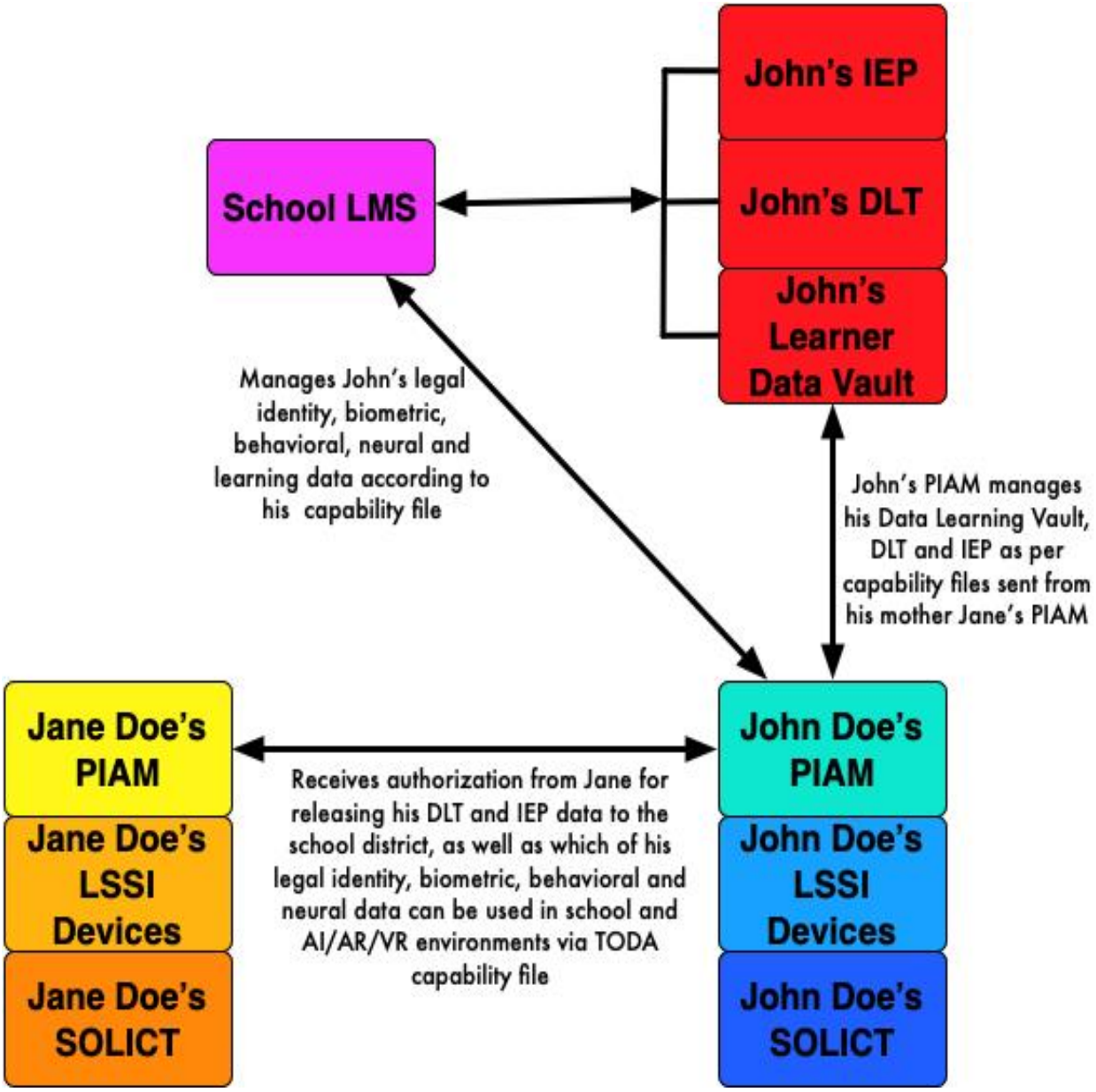
Read the section titled "**Cost Centre - PIAM (Personal Identity Access Management) System**" of "**Cost Centres- Rethinking Legal Identity & Learning Vision**".

Examples:

Jane Doe Walking Down a Shopping Mall

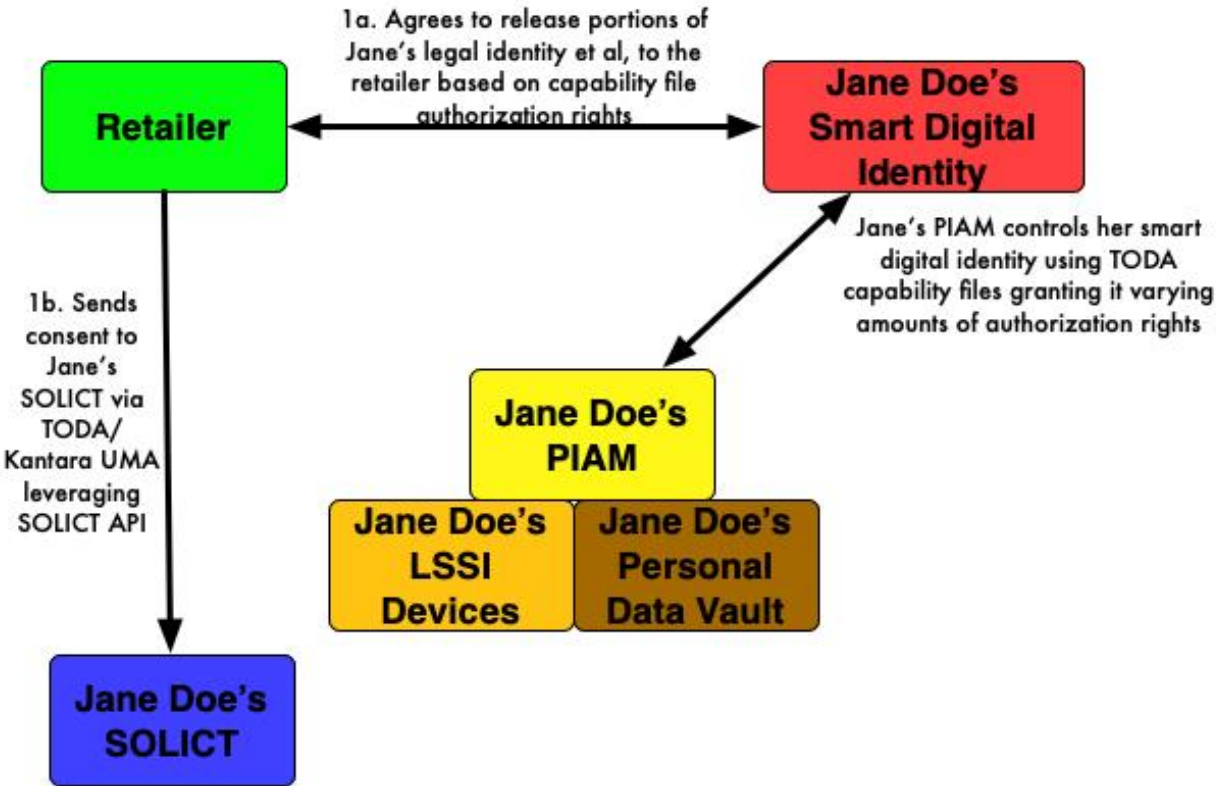


John Doe's in School



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



API

Description:

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?

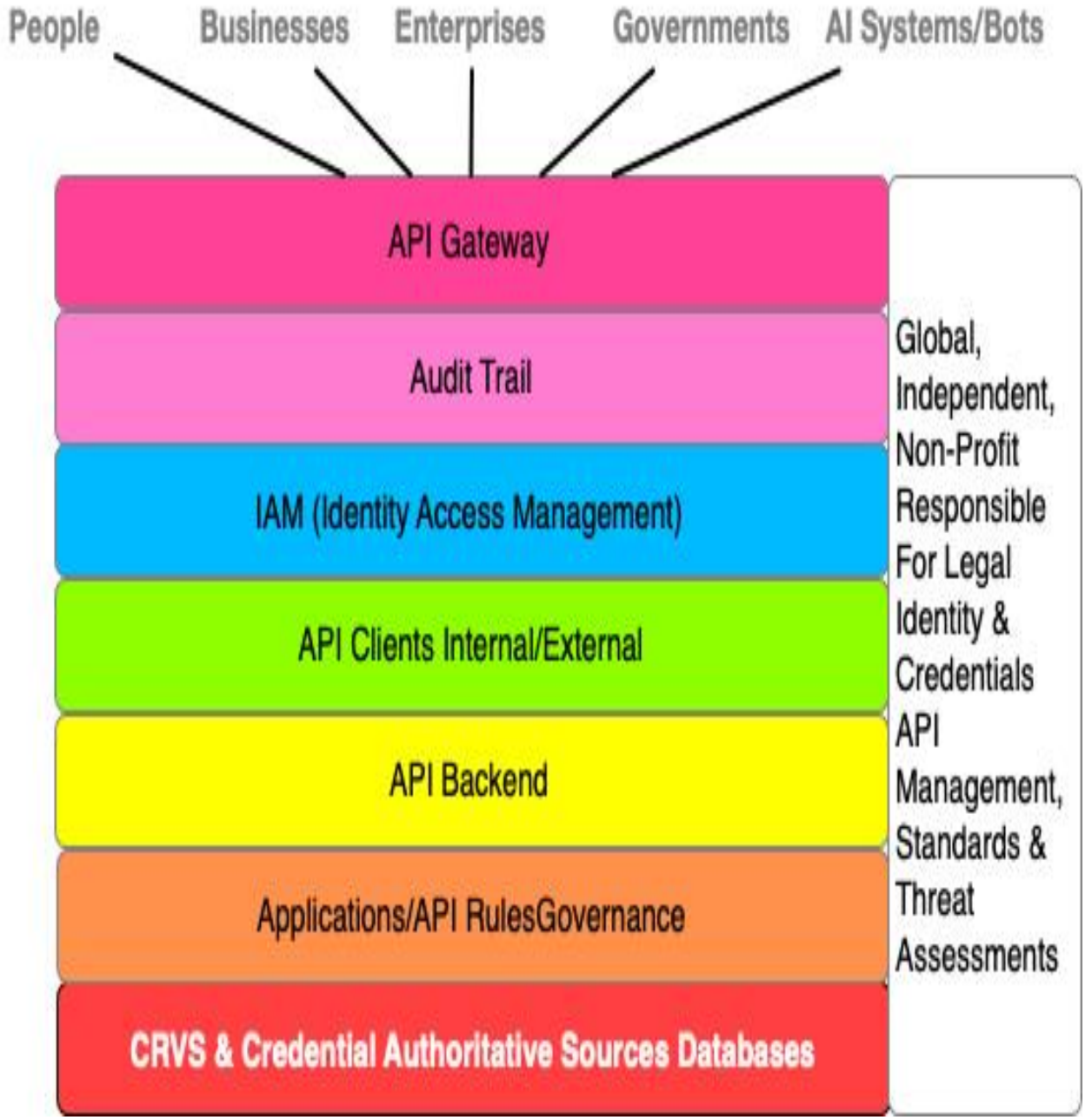
Answer - Create standard API's (Application Programming Interface).

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 Cost Centres:



API Cost Centre Reference Links:

Read the section titled "**Cost Centre: API (Application Programming Interface)**" in "**Cost Centres – Rethinking Legal Identity & Learning Vision**".

Rethought Notaries

Description:

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.

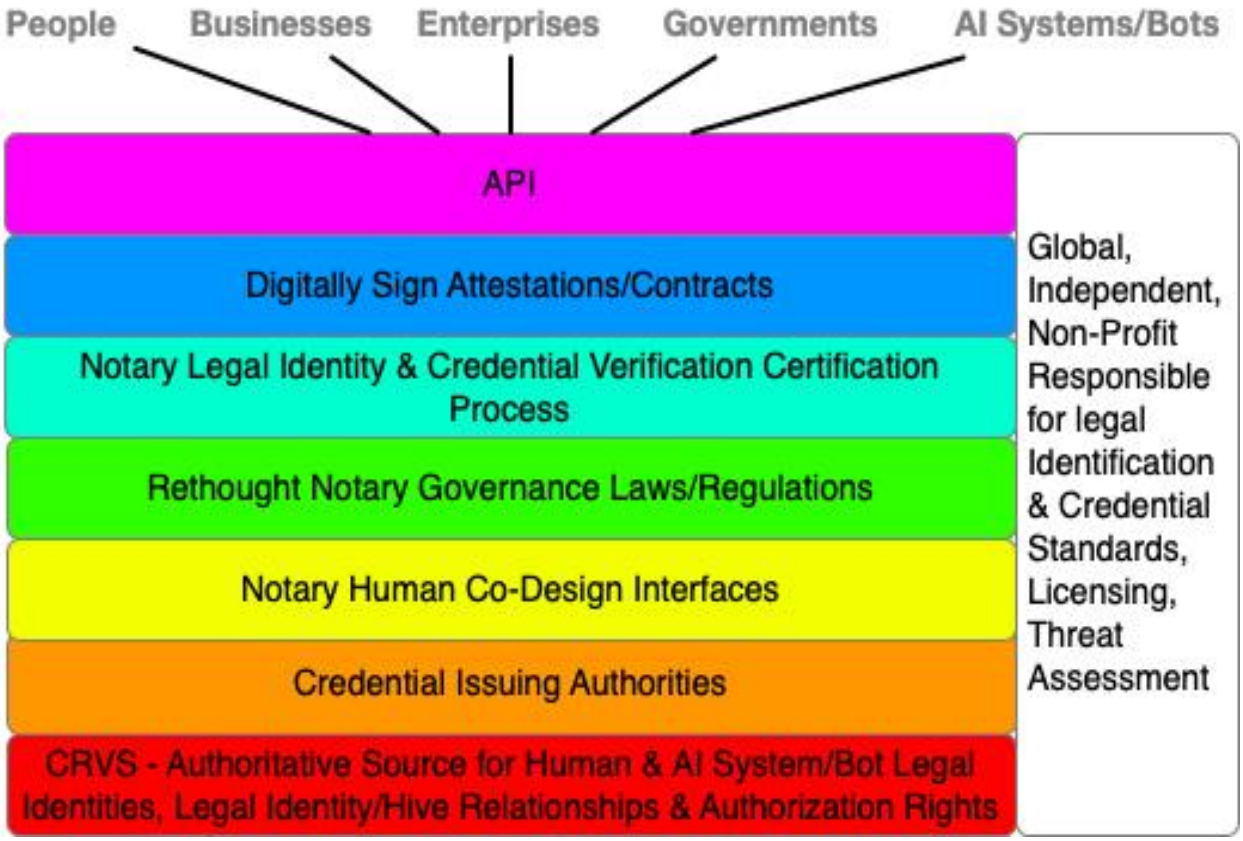
The place to start is by rethinking how they verify entities identities. In today's planet, this can be very challenging, since a person, their smart digital version of them, or an AI system or bot, might be interacting digitally with a local notary, from the other side of the planet.

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.

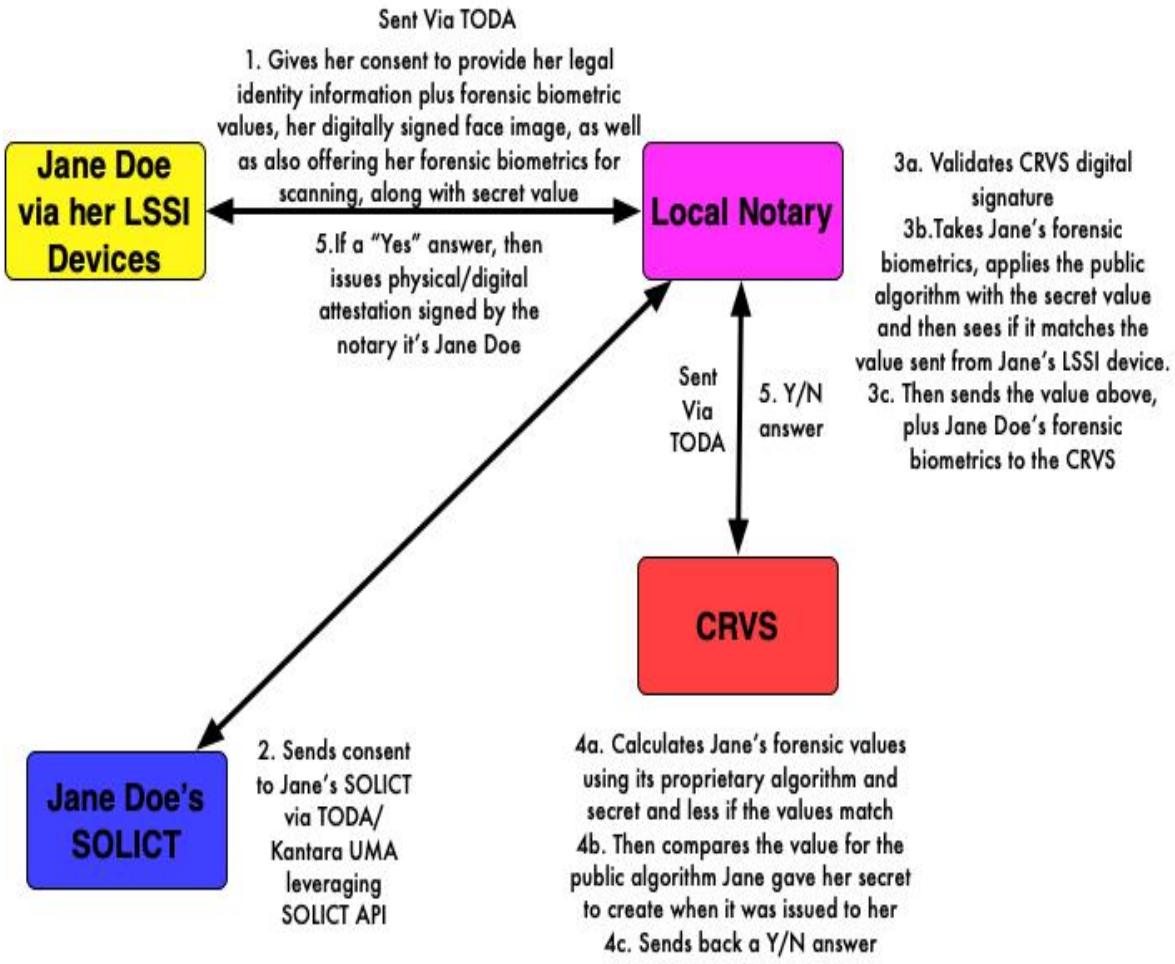
As with the rest of this architecture, it's visionary. I don't want to try to sell the planet on what a wonderful idea it is. Instead, my strategy is to find innovative country funders, with a willing business and notary community, to rethink notaries in small steps. That's what the cost centres call out for. Then, once we've figured it out in real life, rapidly scale.

Rethought Notaries Cost Centre Reference Links:

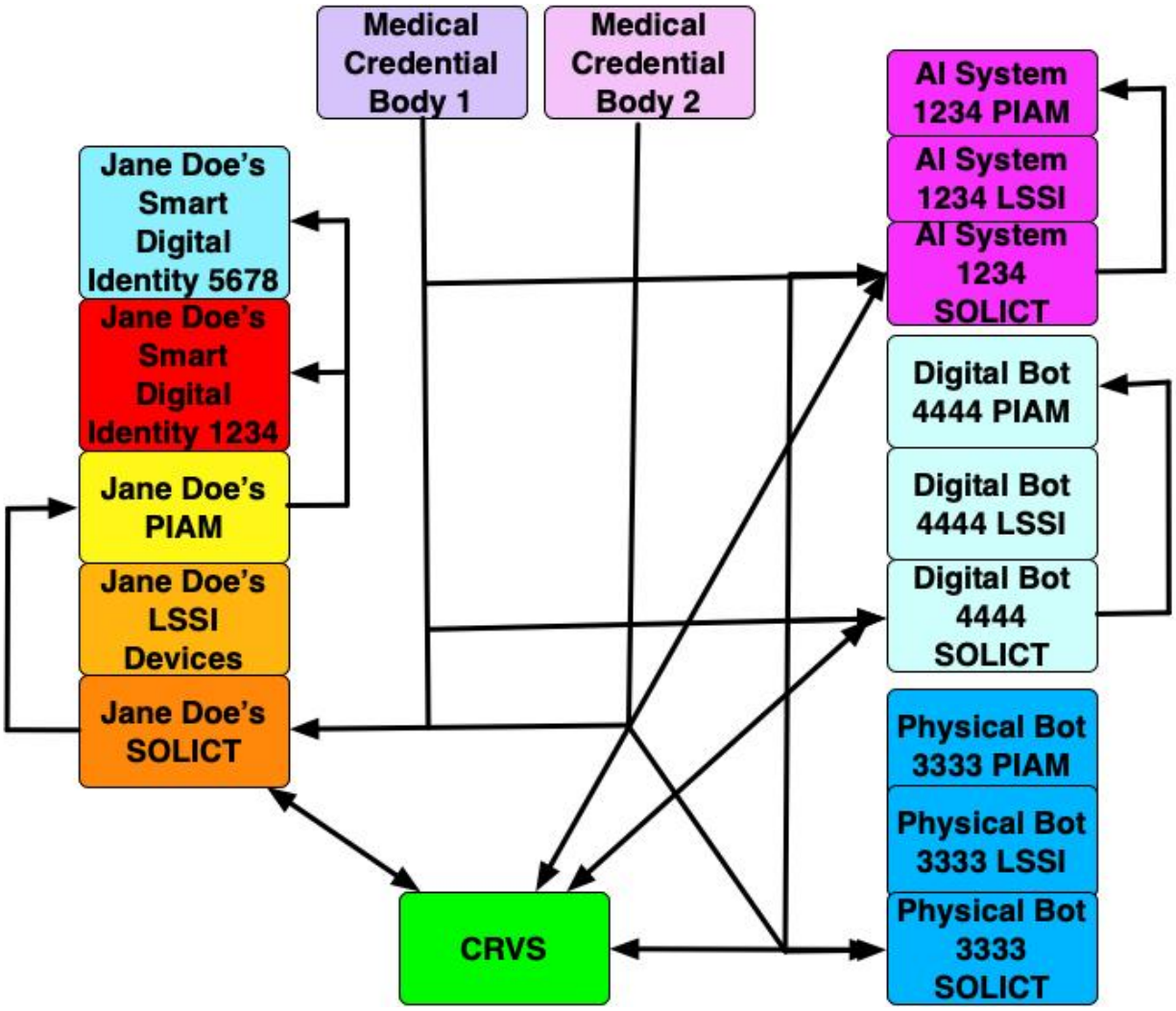


Read the section titled "**Cost Centre: Rethought Notaries**" in "**Cost Centres- Rethinking Legal Identity & Learning Vision**".

Notary Examples:



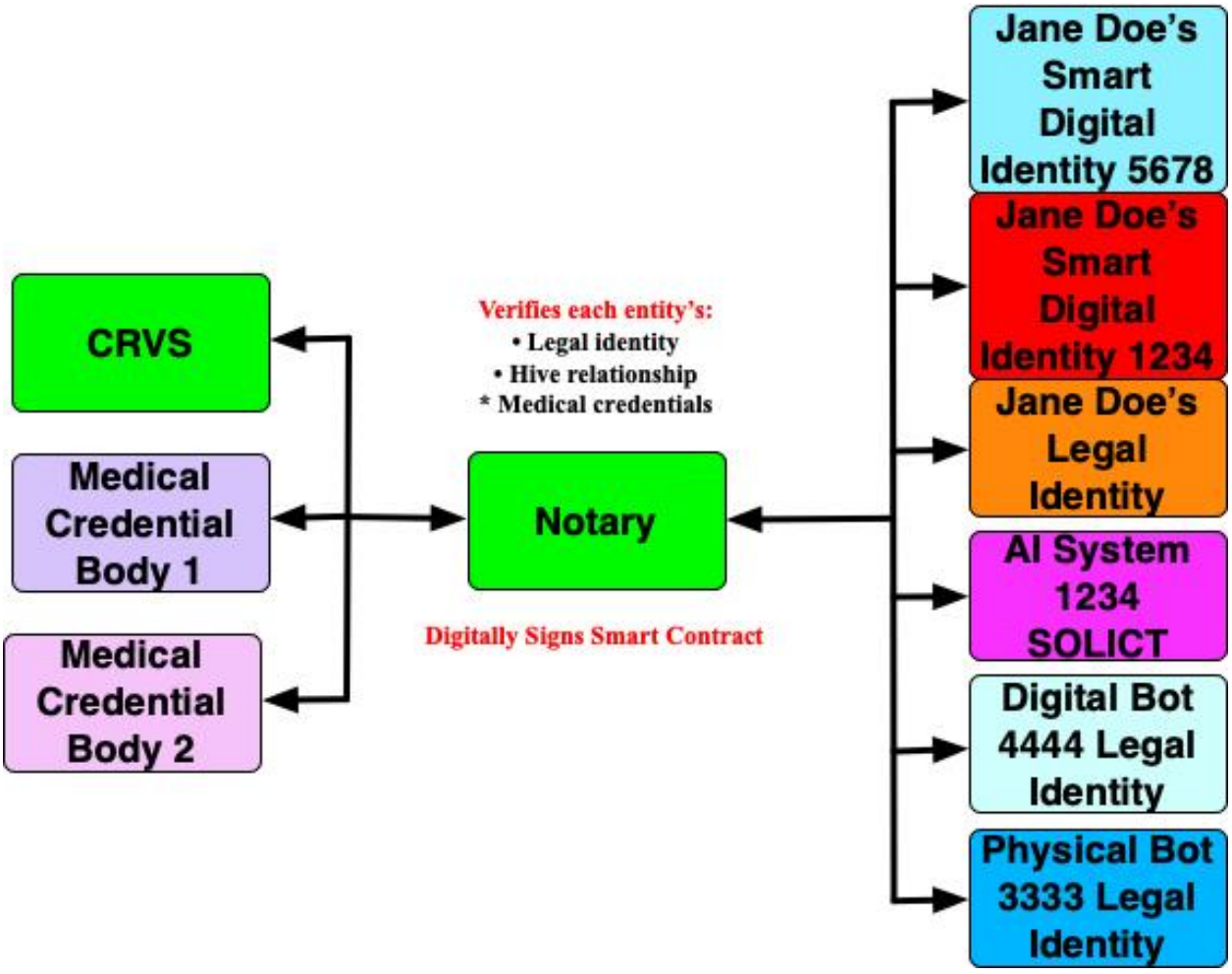
Let's say a legal identity hive is part of Acme Health Inc. which Jane wants to enter into a contract with, requiring identity verification of the entities, via a smart, AI leveraged contract. The two parties might be required to have a notary verify not only the legal identities above, but also their 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:



Global, Independent, Non-Profit

Description:

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 non-profit. Its job is to do the following:

- Establish and maintain new legal identity data standards for humans and AI systems/bots
- Establish CRVS system standards, including legal identity relationships/hives and authorization
- 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
- Run and manage the co-design team for citizen CRVS, SOLICT, LSSI devices, PIAM, credentials, and notary legal identification and credentials queries
- Offer low cost CRVS data conversion systems to rapidly get CRVS's 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

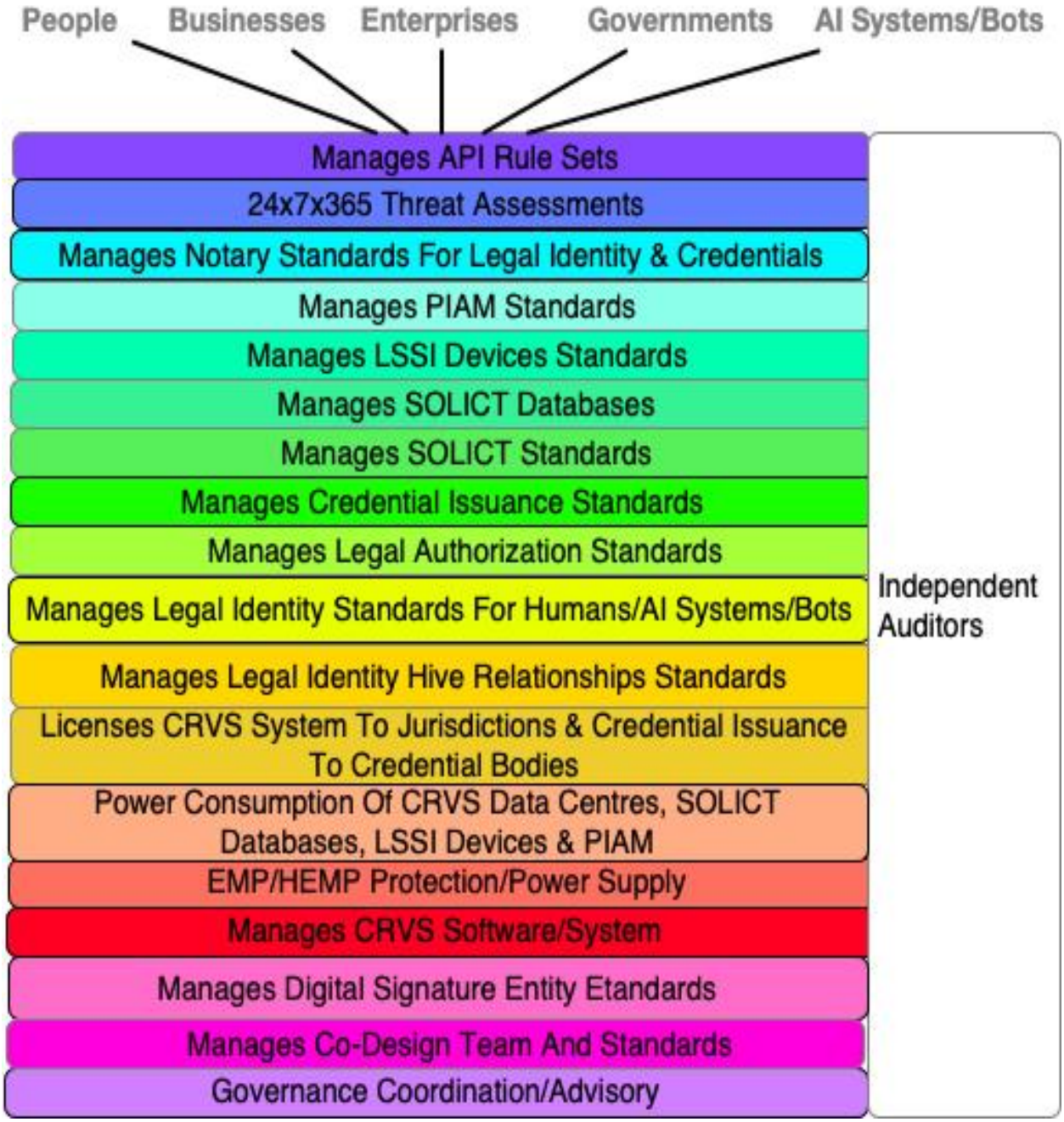
The non-profit will exist in 3 different physical locations, 8 time zones apart. It begs the question, who'll pay for it?

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. My goal was to create a funding structure where the annual income to the non-profit is over $1 billion.

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.

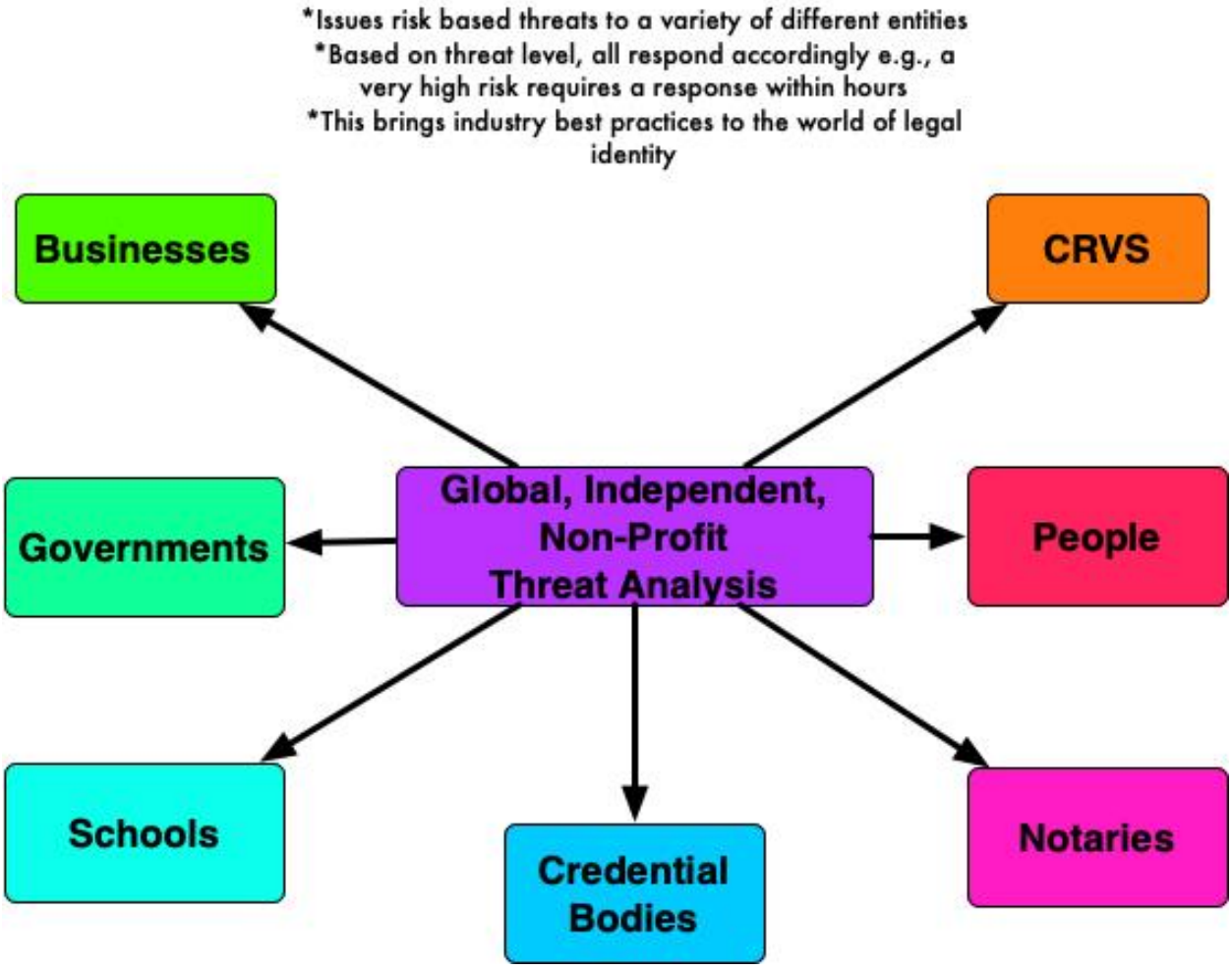
Global, Independent, Non-Profit Cost Centres Diagram:



Global, Independent, Non-Profit Cost Centre Reference Links:

Read the section titled "**Cost Centre - Global, Independent Non-Profit**" in "**Cost Centres-Rethinking Legal Identity & Learning Vision**".

Example:


*Issues risk based threats to a variety of different entities
*Based on threat level, all respond accordingly e.g., a very high risk requires a response within hours
*This brings industry best practices to the world of legal identity
Businesses
CRVS
Governments
Global, Independent, Non-Profit Threat Analysis
People
Schools
Credential Bodies
Notaries

Rethought Business Processes – Competitive Edge

Skim "Give Your Industry A Significant 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?**

The AI/Bot industry they 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.

Rethought Business Processes Cost Centre Reference Links:

Read the section titled "**Cost Centre: Rethought Business Processes – Competitive Edge"** in "Cost Centres- Rethinking Legal Identity & Learning Vision".

Summary

Human legal identity is complex:

- Politically, there's many different local jurisdictions i.e., states/provinces requiring control over their legal identity processes
- Global legal identity standards are required both physically and digitally
- It must be able to work with poor people who don't have access to tech through to those that do as well as for people of all abilities and disabilities
- Address the rapidly emerging smart digital identities of humans
- Needs to be able to handle legally differentiating human clones when they appear
- Must address the rapid rate of change caused by this curve
- Give each of us control over our legal identities
- Create new legal toolkits to easily prove our legal identity relationships including hives

That's what the architecture described in this high-level document delivers.

It will reduce what I call "identity friction" i.e., time, costs and complexities when dealing with legal identities. The first government adopting this will gain for their Ai/bot industry a significant competitive edge. It will also significantly reduce identity theft around the planet.

The strategy this document outlines, and what the cost centres referred to all state, is to crawl, walk and then run. Work with 1-3 countries around the planet to do many different parallel proof of concepts (POC's). Learn what doesn't work, what works, and then do small, tightly controlled pilots. Learn what works in real life. Then rapidly scale.

Achieving this requires an out of the box, innovative country to fund this.

Note:

1. Readers might want to skim, "**Why Should Your Government Fund The Architectures?**"
2. **Total cost guesstimates are between $21.3-35 billion to fund the legal identity/credential and learning architectures.**

About the Author:

Guy Huntington is a veteran, trail blazing identity 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 several countries to fund and deploy.

Guy consults on this.