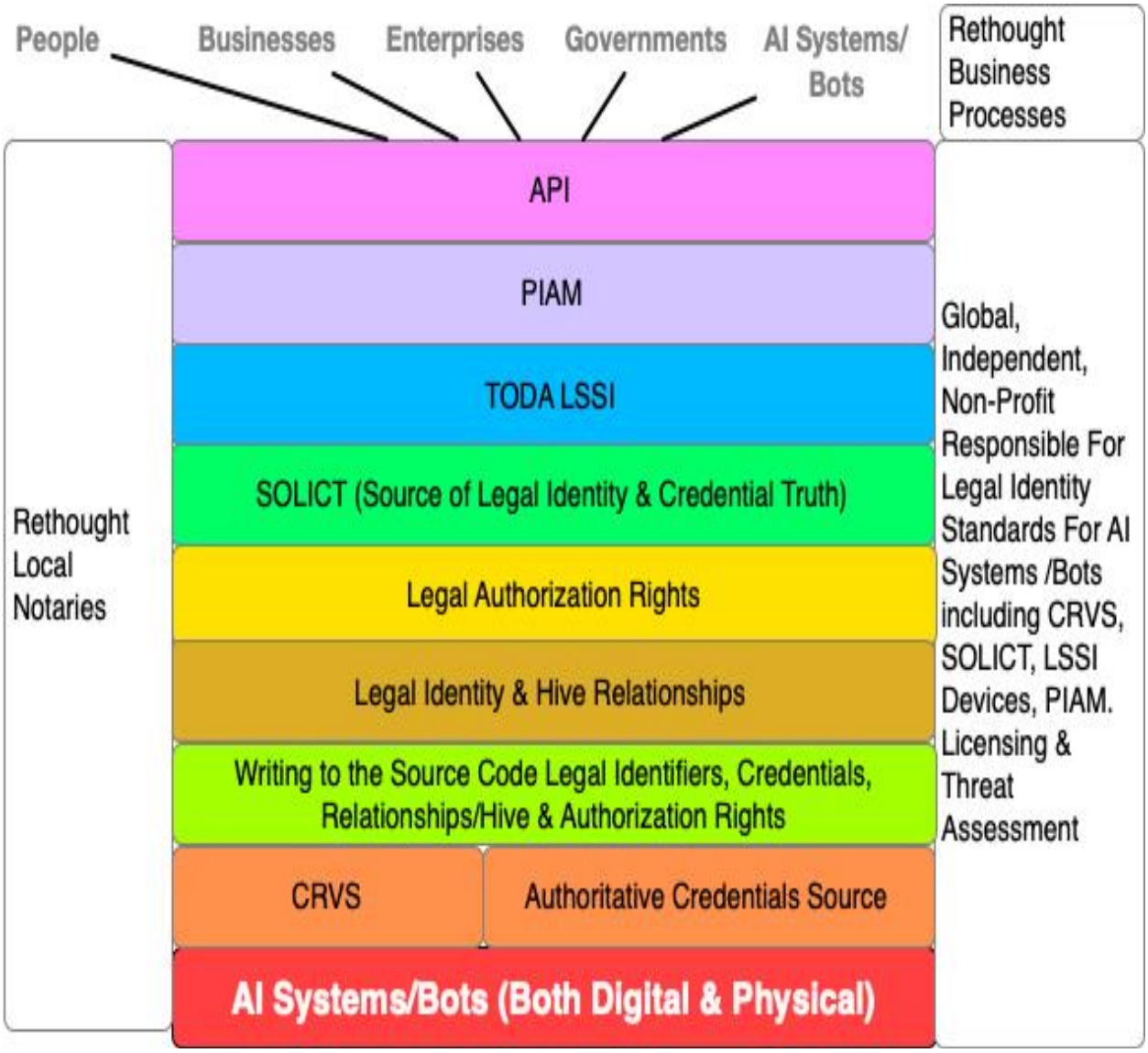
Creating AI Systems/Bots Legal Identity Framework



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

TABLE OF CONTENTS

Executive Summary

The arrival of AI systems and bots is rapidly creating a national security threat. An Evil Inc. or malicious state can leverage an AI system, in one jurisdiction, to produce 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 isn't a legal identity framework to instantly determine entity friend from foe. Thus, we're screwed.

I strongly suggest readers read these articles:

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

To add to this, consider the arrival of hives. Skim "**Hives, AI, Bots & Humans - Another Whopper Sized Problem**". These legal identity relationships can last seconds to years. Further, how will hive membership be managed by hive members?

Then, AI systems and bots require their own abilities to manage their legal identities, credentials, legal identity relationships and consents.

Bottom line? Based on risk, AI systems and bots will require legal identities.

Finally, rapid tech change means new attack vectors can be created against the legal identity framework each hour. How will the architecture be kept continually secure?

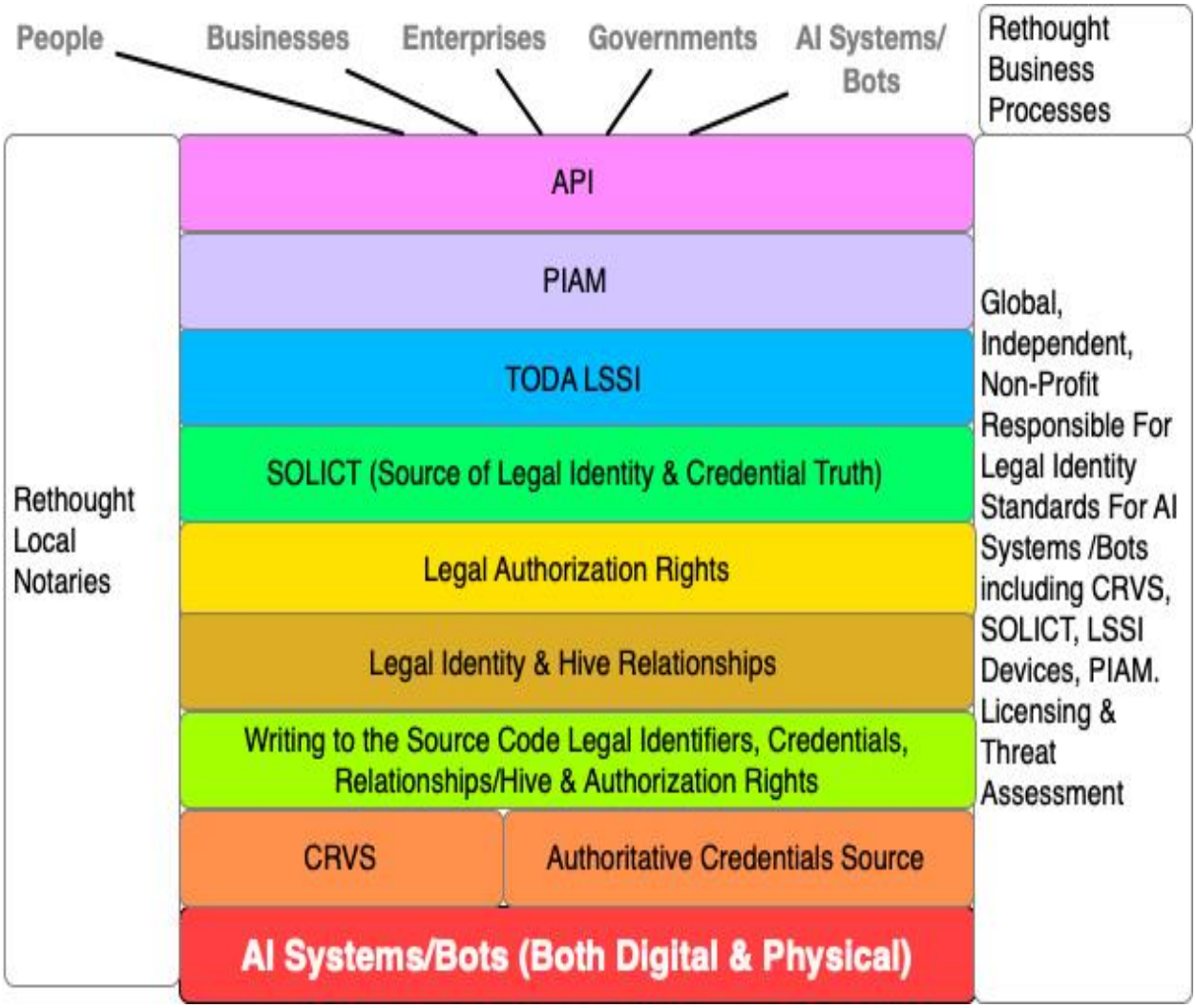
The architecture highlighted by this paper will:

- Instantly prove digital entity friend from foe
- Allow entities to prove their legal identities, relationships, credentials and consents
- Be able to instantly prove hive legal identity relationships
- Be kept continually secure by a new global, independent, extremely well-funded non-profit

Quoting from Albert Einstein, "We can't solve problems by using the same kind of thinking we used when we created them." 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 create a legal identity framework for AI systems and bots. It's written for senior decision makers to get a grasp of the components. It uses this diagram to illustrate the high-level components:



Each component section 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 link to more detailed cost centre information

AI Systems and Bots (Both Digital & Physical)

Description:

The strategy is to find country funders, and then bear down on only 1-2 industry sectors to focus our efforts on. These sectors must include use of:

- AI systems
- Physical bots
- 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:

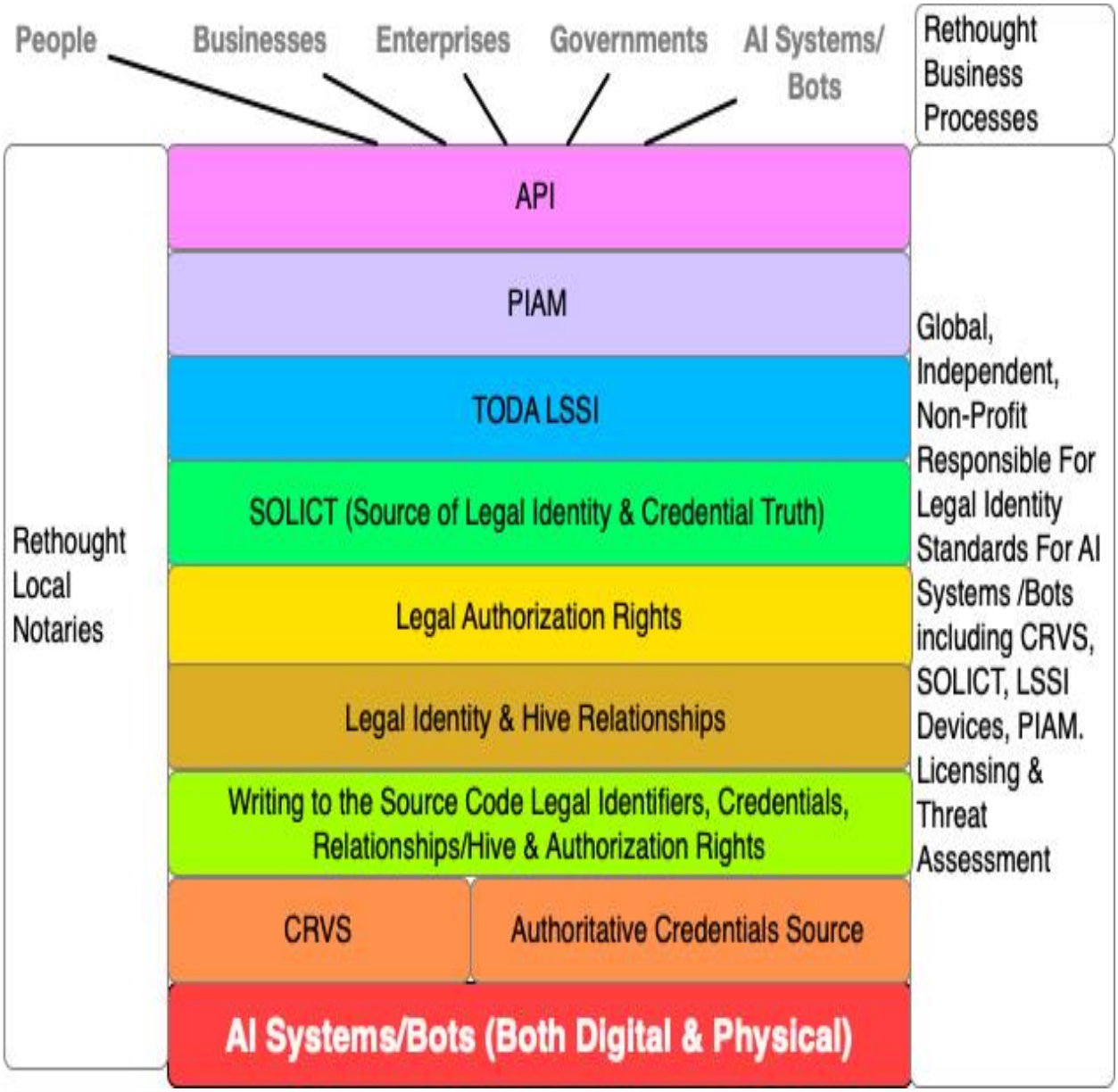
- "**Vision: Learning Journey of Two Young Kids in a Remote Village**"
- "**Sir Ken Robinson - You Nailed It!**"
- "**The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom**"

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

AI System/Bots Cost Centre Reference Links:

Read section titled "**CRVS Artificial Intelligence and Bots Legal Framework Cost Centre"** in "**Cost Centres – Rethinking Legal Identity & Learning Vision**".

AI Systems/Bots CRVS Sub-Component Cost Centre Diagram



AI Systems/Bots CRVS Cost Centre:

Background:

The architecture leverages a new age CRVS system to register AI systems, bot and AI leveraged smart digital identities of humans, in addition to the traditional registration of humans. However, there's a major political challenge in doing this. Legal identity is frequently NOT managed at national levels in many countries on the planet. Instead, it's often done at local state/provincial levels. THEY'RE VERY TERRITORIAL.

Thus, it requires a new framework, still allowing local CRVS jurisdictions to keep control, but plugging them into a global system which can work at "warp speed". Thus, AI systems and digital bots can be registered at transactional speeds into the new age CRVS system.

AI System/Bots CRVS Cost Centre Reference Links:

Read section titled "**CRVS Artificial Intelligence and Bots Legal Framework Cost Centre**" in "**Cost Centres – Rethinking Legal Identity & Learning Vision**".

Authoritative Credential Sources

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 "**Entity Management System**" and "**Verifiable Credentials For Humans and AI Systems/Bots**"

The architecture's strategy is to allow the tens of thousands of different credential bodies on the planet 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 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.

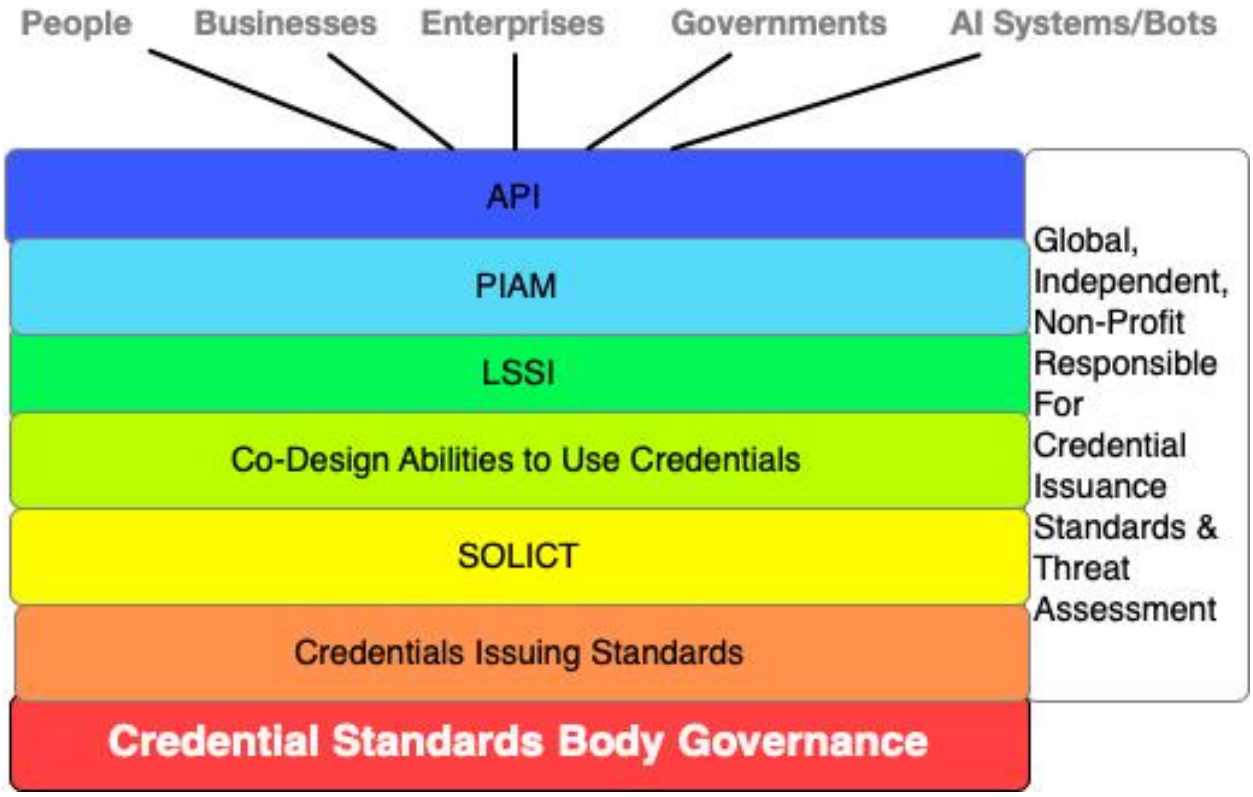
The cost centres associated with this, call out for rapid POC (proof of concept), learning what doesn't work and what works. When ready, do small, tightly controlled pilots in real life. When ready, rapidly scale around the planet.

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 could verify AI MedBot1 has X credentials used in medical diagnosis
- Etc.

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

AI System/Bots Credential Cost Centres:



AI System/Bots Authoritative Credentials Cost Centre Reference Links:

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

Writing to the Source Code Legal Identifiers, Credentials, Relationships/Hives & Authorization Rights

Description:

As noted in **"**The Challenge with AI & Bots - Determining Friend From Foe**"** and **"**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, and then kept up to date 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**
  - 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

For the last four 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.

Skim to page 8 in "Guesstimate Cost Notes: Rethinking Legal Identity, Credentials & Learning" to the section titled, "**Writing Legal Identity to AI Systems/Bots Source Code**". You'll see projected costs of between $1.11-1.59 billion. Why so much? It requires the latest super computers, tech, and the best brains on the planet re programming, legal, security, business processes and governance. If a funding country already has access to this, then the costs will plummet.

That's what this cost centre delivers.

AI System/Bots Source Code Legal Identity/Credential Registration Cost Centre Reference Links:

Read the section titled "**AI/Bots Writing to Source Code Legal Identity/Credential Registration Sub-Component Costs**" in "Cost Centres – Rethinking Legal Identity & Learning Vision".

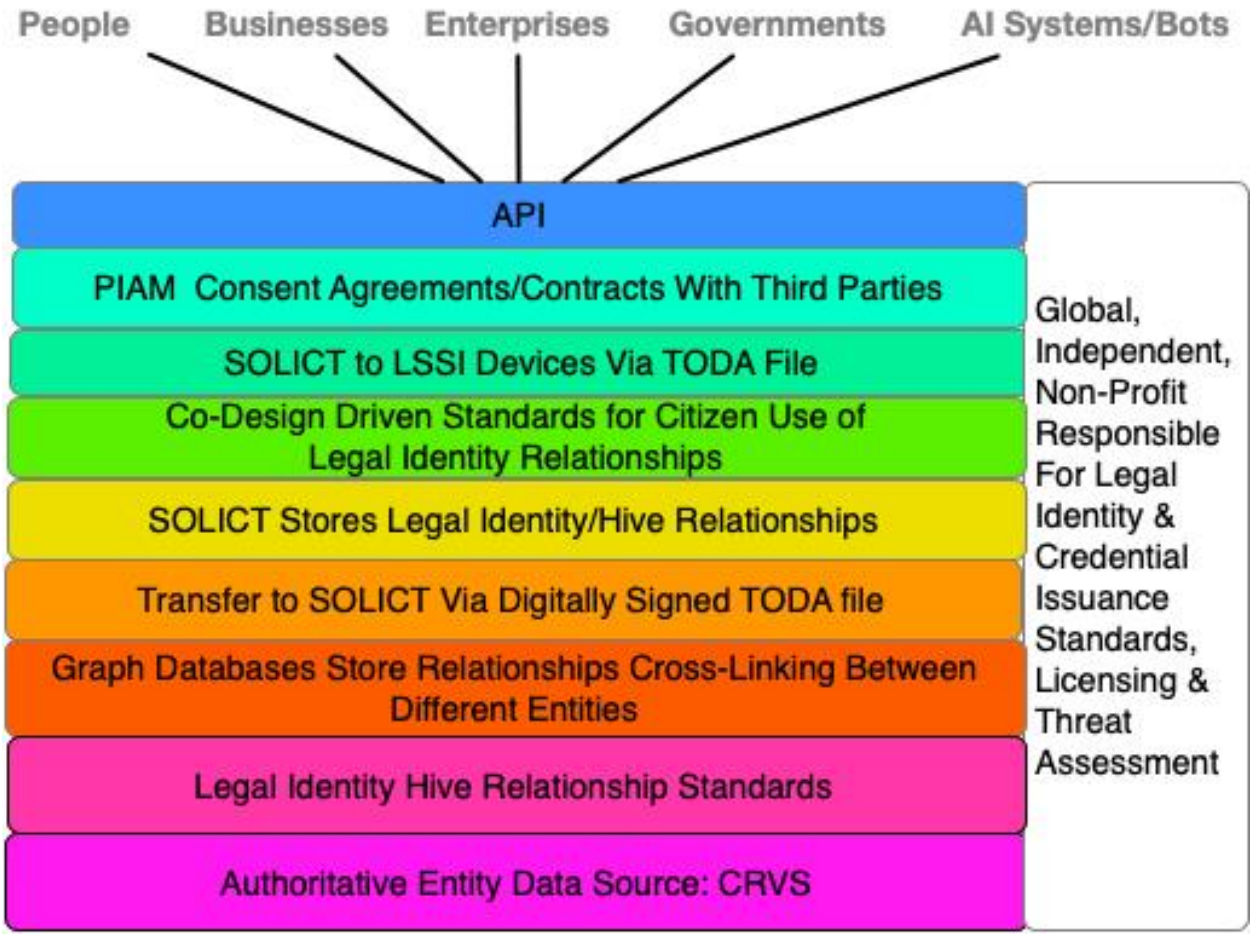
Legal Identity & Hive Relationships

Description:

Skim this article to understand the challenges with legal identity relationships, AI systems/bots and hives, "**Legal Identity Relationships**". It lays out how the new CRVS must be able to manage hives. IT'S NOT A TRIVIAL CHALLENGE.

Thus, as the article states, a new legal architectural toolkit must be used. Skim this, "**TODA, EMS, Graphs – New Enterprise Architectural Tools For a New Age**".

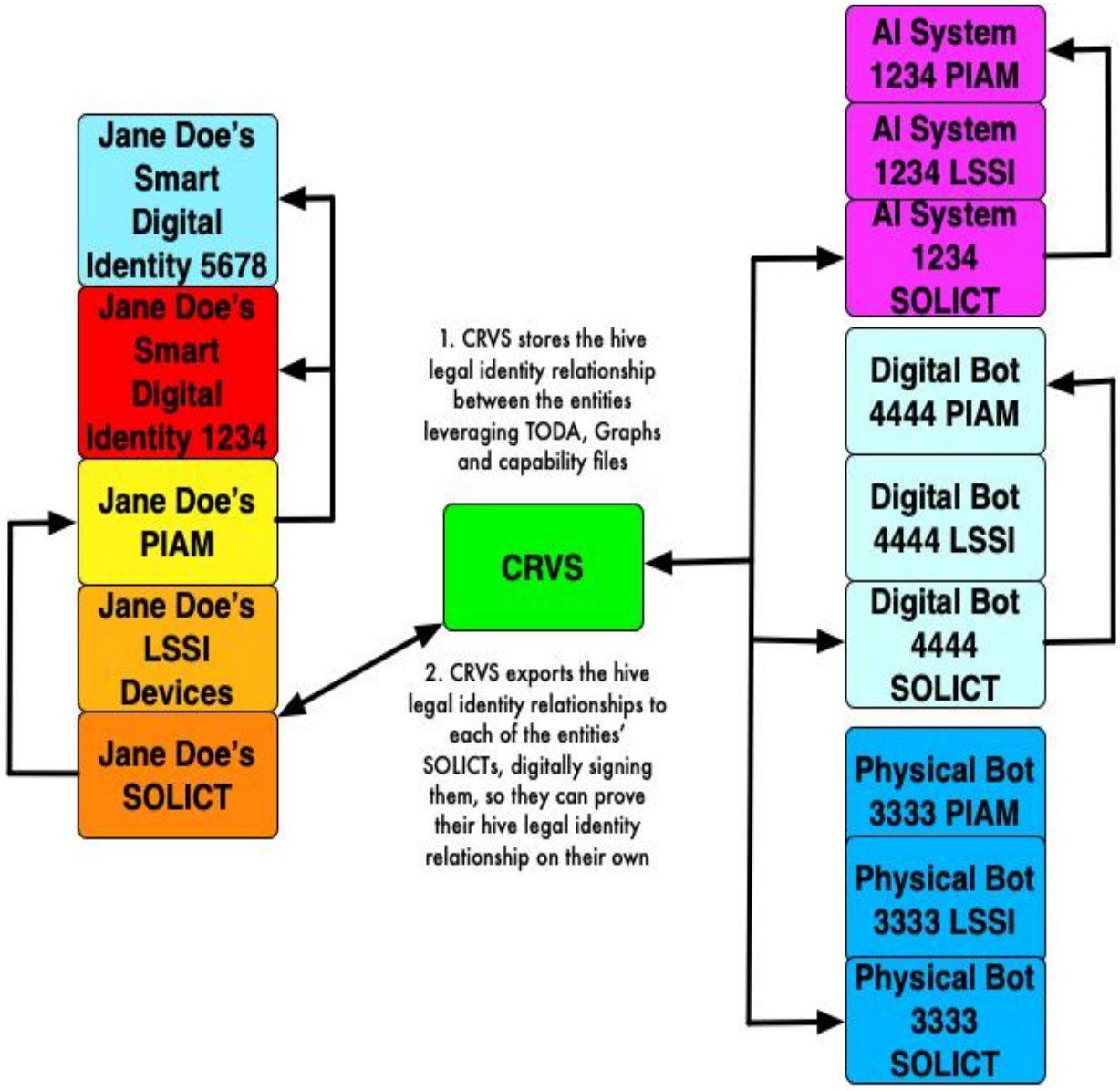
Ai Systems/Bots Legal Identity & Hive Relationships Cost Centres:



AI System/Bots Legal Identity & Hive Relationships Cost Centre Reference:

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

Proving Hive Legal Identity Relationships & Releasing Data Example



Legal Authorization Rights

Description:

Skim this article illustrating legal authorization rights in a global classroom, "**The Coming Classroom Revolution – Privacy & Internet of Things In A Classroom**".

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.**

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**".

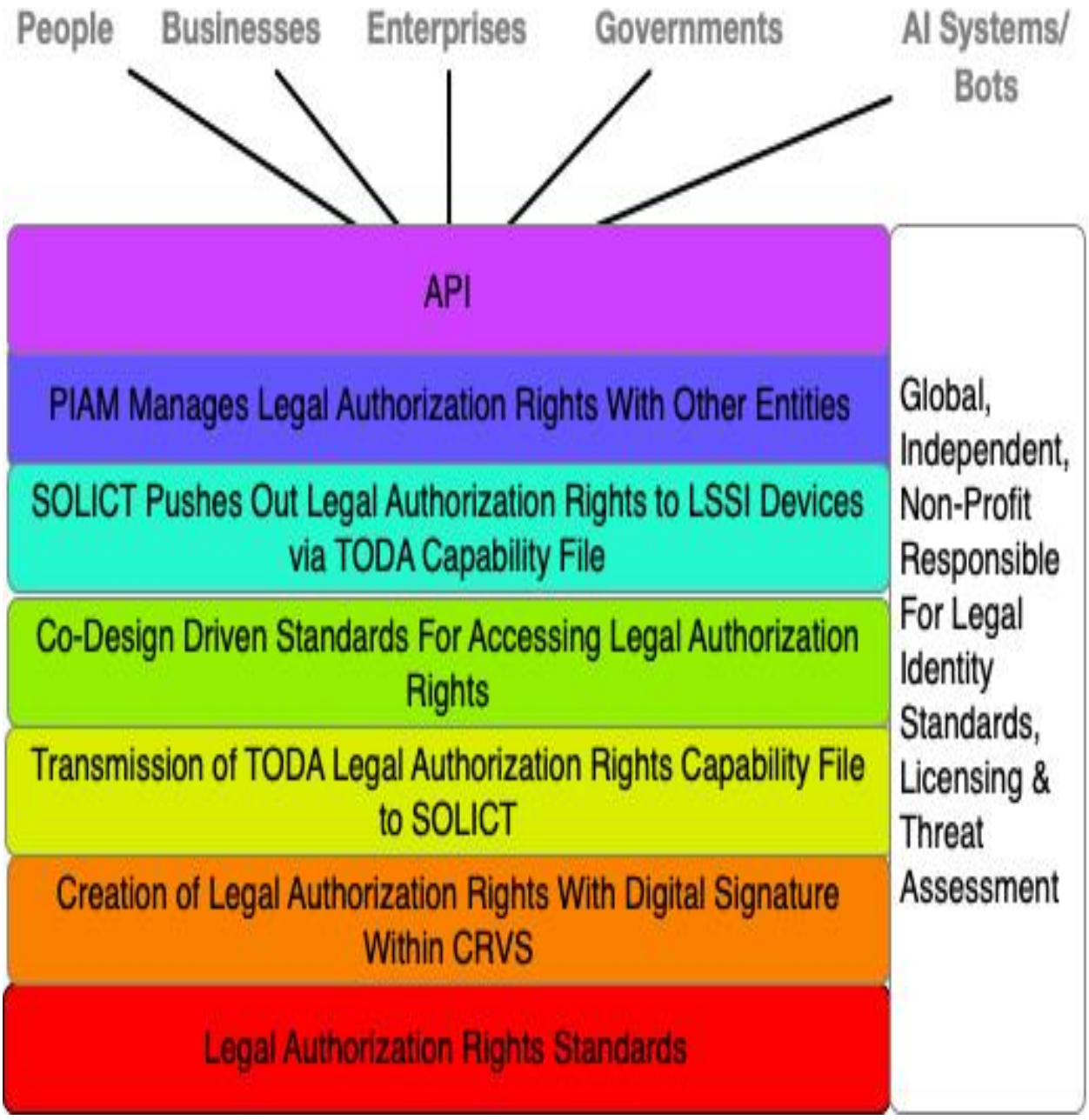
.

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.

My suggestion is to first focus on one industry e.g., education. Try to evolve some standards for AI systems and bots authorization rights, assigning it to a specific legal entity, leveraging Kantara User Managed Access (UMA) to store it in a common, secure, location for each entity. As a last thought, perhaps the Groningen Foundation or, a similar body, might be interested in developing common education contract standards.

There's another large potential problem/challenge with leveraging SOLICTS to store TODA capability files. As mentioned in the SOLICT section, the performance and security considerations MUST be addressed. It applies to TODA capability files as well.

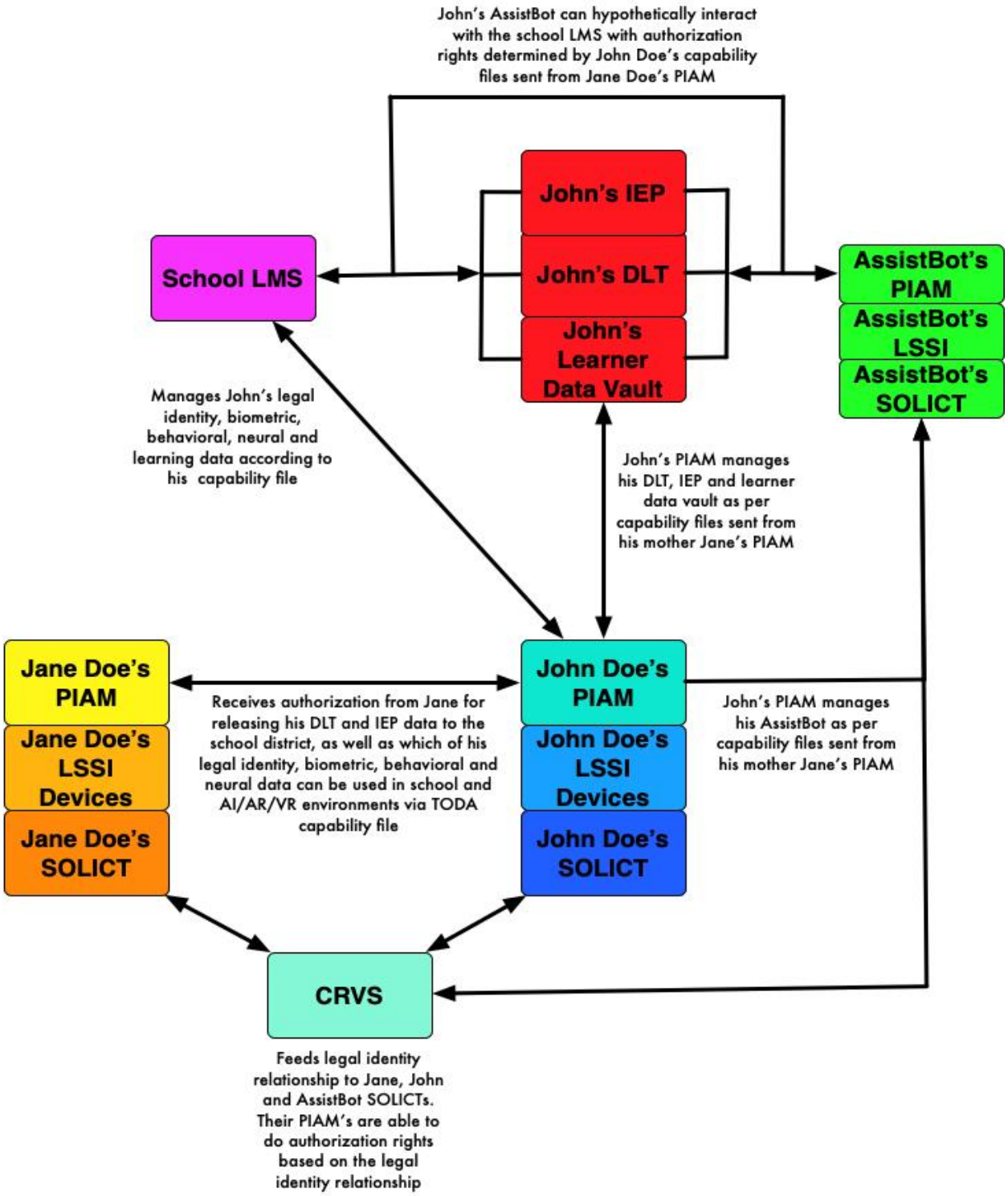
AI Systems/Bots Authorization Rights Cost Centres:



AI System/Bots Authorization Rights Cost Centre Reference Links:

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

AI Systems/Bots Authorization Rights Example:



AI Systems/Bots SOLICT (Source of Legal Identity & Credential Truth)

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:

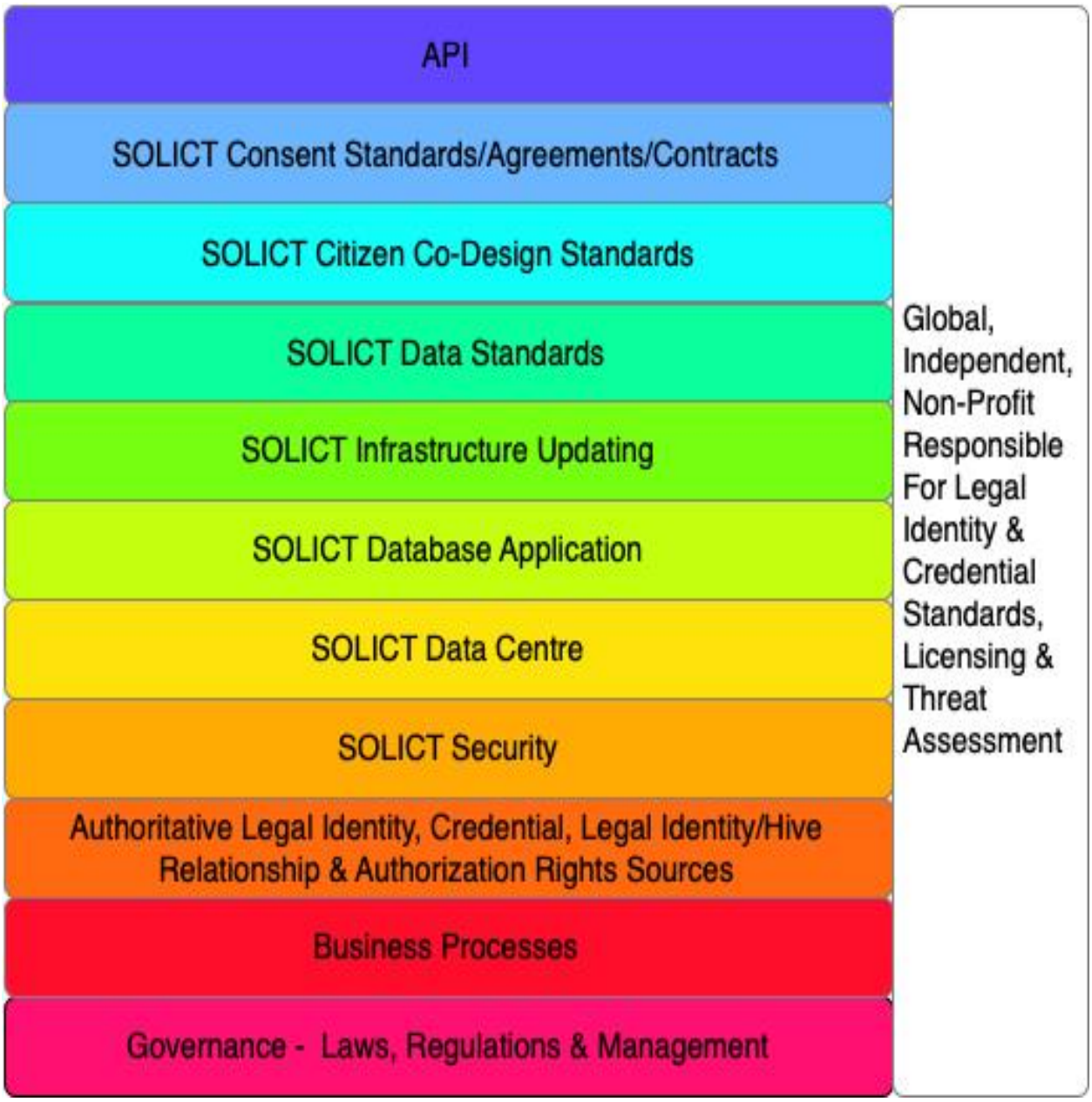
I could easily see how the Evil Inc.'s and malicious states of the planet would leverage this to create new types of denial-of-service attacks against the new age CRVS systems. They could effectively "drown the CRVS" with creations of new entities and sending out to the global, independent non-profit, 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 the above problems/challenges are whopper sized. LOTS OF THOUGHT MUST BE APPLIED BEFORE LEADING TO DESIGN AND POC'S. Caveat emptor.

AI Systems/Bots SOLICT Cost Centers:



AI System/Bots SOLICT Cost Centre Reference Links:

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

AI Systems/Bots LSSI (Legal Self-Sovereign Identity)

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 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:

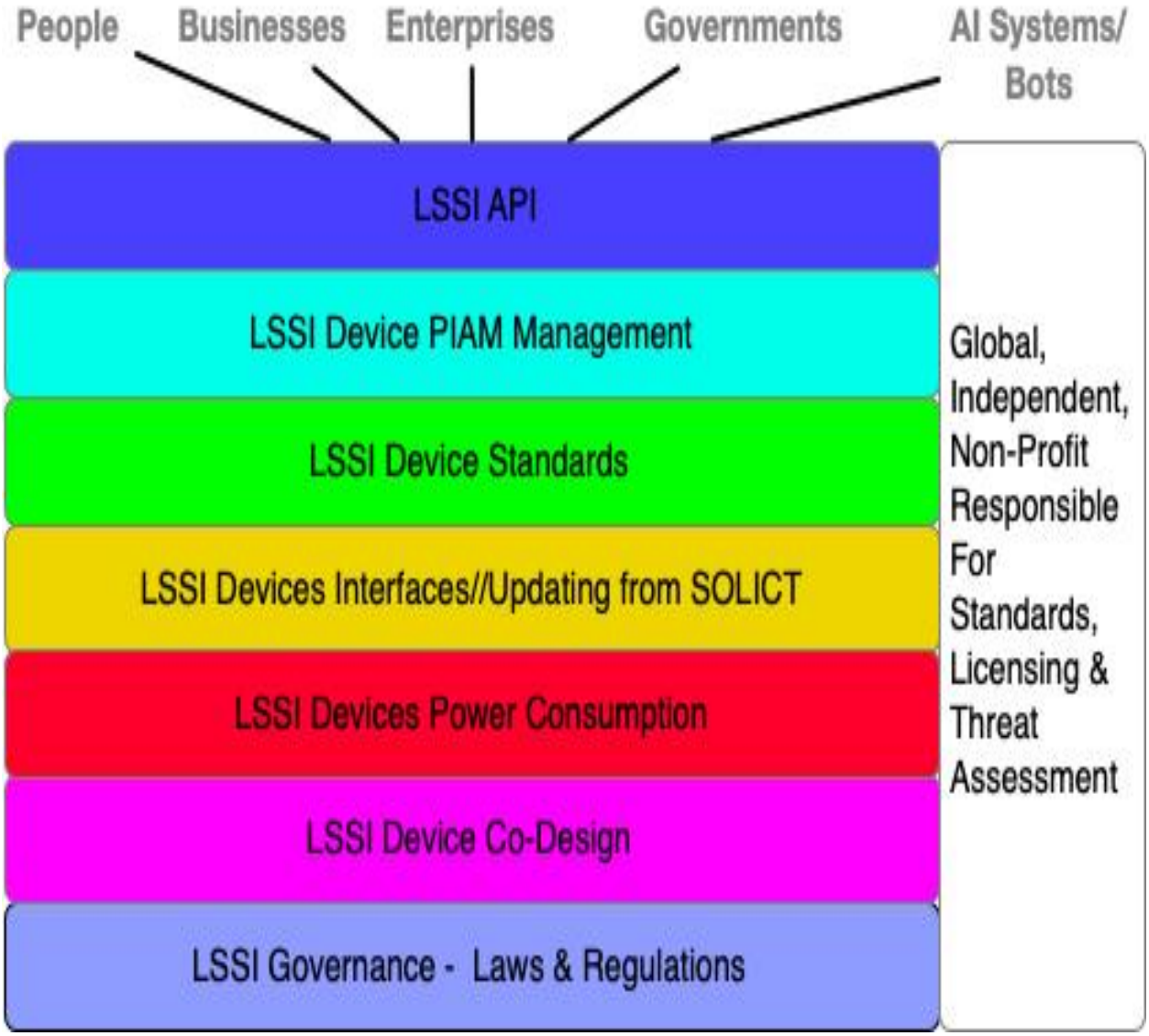
I could see in my mind the awesome speeds at which say digital bots can be created. Over time, it could easily be in the millions or billions per second/. Thus, I saw the new global, independent non-profit managing the SOLICT LSSI creations likely having performance challenges. Thus, this must be addressed 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 of the above problems/challenges are whopper sized. LOTS OF THOUGHT MUST BE APPLIED BEFORE LEADING TO DESIGN AND POC'S. Caveat emptor.

AI Systems/Bots LSSI Cost Centres



AI System/Bots SOLICT Cost Centre Reference Links:

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

AI System/Bots PIAM (Personal Identity Access Management) System

Description:

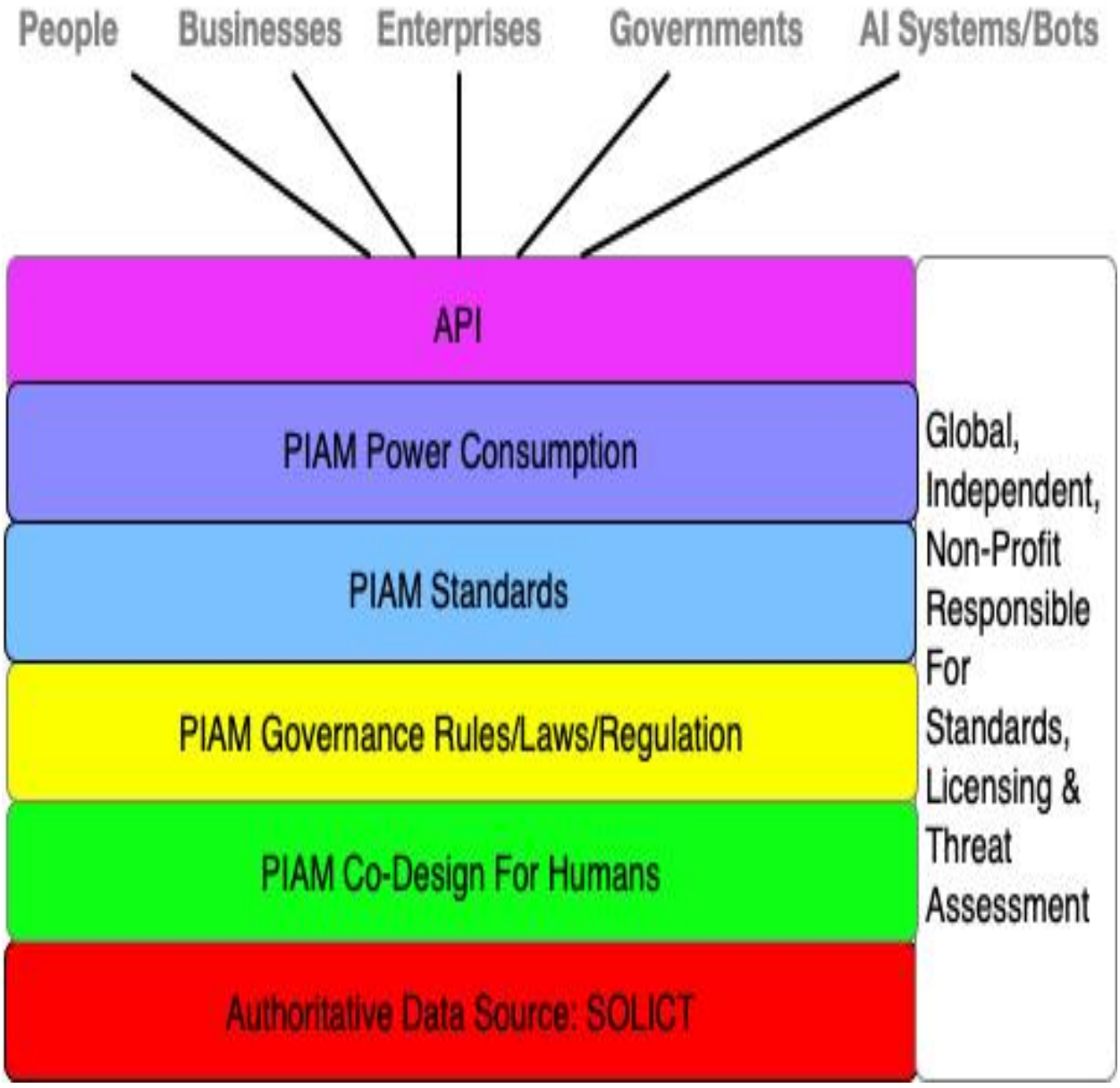
As with the human legal identity architecture, I wanted each entity to have the ability to be in control of their legal identity and consent information. My vision was to create an AI leveraged PIAM able to manage these activities.

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 Cost Centres:



AI System/Bots PIAM Cost Centre Reference Links:

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

API (Application Programming Interface)

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?

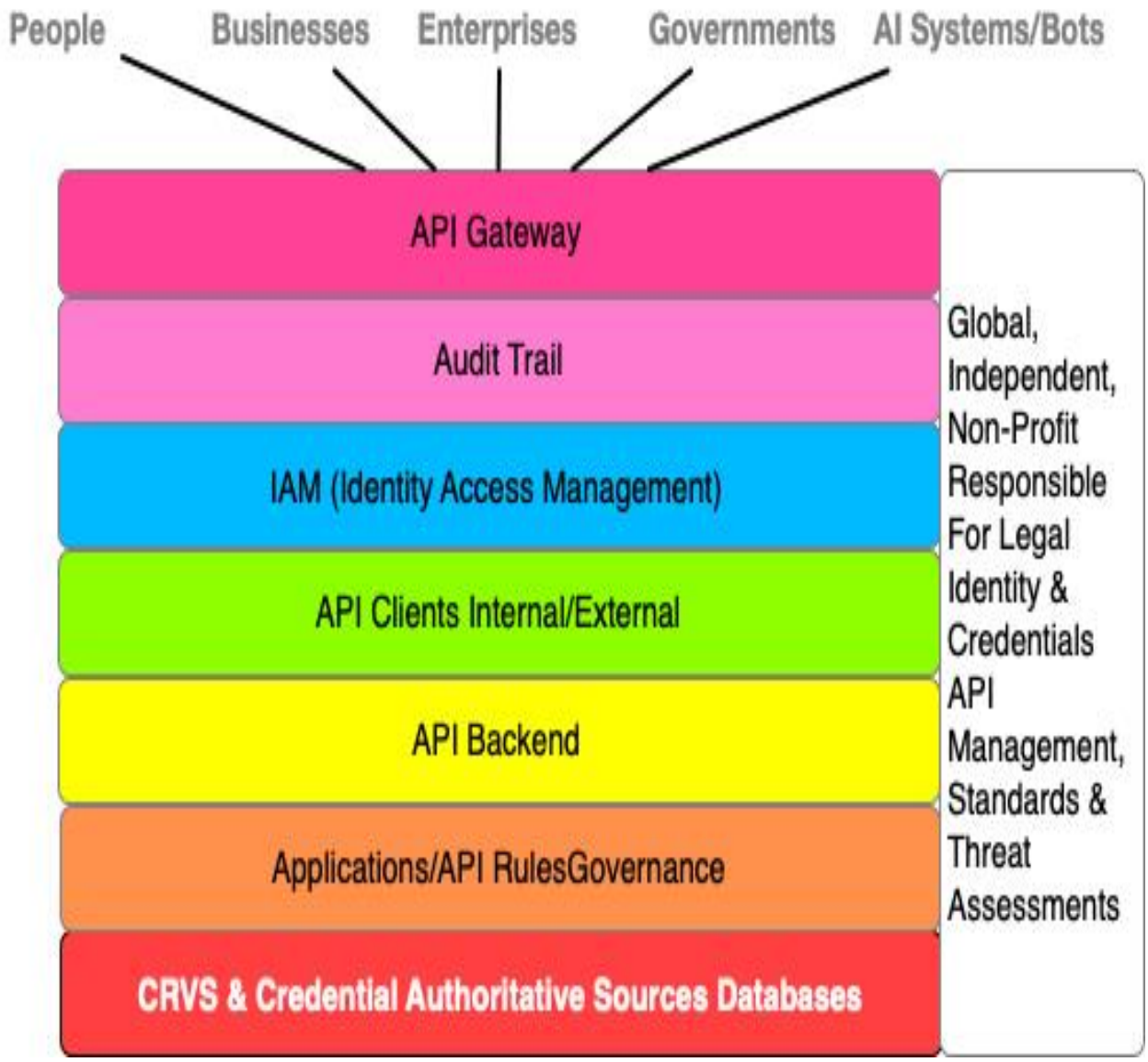
Answer - Create standard API's (Application Programming Interface).

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.

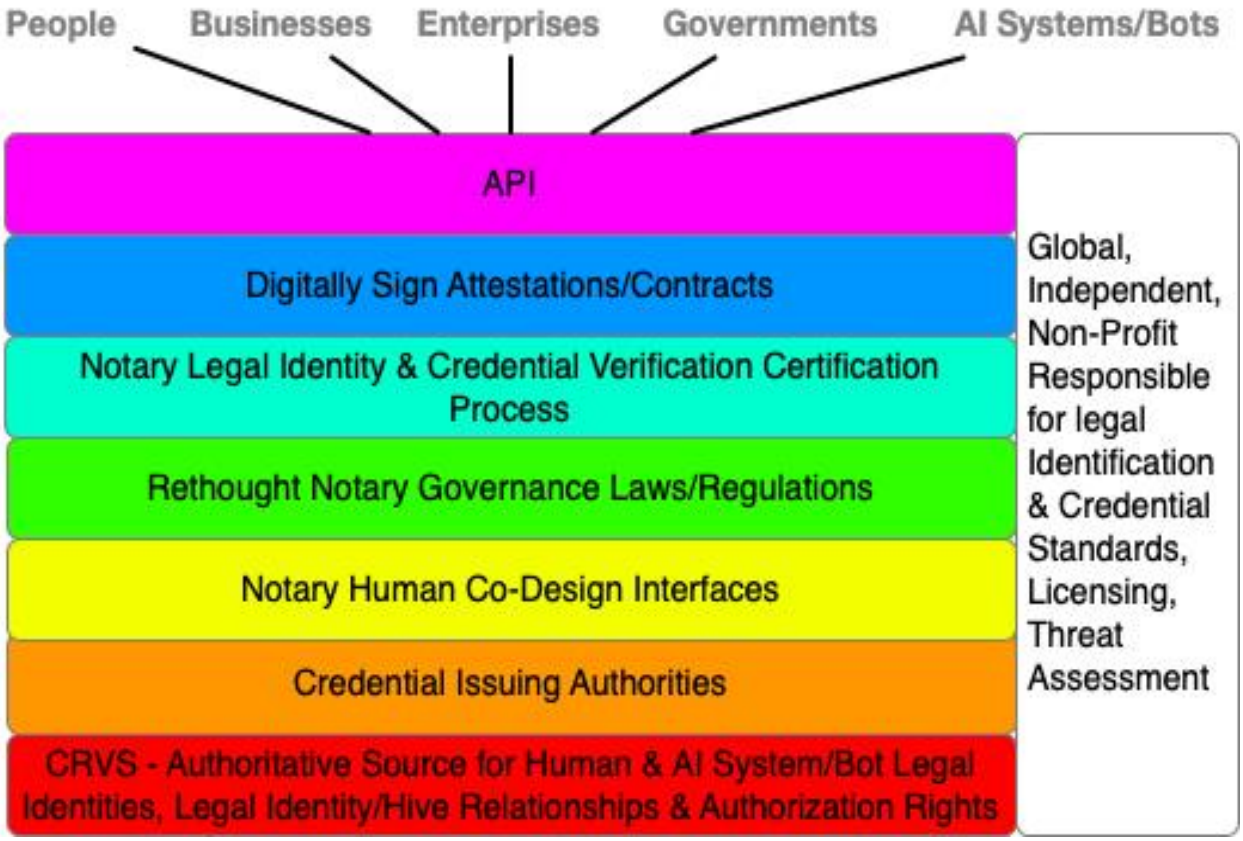
The place to start is by rethinking how they verify entities identities. In today's planet, this can be very challenging, since a person, their smart digital version of them, or an AI system or bot, might be interacting digitally with a local notary, from the other side of the planet.

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.

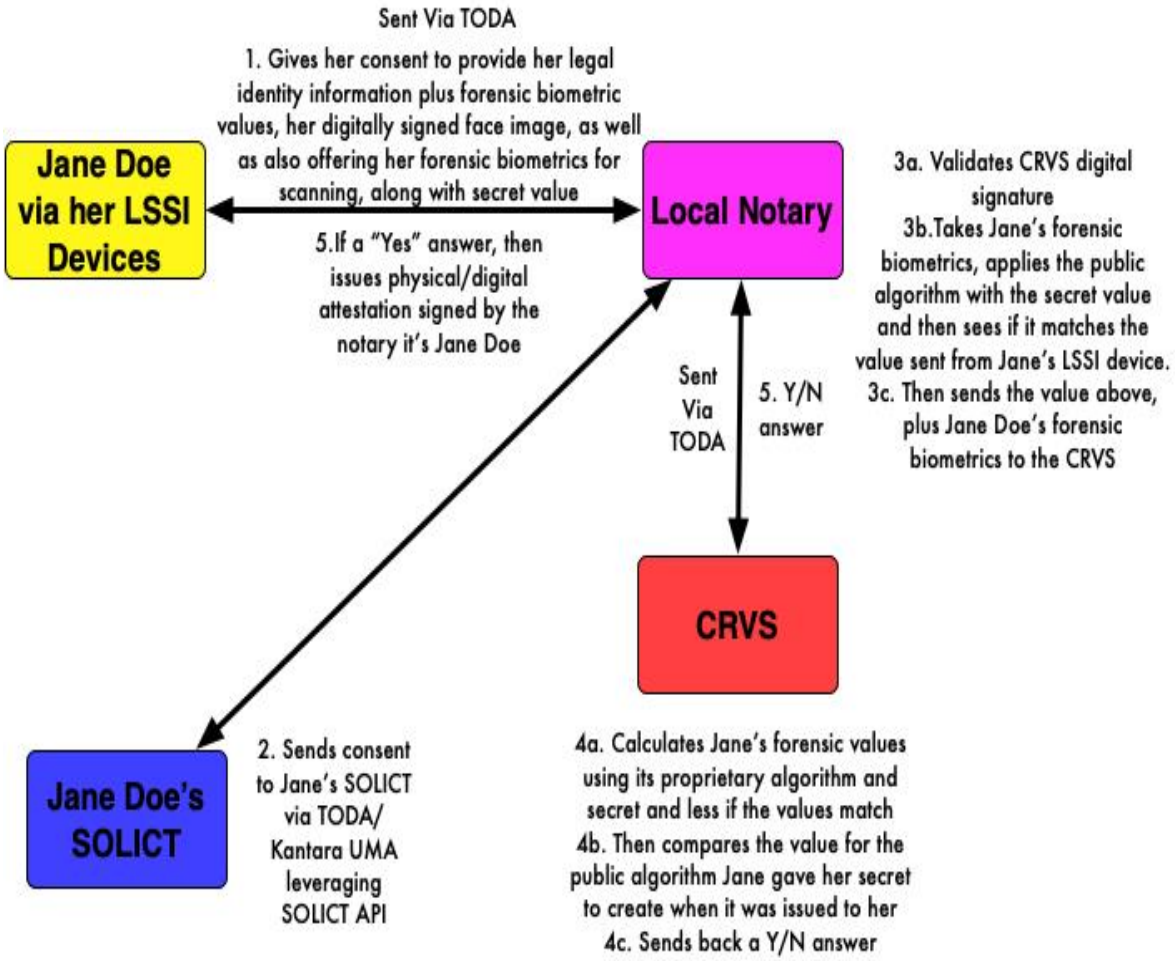
As with the rest of this architecture, it's visionary. I don't want to try to sell the planet on what a wonderful idea it is. Instead, my strategy is to find innovative country funders, with a willing business and notary community, to rethink notaries in small steps. That's what the cost centres call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

Rethought Notaries Cost Centre Reference Links:



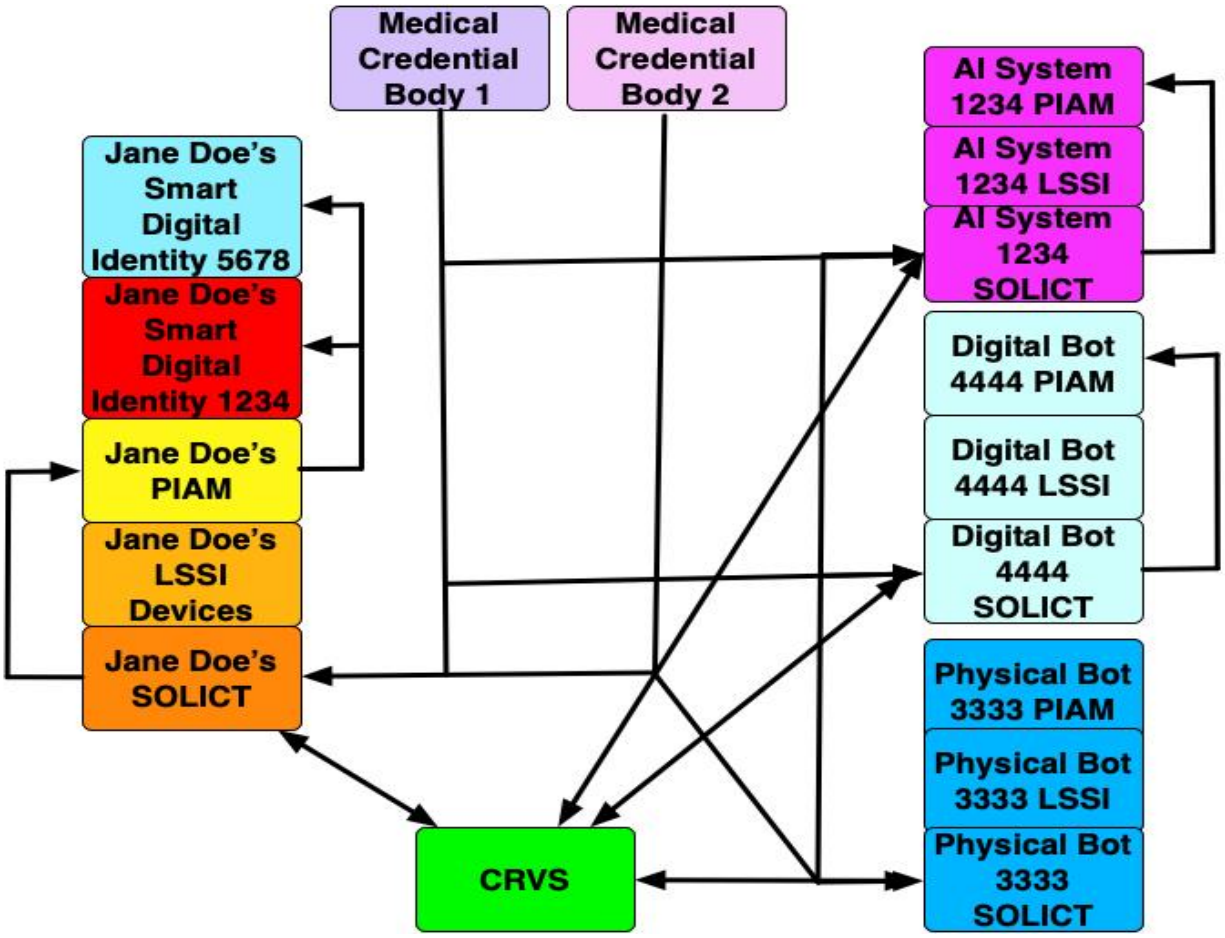
Read the section titled "**Cost Centre: Rethought Notaries**" in "**Cost Centres- Rethinking Legal Identity & Learning Vision**".

Example 1:


Sent Via TODA
1. Gives her consent to provide her legal identity information plus forensic biometric values, her digitally signed face image, as well as also offering her forensic biometrics for scanning, along with secret value
Jane Doe via her LSSI Devices
Local Notary
5.If a "Yes" answer, then issues physical/digital attestation signed by the notary it's Jane Doe
3a. Validates CRVS digital signature
3b.Takes Jane's forensic biometrics, applies the public algorithm with the secret value and then sees if it matches the value sent from Jane's LSSI device.
3c. Then sends the value above, plus Jane Doe's forensic biometrics to the CRVS
Sent Via TODA
5. Y/N answer
CRVS
Jane Doe's SOLICT
2. Sends consent to Jane's SOLICT via TODA/ Kantara UMA leveraging SOLICT API
4a. Calculates Jane's forensic values using its proprietary algorithm and secret and less if the values match
4b. Then compares the value for the public algorithm Jane gave her secret to create when it was issued to her
4c. Sends back a Y/N answer

Example 2

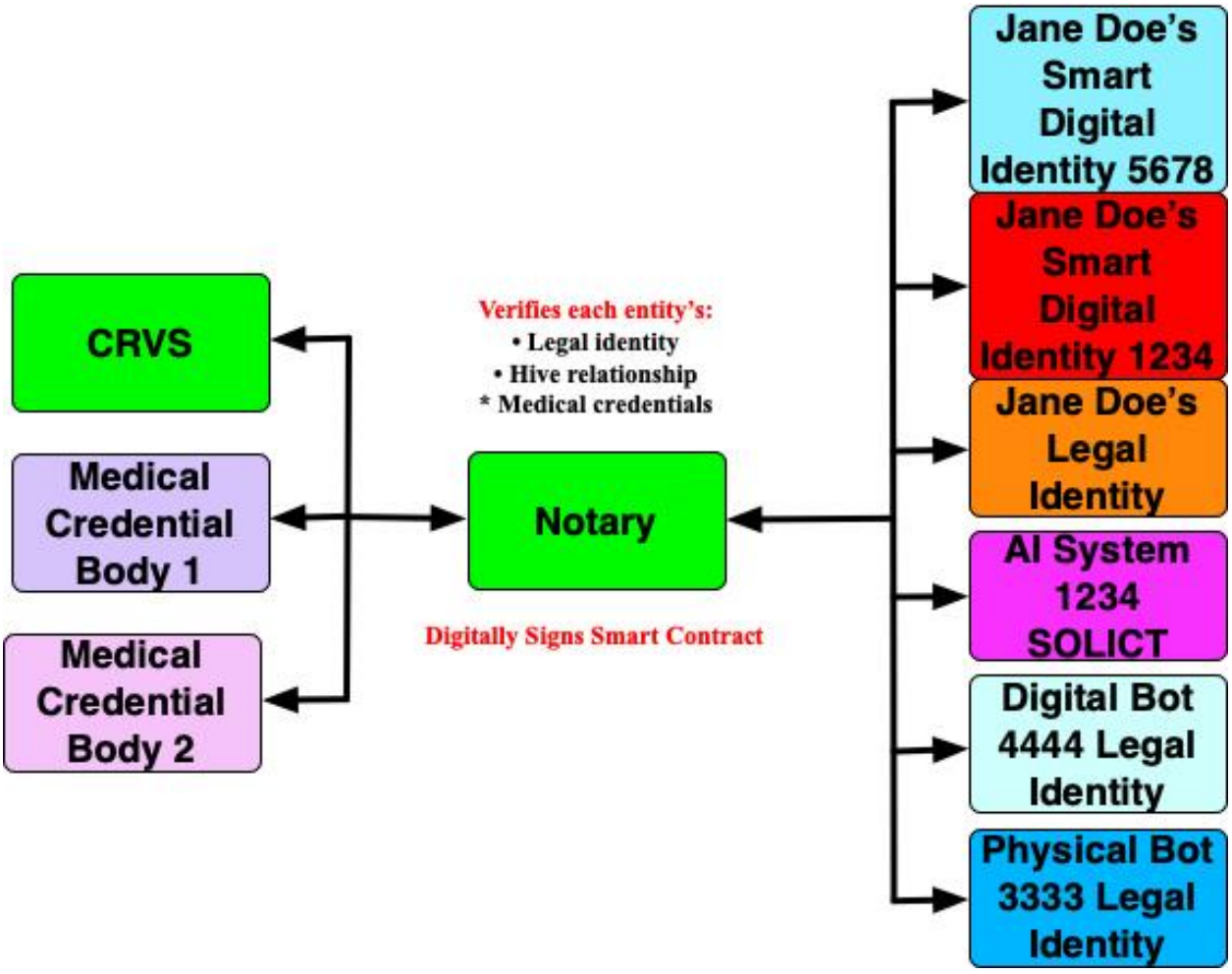
Let's say a legal identity hive is part of Acme Health Inc. which Jane wants to enter into a contract with, requiring identity verification of the entities, via a smart, AI leveraged contract. The two parties might be required to have a notary verify not only the legal identities above, but also their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



AI System/Bots, 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

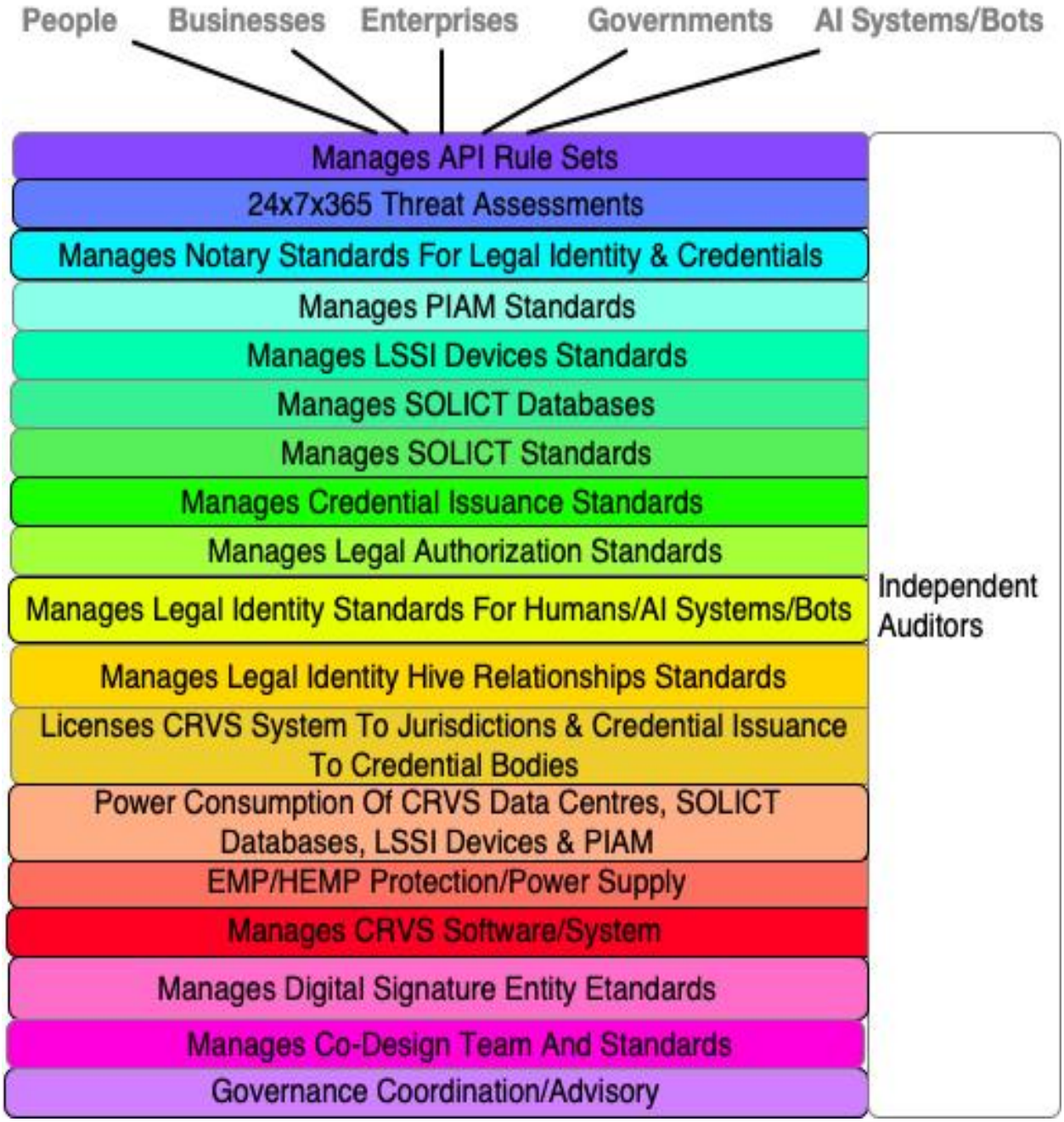
The non-profit will exist in 3 different physical locations, 8 time zones apart. It begs the question, who'll pay for it?

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.

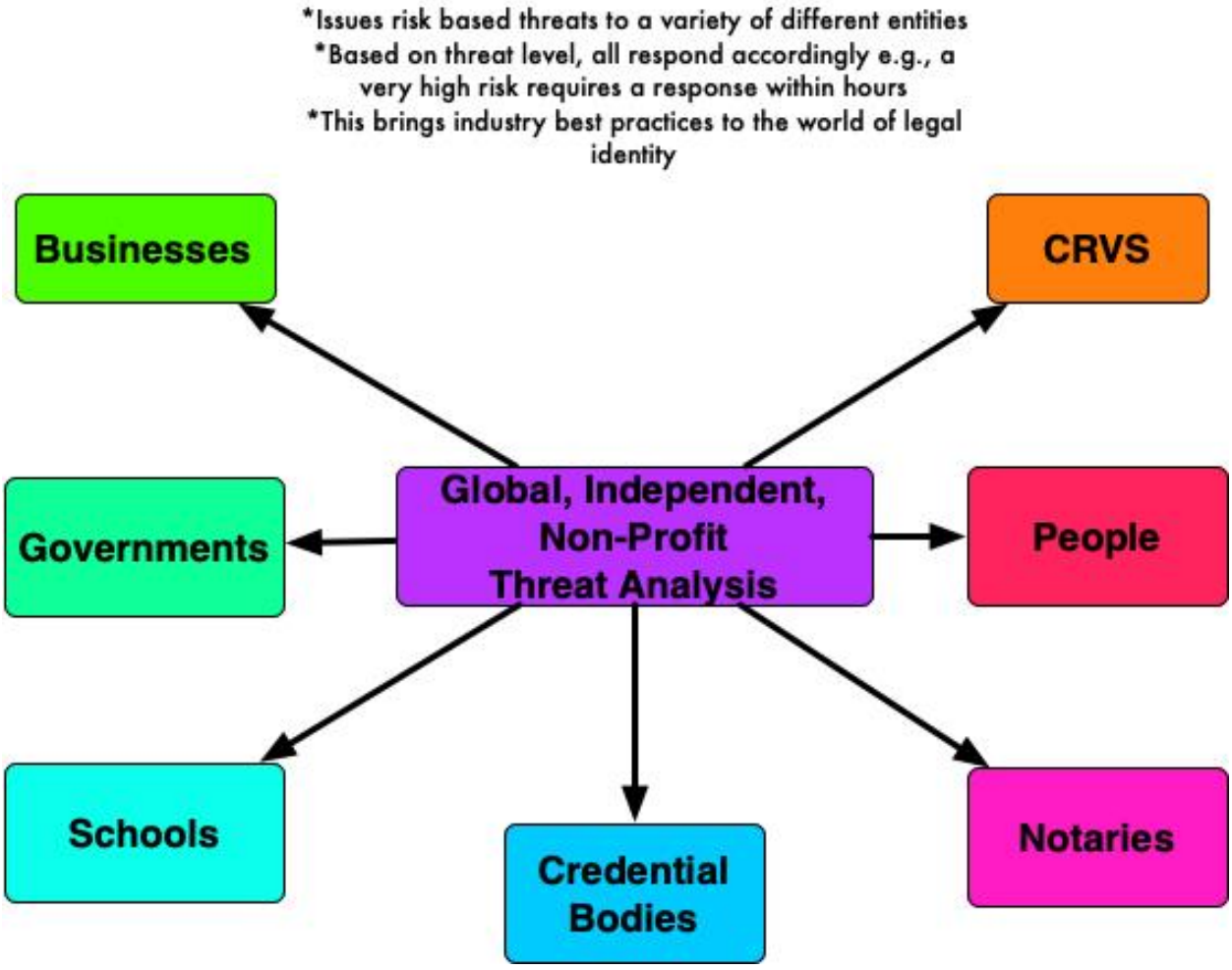
Global, Independent, Non-Profit Cost Centres Diagram:



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

AI systems and bots 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
- Address the rapidly emerging smart digital identities of humans
- Must address the rapid rate of change caused by this curve
- Give each entity control over their legal identities
- Create new legal toolkits to easily prove entity 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 entity 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, 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 out of the box, innovative funding countries and an equally innovative AI system, bot and IT industry.

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.