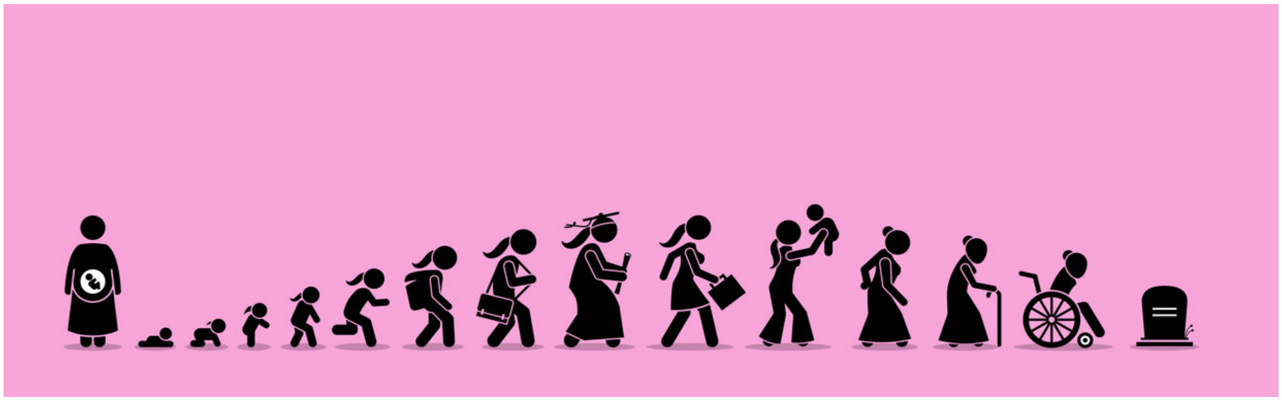
Implementing a Physical/Digital LSSI (Legal Self-Sovereign Identity) - How Much Will It Cost?



Author: Guy, Huntington, President, Huntington Ventures Ltd.

Date: March 25, 2021

Note

Readers of this document should first skim these two posts to understand the current business and security problems from having a crappy physical and digital legal identity system on the planet today, as well as to see an architectural vision for addressing this:

- “Digital Transformation Requires Change to Our Old Ways of Doing Things” - https://www.linkedin.com/pulse/digital-transformation-requires-change-our-old-ways-doing-huntington?trk=portfolio_article-card_title
- "Digital Transformation Vision - Legal Identity, Data & Consent” - https://www.linkedin.com/pulse/digital-transformation-vision-legal-identity-data-guy-huntington?trk=portfolio_article-card_title

The skim the following two-page executive summaries about LSSI:

- "LSSI Executive Summary" - https://hvl.net/pdf/LSSIExecSummaryMar92021GH.pdf
- “Quickly Rethinking CRVS Systems – Executive Summary” - https://hvl.net/pdf/RethinkingCRVSExecutiveSummaryMar132021GH.pdf
- Rethinking Biometric Identification Executive Summary" - https://hvl.net/pdf/RethinkingBiometricIdentificationMar92021GH2PageSummary.pdf
- "AI Systems/Bots Executive Summary" - https://hvl.net/pdf/AISystemsBotsLegalIdentitiesExecSummaryMar92021GH.pdf
- "Commercial LSSI Executive Summary" - https://hvl.net/pdf/CommercialLSSISummaryMar92021GH.pdf

The document repeatedly refers to this paper, “Secure, Network Based, Legal Self-Sovereign Identity (LSSI) - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf which readers should skim. It also repeatedly refers to this diagram which is worth viewing before reading this document - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf.

Within scope of this document is the ability, where risk warrants it, to register smart digital identities of humans, attaching it to the underlying physical legal identity. Out of scope, is the ability to legally register AI systems and bot legal identities. Also, out of scope for this document is development of a commercial version of LSSI.

Funders might want to scan this executive summary proposing rapid development, within two months, of a demo lab and video, using today’s technology, showing people how an LSSI system works (https://hvl.net/pdf/LSSIDemoLabExecSummaryMar182021GH.pdf) along with a cost estimate (https://hvl.net/pdf/LSSIDemoLabProjectedCostEstimates.pdf).

Finally, as background reading, viewers might want to read, Human Migration, Physical & Digital Legal Identity” - https://hvl.net/pdf/HumanMigrationPhysicalDigitalLegalIdentityMar2020.pdf.

Table of Contents

Executive Summary

Legal identity is VERY political, and is what this paper calls a "complex, "higgledy-piggledy identity mess". Other papers and posts I've written show the future madly coming at us, including smart digital entities of us, human cloning, along with the rate of technological change rapidly creating new attack vectors each hour. This is something not on most people's identity radar screens.

Then there's poor people around the planet, many of which don't have a legal identity and/or access to technology, with no ability to partake in the digital revolution we're living in. They're the first to feel the effects of global warming, being forced to migrate, often across numerous borders, without legal identity documentation. Up to 50% of these are children. How can they prove their legal identity?

As a very old, experienced identity architect, I've spent the last five years thinking, writing and searching for new pieces with which to rethink human legal identity, both physically and digitally around the planet, addressing the above. I was looking for an architecture, which allowed a local jurisdiction to still keep control of their legal identity processes, but be able to export it to a global standard, both physically and digitally. I also wanted to be able to tie the legal identity, biometrically to the person, GIVING THEM CONTROL OVER THEIR BIOMETRICS AND THEIR LEGAL IDENTITY INFORMATION.

The papers and posts referenced in the introduction show I now have a functional architecture, which works, using today's technology. This leads to the next obvious question, "How much will it cost to implement this?" That's what this paper addresses.

I wanted to think my way through this as a major funder, country leader, program manager and architect. I've created what I call in my head "Version 1.0 of a funding and implementation playbook". The "playbook' describes not only the costs of each cost centre, but perhaps more importantly, how to steer this through the myriad of political challenges of jurisdictions, special interest groups, etc.

The costs will likely be too large for one funder to fund it on their own. Thus, throughout the document, I lay out the components, which perhaps a funder can choose which ones to fund.

This is a transformational program. It affects the very poor, kids, parents, and all types of people, in their daily lives. It gives them new tools with which to not only prove their legal identity, but also such things as Covid vaccinations, education credentials, etc. It will transform businesses and different levels of governments around the planet.

I'm not only looking for funders with your money. What I really want is to find partners who can bring 1-3 jurisdictions to the table, where we can quietly pilot out the components, learning what works, and more importantly, what doesn't work. Then adjust and design the systems to be rapidly scalable, maintainable and sustainable, long term, in the face of rapid change.

Introduction

Legal Self-Sovereign Identity "LSSI" has many different "parts" with different political, governance, business process, technical and end user requirements. Many of which exist today, others where the technology exists but needs to be assembled to do the tasks, and still others where the technology "might" exist but needs to be proven.

Further, telling someone the cost will be "X" isn't easy, because the first one to three jurisdictions will bear the brunt of the initial costs, with subsequent ones at a far lower cost, i.e. "Y". Finally, as I've written, defending legal identity systems, against rapidly changing technology opening up new attack vectors, is becoming increasingly complex. Thus, there's the annual global cost to create and maintain a threat analysis system which might be "Z". How it's prorated to jurisdictions needs to be determined.

I'm a very experienced architect, program and project manager, who likes to bear down on variables, determining exactly what the outcomes and costs will be. Thus, this paper:

- Identifies the major cost centres
- Discusses what's possible today, using existing technology, business processes et al
- Estimates costs for these or, laying out steps needed to be taken to determine them
- Discusses how economies of scale can be achieved
- Outlines cost areas where the technology either doesn't exist yet, or must be proven to be applicable out in the field
- Discusses the overall governance model for LSSI and then determine costs for it
- Gives my thoughts on pro-rating maintenance costs to jurisdictions

I don't think one funder can bear the total costs, i.e. it will be too large. However, portions of it are likely very applicable to different types of funders. Thus, this paper will give all potential funders a bird's eye view of the lay of the LSSI land as it applies to costs.

As mentioned in the executive summary, in my head I call it, "Version 1.0 of a funding and implementation playbook". It not only addresses the costs, but proposes initial strategies for successfully addressing the complex political world LSSI is entering.

Major Cost Centres

Here are the major cost centres:

- **Rethought CRVS (Civil Registration Vital Statistics) system including:**
    - Actual CRVS system
    - Registration/identity verification costs for each person experiencing a CRVS event
    - System maintenance/defence costs
        - Local costs plus
        - Pro-rated costs from the global, non-profit
    - System governance costs coordinating laws/regulations across multiple jurisdictions
    - Create standards for major CRVS events including birth, name/gender change, marriage, divorce and death for urban and field settings
- **LSSI (Legal Self-Sovereign Identity) including:**
    - Creating and maintaining standards for this, as well as interfacing with standards like Kantara User Managed Access (UMA)
    - This extends beyond legal name, to include things like standards for vaccinations, education credentials, etc.
    - API standards for the LSSI
- **Rethought jurisdiction legal identity cards and digital application**
    - All the population within a jurisdiction should have one, i.e. cradle to grave
    - Costs associated with changes due to standards and/or threats
- **PIAM (Personal Identity Access Management) system**
    - Creating and maintaining standards for this
- **Global, Independent, Non-profit including:**
    - Standards setting and/or coordination with other standard bodies which are responsible for pieces of an LSSI, e.g. education credentials, vaccinations, Kantara UMA, etc.
    - 24x7x365 threat analysis against the governance, business processes, technological infrastructure and people users of the LSSI system
- **Global Notary including:**
    - Secure, protected storage of peoples' LSSI
    - Secure access by local notaries only able to do singular searches and not be able to troll the database

Rethought CRVS (Civil Registration Vital Statistics) System

Note: Readers should first review the following two documents before reading on:

- "Quickly Rethinking CRVS Systems – Executive Summary" - https://hvl.net/pdf/RethinkingCRVSExecutiveSummaryMar132021GH.pdf
- "Secure, Network Based, Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf

Desired End State:

Today's technology:

- CRVS operating to new global data standards
- CRVS able to securely store forensic biometrics
  - Fingerprints
  - Iris
  - Possibly face – used for legal anonymous identification
  - Other biometrics for when a person does not have fingers or eyes
- CRVS able to store agreed upon vital statistics
- Ability for the CRVS to be queried with consent by other CRVS systems around the planet, i.e.
  - A one to many search
  - A one to one search
- Ability for the CRVS to digitally sign legal identity attestations with the ability to write these to the following three types of end points as the authoritative legal source:
  - A person's LSSI physical Toda file
  - A person's LSSI Toda digital file
  - The person's global notary LSSI file
- **VERY strong security within the CRVS**:
  - Note: With LSSI, the CRVS becomes a lucrative high attack target for criminals. As stated on page 29 of this paper https://hvl.net/pdf/Where%20Shit%20Happens%20March%202019.pdf "As the new age civil registration system comes into being, it will make it much harder to pose as another identity. Thus, the need for people who want to act as another will increasingly rise, as will the price to be paid for this. People, criminals and malicious nation states will become more motivated to find ways to "crack the system"."
  - No biometric ever leaves the system

  - End to End CRVS Security Standards:
    - Standards need to be developed for end to end CRVS security
    - These will likely rapidly change over time due to the effects of this curve - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf. End to end security, e.g. digital signature/encryption of data/query in transit, DMZ endpoints, DMZ security, load balancer security, enterprise endpoints, network security, app server security, data base security, admin security, etc.
    - Strong, multifactor authentication requirements for administrators doing sensitive tasks on the CRVS system
    - Excellent archiving and storage of any administrative actions on the CRVS
    - Strong physical security on data centre locations hosting CRVS servers, firewalls, load balancers, etc.
    - Continual threat assessments against local CRVS systems 24x7x365 by red teams
    - Security standards for CRVS event entering by registrars working off-site
      - Ability to standardize biometric and legal identity data collection and transmission
        - E.g. as per pages 25-27 of this paper https://hvl.net/pdf/Where%20Shit%20Happens%20March%202019.pdf
      - Ability to prevent misuse of the CRVS system by corrupt administrators or, by malicious people holding guns to the head of registrars out in the field
        - E.g. as per pages 29-30 of this paper https://hvl.net/pdf/Where%20Shit%20Happens%20March%202019.pdf

- Ability for a CRVS system to register smart digital legal identities of people, attaching them to the underlying physical legal identity

- Creating standardized legal, business and technical processes for CRVS events including birth, name/gender change, marriage, divorce, and death for both urban and field settings:
    - Birth:
        - Establish standardized procedures for obtaining infant fingerprints at birth along with obtaining their legal identity information which work not only in urban settings but also out in the field
    - Death
        - Revising existing legal death confirmation procedures by amending existing processes if the deceased has forensic biometrics available, which can then be searched at all CRVS's around the planet to confirm the legal identity
        - Developing standard business and technical processes for death notification including but not limited to:
            - Automatic notification to registered entities which the deceased, prior to their death, provided their consent for their death notice to be automatically sent via the CRVS to the registered entities, e.g. banks, tax agencies, etc.
            - Standard Toda LSSI interfaces to death notification services which the deceased may or may not choose to use
            - Creating the ability for an executor of an estate to legally manage the deceased's legal identity until the deceased estate is wound up
            - Determining what legal and business processes to use in terminating registered smart digital entities of the deceased person
        - Much of the above is depicted on page 13 of the paper, "Secure, Network Based, Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf
    - Other CRVS events:
        - Develop standardized legal and business processes for confirming an identity and their CRVS status, before executing the CRVS event
            - Example Marriage– confirm an identity by obtaining, with the person's consent, their legal identity information plus their forensic biometrics and search all CRVS systems around the planet to determine the person isn't married, before proceeding with the marriage registration
    - Exceptions:
        - People will be born with no fingers or eyes or, during their life might lose these
        - Thus, standardized technical, business and legal processes must be developed to legally identify these people

- CRVS Availability
  - Ability to ensure the CRVS systems is available at a minimum availability of 99.999%
  - Ensure events like a GMD/HEMP won't adversely affect the CRVS data
    - E.g. this paper "When Our Legal Identity Trust Goes Poof!" - https://hvl.net/pdf/When%20our%20legal%20identity%20trust%20goes%20poof%20Jan%202019.pdf
    - E.g. pages 24-25 of this paper https://hvl.net/pdf/Where%20Shit%20Happens%20March%202019.pdf
- Ability to record consents for each CRVS search as well as to archive them in a secure data repository
- Ability to store CRVS events for a person, long after they and their legal digital entities have died and/or been terminated in a secure data repository
- Ability for the CRVS system to feed other jurisdiction's identity applications, e.g. national population registries, health systems, driver's licenses, etc.

CRVS Technology Needing to be Developed and/or Confirmed:

Biometrics:

Biometric Standards for Infant Fingerprints:

- Good news the technology now exists and has been piloted
- 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

Biometric Standards for Legally Determining Physical Identity of a Deceased Person

- Develop 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

Anonymous Biometric Identifiers:

- (as per Rub Bolle's paper - https://hvl.net/pdf/BolleAnonymousBiometricIdentifiersRevisited2015.pdf)
- Research and testing needs to be funded determining if this is viable out in the field
- Refer to this executive summary - https://hvl.net/pdf/RethinkingBiometricIdentificationMar92021GH2PageSummary.pdf

Storage of A Randomized Digital Biometric Rather Than the Actual Biometric:

- Research and testing needs to be funded determining if this is viable out in the field
- Refer to this executive summary - https://hvl.net/pdf/RethinkingBiometricIdentificationMar92021GH2PageSummary.pdf

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

- Standards need to be agreed upon for the way fingerprints and iris are obtained out in the field such that they're reproducible as well as secure
- Standards need to be agreed upon for obtaining of the same biometrics in urban locations such that they're reproducible as well as secure

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

- Research out in the field 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.

Automation of Forensic Biometric Collection:

- Research needs to be done examining ways to automate collection of forensic biometrics to lower costs and increase verification accuracy/reproducibility of them

Research Confirming Fingerprints/Iris Are Enough to Legally Differentiate Human Clones

- Research needs to occur such that CRVS registration procedures using fingerprints and iris to differentiate identical DNA clones of Jane Doe 1,2,3,4,5 etc. will stand up in a court of law

Off-the-Wall Idea for Creating A Wearable Toda LSSI Bracelet Biometrically Tied to the User from Infant to Old People

- Toufi Saliba, global chair IEEE AI standards and I believe the technology now exists to create a wearable Toda LSSI wristband biometrically tied to the user, from infants to old people
- Skim this for more information - https://hvl.net/pdf/OffTheWallExecSummaryMar222021GH.pdf

Smart Digital Identities

- Standards need to be developed for registering a smart digital identity within its code and then cross-linking it, not only within the CRVS system to the underlying physical identity, BUT ALSO cross-linking the digital identities LSSI Toda file to the physical person's LSSI Toda files

GMD/HEMP Event Protection Standards:

- Standards need to be developed for CRVS GMD/nuclear event protection
- Readers should skim this paper "When Our Legal Identity Trust Goes "Poof!" - https://hvl.net/pdf/When%20our%20legal%20identity%20trust%20goes%20poof%20Jan%202019.pdf
- Thus, as we digitize our legal identity, it becomes imperative the data centres storing the records will survive both a GMD or HEMP event

CRVS Data Conversion:

- Research needs to be rapidly done on converting paper, old electronic format data to the new digital standard
- I can see both physical and virtual bots being used to do this
- It needs to rapidly be POC (proof of concept), mistakes learnt, retested, piloted and then designed to rapidly scale, cost effectively

Estimated CRVS Costs

CRVS System

Option 1: Leverage OpenCRVS

Plan International has already built an OpenCRVS system, which is currently deployed in Zambia and Bangladesh (https://www.opencrvs.org/). 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 show-stopper, 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 LSSI data from the Toda file
        - Their systems today, 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 show-stopper if business communities in particular aren't willing to support the Toda LSSI file standards
    - Thus, my suggested approach would be to:
        - First determine what each jurisdiction around the planet's CRVS data standards are today
        - Then stand back and consider the end game we're driving at, i.e. wide spread quick global adoption of a Toda LSSI file
        - Then create a strategy which delivers the goods so to speak
        - This might or might not include:
            - Adopting HL7
            - Creating a new standard
            - Creating free adaptor type programs which can rapidly convert the LSSI Toda file standard to a different format
            - Etc.
        - Then sit down with Plan International to discuss
            - All of the above will likely impact costs

- End to end security
    - As the prior sections stated, 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
- Physical identity cards and 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 (UI)
    - They also print physical birth certificates
        - I'm not sure if they'll be amenable to altering this to a 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 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 agreed 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 of 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, nor do I know, yet, how to estimate the roll-out costs
- Modify Open CRVS to accept smart digital identities
    - See "Costs for CRVS Technology Needing to be Developed and/or Confirmed" section below
- **Bottom Line**:
    - **I REALLY like what Plan International has done with OpenCRVS**
    - Assuming significant funding with political connections to rapidly bring several jurisdictions to deploy CRVS systems comes into play, I feel we can find a way to work with them
    - The initial costs will be calculated using today's existing technology and not include doing automated legacy data conversion, anonymous biometrics, etc.
        - i.e. The program and individual projects must crawl before walking and running
        - See next section for additional costings for projects which can be run in parallel to the crawling stage
    - How much will it cost?
        - TBD for development costs
        - Roll out costs are another cost centre, which can be developed, assuming Plan International agrees

Option 2: Create a New CRVS System

This option should only be explored, based on the results of the discussions with Plan International and OpenCRVS. The costs will likely be much higher, as well as longer timelines to deploy

Costs for CRVS Technology Needing to be Developed and/or Confirmed:

Biometrics:

Biometric Standards for Infant Fingerprints:

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

- Discuss with Dr. Anil Jain and UCSD's KidPrint the deliverables required
- For each one estimate type of resources required, timelines and costs

Biometric Standards for Legally Determining Physical Identity of a Deceased Person

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

- Create a team composed of the following:
  - Forensic pathologists
  - Biometric experts
  - Field experts handling death registrations in the field
  - Legal experts
  - Business process experts
- Determine the efficacy of using fingerprints and iris scan post death to determine the legal identity of the person
- Based on the above, create modified death process standards and business processes for determining the legal identity
- 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
- For each of the above, estimate type of resources required, timelines, deliverables and costs

Anonymous Biometric Identifiers:

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

- 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

Storage of A Randomized Digital Biometric Rather Than the Actual Biometric:

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

- 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

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

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

- 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

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

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

- Review with leading biometric research experts to get their perspective on existing research, areas where possible additional research is required, etc.
- Then create deliverables, resources, costs and timeline estimates to do the research/testing

Automation of Forensic Biometric Collection:

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

- Discuss with the academic and biometric industry communities the potential requirements
- Then create deliverables, resources, costs and timeline estimates to do the research/testing

Research Confirming Fingerprints/Iris Are Enough to Legally Differentiate Human Clones

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

- Do a research literature search to determine what research has been done to date on differentiating clones
- Then discuss with the research community potential requirements to address any gaps
- Then create deliverables, resources, costs and timeline estimates to do the research/testing

Off-the-Wall Idea for Creating A Wearable Toda LSSI Bracelet Biometrically Tied to the User from Infant to Old People

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

- Create a high-level requirements document outlining potential deliverables
- Do a research search through existing academic literature looking for potential technologies
- Assemble a group of researchers in this field to provide comments, criticisms, insight etc.
- Determine deliverables, potential resource requirements, timelines and costs
- Fund development to see if it can be done

Smart Digital Identities

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

- Assemble a team to determine the following:
    - How the AI smart digital entity of a person could have its code altered to show the digital legal identity, such that it can't be copied, edited, deleted or misused
    - Determine what type of Toda LSSI file to create for the smart digital legal identity
    - Determine how to cross-reference the smart digital legal identity with the physical legal identity of the person
    - Determine business processes for being able to do the following:
        - Check to see if the digital entity is already registered
        - Assuming it's not, determine business processes to register the identity
        - Determine what happens to the underlying digital legal identity when the physical person dies
    - Determine legal laws and regulation changes required
    - Determine standards to be created for registering a smart digital legal identity of a person
    - Assemble a red team to attack the technology, governance and business processes associated with the above
    - Do POC's to determine how to make it work
- Pilot all the above in 1-3 jurisdictions, and once successful rapidly scale
- For all the above, determine deliverables, potential resource requirements, timelines and costs

GMD/HEMP Protection Standards:

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

- Contract GMD/HEMP experts to come up with recommended standards for protecting data centres housing CRVS data, with a cost estimate calculator based on different conditions of existing data centres housing CRVS data
- Find funding to do 1-3 jurisdictional data centre conversions
- Do a lesson learnt from the above, refine the process, and then determine an accurate cost estimate for each jurisdiction wanting to adopt the Toda LSSI model
- Find funding for each jurisdiction as they join

CRVS Data Conversion:

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

- Determine high-level requirements - I suggest the following for consideration:
    - 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, to a high degree of accuracy, at a low cost
- Assemble a group of experts in:
    - Document conversion leveraging AI and machine learning
    - Robotics – both physical and virtual
    - Researchers in the above fields
- Ask them to propose 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
    - Find funders to fund the above

Estimated LSSI Costs

Background

Existing Credential Standards

As the diagram on page 9 of “Secure, Network Based Legal Self-Sovereign Identity (LSSI)” - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf indicates, there are other components to a person’s LSSI outside the scope of a CRVS system. This includes things like health records/vaccinations, education history/credentials, etc.

Existing Physical Legal Identification Cards

Today’s use of physical identity cards typically leverages physical driver’s licenses and/or jurisdiction identity cards. These typically show the person’s name, address, age etc.

However, I have an underlying premise – the physical legal identity cards shouldn’t reveal on the surface much about the legal identity of the person. Instead, without consent of the user, they should only reveal the holder is a human, and possibly only display their face. The cards may or may not be set up to reveal if the person is above or below age of consent. The rest of the legal identity information should only be released with the consent of the user. This is privacy by design.

As an example, if a person wants to prove they are of age of consent to enter say a bar, they would present their card, tap it against an NFC reader, and give their consent for their age of consent to be confirmed. The card would transfer the face image from the card, plus a digitally signed attestation by the local authorities the person is of age of consent. The bar might or might not make a quick electronic trip to confirm the digital signature, then match the face presented from the card to the one of the person holding the card. Assuming they match, and the person is of age of consent, they’d be granted entry to the bar, without having to reveal any more legal identity information about themselves.

In the future, assuming the off the wall idea works for a biometric Toda LSSI bracelet, the person would simply tap their bracelet against the NFC reader. In the future, it’s also hypothetically possible for a physical chip within the person to broadcast out, with consent of the person, the age of consent information plus a digitally signed image of the person by the local authorities. Over time, not overnight, coupled with digital Toda LSSI apps, I see the beginning of the end of the use of physical identity cards.

Further, legal identity cards must begin at birth. In many jurisdictions around the planet, this will be a change, resulting in increased deployment cards.

Existing Digital Legal Identity Applications

There's not yet a uniform global standard for digital identities, there are different models used (e.g. federated identity) and where standards do exist for some forms of digital identities (e.g. digital driver's licenses – e.g. ISO/IEC 18013-1-3) which not all jurisdictions adhere to it. Further, digital identity is frequently viewed from a country perspective, i.e. it becomes silo-ized within the jurisdiction or between limited numbers of jurisdictions (e.g.EU e-ID - https://digital-strategy.ec.europa.eu/en/policies/e-identification). Finally, as noted in reasons to deploy a Toda LSSI, the underlying physical legal identity used to generate the digital identities is flawed.

Rapid Rate of Change

Then consider the rapid rate of change, i.e. https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf. It means that standards, governance, business processes, technological infrastructure and people, are under new attack vectors each hour. This is something that most designers of physical digital identity standards, deployments, etc. are unprepared for, still mostly using long-time horizons to respond.

THE PROBLEM IS THE OPPORTUNITY

This complex, "higgledy-piggledy identity mess" is the political world Toda LSSI's entering. So, yes, there are MANY different political reasons an LSSI program can fail**. However, the lack of a uniform global solution means the opportunity exists to carefully address it.**

Here are my thoughts on this:

- Start with the authoritative source for a human identity, e.g. the underlying CRVS, and rethink this as laid out in this and other documents
- Make it the source of truth for most, but not all of a jurisdiction's peoples. Why not all?
- Many people within a jurisdiction aren't from the jurisdiction
- Thus, until all jurisdictions around the planet adopt LSSI, it means traditional methods of doing legal identity verification will still have to be used
- This will result in identity fraud and identity collisions, i.e. where a "real identity", e.g. Jane Doe, discovers someone else is masquerading as her, e.g. Sally Smith
- Develop standardized business processes addressing identity collisions which can be replicated in different jurisdictions around the planet, until Toda LSSI becomes common
- Then use the LSSI Toda CRVS system as the source of truth for most, but not all, of a jurisdiction's other identity systems, e.g. education, health, tax, population registers, driver's licenses, passports, etc.
- For people not from the jurisdiction, a hybrid approach must be used, e.g. relying upon other identification methods as described above
- Standardize the jurisdiction's legal physical identity cards and digital legal identity applications onto one combined global standard – the underlying technology MUST INCLUDE the LSSI Toda file

- Then design integration between the physical/digital Toda LSSI with other systems like digital driver's licenses et al. The issuance of say a driver's license, be it physical and/or digital, should be reliant upon the underlying legal identity, which is what Toda LSSI brings to the party
- Where higher levels of identity assurance are required, e.g. passports, then it's hypothetically conceivable the applicant must give their consent, provide their legal identity information plus their forensic biometrics, which are then searched against CRVS systems planet wide, to confirm their identity
- **DON'T TRY AND TAKE ON THE PLANET WITH THEIR EXISTING IDENTITY STANDARDS IN THE BEGINNING** – this will result in entering a quagmire of vested interests. In other words, build it to a new global standard, which others can then learn to integrate with
- I don't recommend existing standards bodies be used to manage the overall Toda LSSI standards. Why?
- The rate of change. Legal identity is much more than a standard, e.g. Toda LSSI standard. It's a set of laws/regulations, governance, business processes, technological infrastructure used and people using it. All are potential attack vectors, changing each hour. Most existing standards bodies weren't set up to address this, nor do they have the funds to do so
- Thus, I recommend creating the global, independent non-profit to do the continual threat assessments, as well as provide a global governance body
- **HOWEVER, it may very well be within LSSI portions of the data might be administered to standards set by other bodies - Thus, I'm NOT RECOMMENDING the global, non-profit take it all on, for it will politically fail**
- Where existing standards exist, are robust, and global, adopt them
  - For example, they should likely adopt existing global health standards for things like vaccinations
  - Global standards should likely be developed in other bodies for education credentials including secondary, post-secondary, etc. and then adopted into Toda LSSI
- Then design the system to feed other gov't systems such as driver's licenses, jurisdictional identity cards et al.
  - That's the design approach of OpenCRVS – e.g. the image towards the bottom of this page where the CRVS systems feeds the various government systems on the right (https://documentation.opencrvs.org/opencrvs-core/)
- Delegate some authority to the driver's license/jurisdictional identity issuing gov't body to be able to write to a person's LSSI Toda file for circumstances where the person's not from the jurisdiction and their originating source of truth for their CRVS is not using Toda LSSI
- I can see 1-3 jurisdictions being the lighthouse pilots
  - There must be a very large budget assigned to political navigation, where experts from existing standards bodies are contracted, and a political path through the potential quagmire plotted, where the strategy is tested out within the jurisdictions

Legal Identity & Credentials

As the diagram on page 9 of "Secure, Network Based Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf indicates, there are other components to a person's LSSI outside the scope of a CRVS system. This includes things like health records/vaccinations and education history/credentials, etc.

When implementing a LSSI system, the initial scope should be "tight", i.e. limit all the deliverables LSSI can deliver. My recommendation is to crawl, walk and then run, i.e.:

- Start off with legal identity
    - i.e. get the CRVS systems rethought with a physical and digital Toda LSSI a person can use in their day to day life
    - This must include adoption and integration of Kantara User Managed Access (UMA) - https://kantarainitiative.org/confluence/display/uma/Home
        - I don't know if UMA will have to modified or not to work with LSSI Toda
            - UMA experts need to be contracted, requirements determined, gap analysis determined, integration deliverable determined, resource requirements, timelines and costs determined
- In parallel to this, assemble teams to determine best global standards to use for:
    - Health:
        - Covid vaccinations
        - Vaccinations in general
        - Health records
    - Education:
        - K1-12 (primary/secondary) credentials
        - Post-secondary, technical school credentials
    - Professional credentials e.g.
        - Teachers
        - Doctors
        - Dentists
        - Accountants
        - Lawyers
        - Etc.
- Rate them on quick ease of adoption, i.e.
    - The global standard body MUST already exist, be globally recognized, has a solid data standard, and the ability to rapidly adjust as times change
    - Ability for the issuing authority to securely, digitally sign attestations
    - Ability for the issuing authority to issue them as a Toda file
- Then select the easiest ones to adopt
    - As the Toda LSSI is deployed, adding in new Toda files and standards isn't that complicated – see next point

- Develop a standardized process for integrating new LSSI features. This MUST include:
  - Governance processes, including notification processes to end users, Toda governance authorities, jurisdictions, issuing authorities etc.
  - Standardized business processes for managing not only the initial integration but changes required to either the existing Toda files, etc.
  - Standardized security standards for an end to end process of the relevant authority to the end user's Toda files
  - Emergency change processes when quick changes are required
- Develop cost models for all the above, i.e.
  - Determine time, deliverables, resource requirements, timelines and costs
  - Determine ongoing maintenance/governance costs
- POC, determine what didn't work, retest, pilot and then rapidly scale
- Finetune the integration model as the number of LSSI integrations grows
- Note: **Some of the above may come under the global, independent non-profit cost centre**

Toda API

Page 30, of "Secure, Network Based Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf, describes the Toda LSSI API (application programming interface). As the paper states, **"The API for the LSSI Toda file becomes the gateway to the Toda file components, and MUST BE VERY SECURE."**

There are three main cost centres associated with the Toda LSSI API:

- Governance and licensing agreements for use of the Toda LSSI API
- Design, initial creation and implementation of a secure Toda LSSI API
- Ongoing security assessment and changes to the Toda LSSI API

Governance and Licensing Agreements for use of the Toda LSSI API

This needs to be very carefully thought through because, over time, the importance of the API will become very large as billions of people, businesses and governments leverage the API interfaces daily. Here are my thoughts on how to approach and fund this:

- Do the governance of this from the global, independent non-profit
  - See the non-profit section in this document
- Create standards for the Toda LSSI API
  - See next section
- Create licensing agreements for the Toda LSSI API
  - See non-profit section of this document

Design, Initial Creation and Implementation of a Secure Toda LSSI API

- Keep the initial target of the API tightly focused
    - Start with the Toda legal identity information flowing from the CRVS and other authoritative sources to the Toda LSSI
    - Design it such that the API can manage the data inflows of not only the legal identity but also the consents leveraging Kantara UMA
- Start with a red team to constantly attack the initial API design
    - This is critical to the immediate and long-term success of Toda LSSI
- Create standards for the LSSI Toda API
- For all the above, determine requirements, deliverables, resource requirements, timelines and costs
- Much of this cost will likely be borne by the global, independent non-profit
    - See non-profit section of this document

Ongoing Security Assessment and Changes to the Toda LSSI API

- Create standardized business processes for changes to the Toda LSSI API
- Do 24x7x365 threat assessments against the API and, via the licensing agreements force licensed parties to update to various time frames based on the threat assessment risk levels
- For all the above, determine requirements, deliverables, resource requirements, timelines and costs
- Much of this cost will likely be borne by the global, independent non-profit
    - See non-profit section of this document

Estimated Costs of Rethought Legal Physical Identity Cards and Digital Application

Here is a recommended cost deployment strategy for 1-3 initial jurisdictions:

- Create a steering group regarding rethinking physical identity cards and digital legal apps
    - This should include local legal authorities, police agencies, and privacy groups
    - Develop use cases for use of the new rethought physical legal identity cards and digital apps
- Design a staged implementation strategy. This will likely include:
    - Leveraging existing cards, modifying them to accept a Toda LSSI file
        - Security standards for these MUST be developed
    - Possibly also leveraging existing legal digital applications
    - Create pilots using a rethought legal physical identity card and digital app
        - Test them out, find out what works, what doesn't work, redesign the cards/app, business processes et al, retest until it works as advertised
    - Then rapidly scale
- For the above, determine requirements, deliverables, resource requirements, timelines and costs
- My last point – rather than try to shove into a jurisdiction a completely rethought physical legal identity card/app, it's politically desirable to co-opt the local parties, work with them, and have them agree on design and implementation processes
- **Bottom line:**
    - The first few jurisdictions Toda LSSI is implemented in, the upfront costs may be contained at first by trying to leverage existing physical legal identity cards and/or digital app if technically feasible
    - There will likely be some significant costs, and longer timelines, in getting all the parties to agree to rethinking them
    - The next stage of costs will likely be larger, given the size of the population and cost per person to reissue new types of physical legal identity cards and digital app
    - Once a few jurisdictions have gone through the process, the implementation costs for subsequent jurisdictions will likely be relatively easily calculatable

Cost Centre – Researching Use of Toda LSSI Computer Chips Inserted into People

The speed of this curve, https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf, 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.

A funder should be found to work with academic researchers on the privacy, security and health issues associated with doing this. This should lead to tightly controlled POC (proof of concept) trials. A sophisticated red team should be involved in any testing, doing extensive attacking and potential hacking of the technology. From this effort, a scientific, security focussed, measured approach can be taken, either proving the technology will safely work or, deciding the time is not yet right.

For all the above, scope, requirements, deliverables, resource requirements, time lines and costs needs to be determined.

Estimated Costs for a PIAM (Personal Identity Access Management) System

Background:

In the paper, "Secure, Network Based, Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf, on pages 30-33, I describe the PIAM. It refers to an example of Jane Doe walking down the street, in the not so distant future wearing AI/AR glasses, with her LSSI, using the PIAM (https://www.linkedin.com/pulse/advertising-fraud-identity-future-guy-huntington?trk=portfolio_article-card_title). On slides 15-17 of this deck, https://hvl.net/pdf/DigitalBankingIdentityDeckMar92021.pdf, I describe how PIAM will be the key to becoming close to the customer. Finally, in the image used for this post, https://www.linkedin.com/pulse/digital-transformation-vision-legal-identity-data-guy-huntington?trk=portfolio_article-card_title, I have the PIAM as a critical piece directly above the LSSI, enabling on top of it, rethought consent, citizen vaults for their data repositories, which companies and governments can then interact with.

Does it exist today? No. Thus, establishing standards for it, early on in the development of LSSI, is critical to ensuring the playing field is level for different companies and enterprises to leverage it. More importantly, it also must give the customer control over their legal identity.

Finally, there is this rate of change curve to keep in mind when developing PIAM standards - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf. Especially with respect to AI, I feel the use of the PIAM will explode over a relatively short period of time. Thus, any standard created MUST BE BUILT TO QUICKLY CHANGE, as well as make changes to security of the PIAM.

Estimated Costs:

Here is a recommended cost deployment strategy for 1-3 initial jurisdictions:

- Create a sub-committee of the proposed global, non-profit which is just devoted to developing the initial PIAM standard
- Hire very skilled contractors/employees who have the following skill sets:
  - Legal
    - Especially with identity federation experience, new legal tech with respect to AI contracts and also bots
  - Business Processes
    - Some very experienced business process analysts will be required to work their way through documenting the user to business/enterprise/government experience the PIAM will likely manage
  - UI/UX
    - The interfaces will likely have to work across a broad spectrum of devices, e.g. AI/AR glasses/contact lenses, smart phones, tables, laptops, computers, etc.
    - Making the PIAM intuitive and easy to use, especially with choosing different levels of consent is critical

  - Security
    - Hire the best and brightest to form a Red Team
    - This will be extremely critical in all stages of design, implementation and maintenance
  - Bots
    - It's highly likely the PIAM will become an interface to direct bots either a person owns, or contracts, to operate on their behalf
  - Governance
    - Beyond the actual legal functions the PIAM does, it will likely involve changes to existing laws and regulations within jurisdictions
    - Thus, hire people who have excellent regulatory/government law experience both locally and globally
  - Privacy
    - Ensure highly skilled privacy people, with not only local but global experience are contracted
- Develop a very limited initial set of requirements and deliverables, while at the same time understanding where future development might lie
  - I'm a big fan of crawl, walk and run strategies
  - Thus, keep the initial scope tight to keep the team on target
  - Then design a rapid set of iterative POC's, proving out certain components of the PIAM
- From the above, assemble requirements, deliverables, resource requirements, timelines and costs
- It's likely the initial costs will range in the tens of millions of dollars

Estimated Costs for the Global, Independent Non-Profit

Background:

On page 6 of "Secure, Network Based, Legal Self-Sovereign Identity (LSSI)" - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf it shows as part of the architecture, on the right hand side, a global, independent, non-profit, responsible for standards, licensing and threat assessments". It's then described on page 34, along with Red Teams, and paying for external parties to produce successful attack vectors.

It all starts with this curve - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf. It means, each hour, new attack vectors are being created not only against the technology used in legal identity, BUT ALSO THE GOVERNANCE, BUSINESS PROCCESS AND PEOPLE USING THE SYSTEM. That's why in this LinkedIn post, "Digital Transformation Vision - Legal Identity, Data & Consent" - https://www.linkedin.com/pulse/digital-transformation-vision-legal-identity-data-guy-huntington?trk=portfolio_article-card_title, it begins with a three dimensional triangle, showing each of the possible stack targets.

My underlying premise – except for large countries and companies who can continually defend themselves against the curve, the rest are increasingly prone to successful attack. Criminals and malicious states will leverage the curve to find weaknesses in the legal identity system, exploiting them. Since this is the underlying system legally proving who a person or entity is, it can render meaningless existing security defences protecting each person.

That's why the idea of having a global, independent non-profit arose in both my mind as well as Michael Kleeman, co-founder of many different telcos around the planet and ex-CTO of Boston Consulting Group. Both of us believed finding a way to substantially, continuously fund the non-profit, it would have enough experienced people and technological resources to do continual 24x7x365 threat assessments against all the components of a legal self-sovereign identity.

As mentioned in the Cost Estimates for LSSI section of this document, the global non-profit would also act as the global standards body for LSSI, BUT NOT BE RESPONSIBLE FOR ALL STANDARDS USED IN LSSI. As I see it, its job is to oversee the standards, ensuring they rapidly change, as either new ways of thinking arising from the fast-paced change occur or, due to threats.

LSSI involves many different legal jurisdictions. Thus, as part of its mandate, I see the body coordinating laws and regulations across different jurisdictions allowing LSSI to work globally.

In summary, the global, independent non-profit is very different than today's typical standard bodies. It's a new age type entity required to meet the challenges of the times. Thus, the question becomes who controls it, and how's it continually funded?

Governance, Location, Costs and Funding:

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

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.

On page 34 of "Secure, Network Based, Legal Self-Sovereign Identity (LSSI) - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf it discusses who watches the watchers? It suggests having a group of independent auditors to audit the enterprise regularly. 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.

Location of the Global, Independent Non-Profit

I can see the body's head-quarters being located 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 located 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.

Costs

There are 3 main cost centres associated with the global, non-profit:

- Governance
- Standards
- Threat Assessments

Governance

Governance is composed of:

- Management team
- Interactions with other management of standards bodies who either are the standards body for pieces of the LSSI or, are wanting to consume Toda LSSI as part of their standard
- Interactions with jurisdictions leaders and senior business community
- License specialists for designing and administering the pro-rata licensing fees
- To estimate costs, the above needs to be determined in detail

Standards

Standards is composed of:

- Specialists for each standard used in Toda LSSI
- Legal specialists
- Technical specialists
- Business process analysts to design and maintain rapid response processes for standards changes based on threats
- Training specialists to design continual training/education for users of the Toda LSSI standards as well as assist in designing education material for rapid changes to end users
- To estimate costs, the above needs to be determined in detail

Threat Assessments

Threat assessments is composed of:

- VERY SKILLED PERSONNEL covering a wide range of specialties including but not limited to:
    - Biometrics
    - Cloning
    - Artificial Intelligence (AI)
    - Bots both physical and virtual
    - Augmented Reality (AR)
    - Virtual Reality (VR)
    - Networks
    - Software programming
    - Databases
    - Cyborgs
    - Geomagnetic Disturbance (GMD)/High-Altitude Electromagnetic Pulse (HEMP)
    - Physical and virtual security
    - Quantum computing
    - Communications
    - Encryption
    - Etc.
- Red Team designed to act independently doing continual attacks against the governance, business processes, technological infrastructure and users of the Toda LSSI system
- A WIDE RANGE OF LATEST TECHNOLOGICAL RESOURCES enabling the above
- All of the above needs to be determined in detail with costs
- Bottom line – I can easily see this portion of the annual budget being well over $100 million a year or much more

Funding

I can see the following occurring to create a funding structure for the global, independent, non-profit:

- Have the non-profit heavily subsidize changes to each jurisdiction's CRVS system, i.e. almost give it away for no-upfront cost
- Then charge each jurisdiction a small fee per CRVS event to a maximum cap
- This will result in annual cash inflows to the non-profit
- Then license the use of Toda LSSI to jurisdictions and companies using the standards
- Keep the license fees relatively low to ensure wide adoption and continual use, but design them such that this in turn also generated regular revenue for the global non-profit
- The devil is in the details – thus initial funders must carefully work through:
    - Pro-rata CRVS funding structure
    - Licensing fees
    - Determine how much initial costs need to be subsidized until the cash flow comes in from the above

Estimated Costs for a Rethought Global Notary

Background:

In the summer of last year, I assembled a small team of experts to rethink legal identity leveraging Toda LSSI. I carefully choose the first use case I gave them, selecting one I knew was very hard to solve. I knew if we could solve this, then addressing all the other legal identity use cases would be easy. Here's the use case I gave them:

> **"Jane Doe's born to a family being targeted by the government jurisdiction A. They're forced to flee the country, without any form of legal identification. The government deletes Jane Doe's records in the CRVS, national identity, etc. How's Jane Doe going to prove her legal identity in another Jurisdiction B?"**

The solution we came up with involved rethinking notaries. At birth, the jurisdiction's CRVS would not only write Jane Doe's legal identity plus her forensic biometrics to their CRVS system, and write to Jane Doe's physical and digital Toda LSSI files, BUT ALSO WRITE TO A GLOBAL NOTARY DATABASE.

Jane goes to a local notary in Jurisdiction B and, with her consent, provides her name, date of birth and location, along with her forensic biometrics. THE LOCAL NOTARY IS ONLY ABLE TO DO A SEARCH ON A SPECIFIC ENTRY, AND NOT BE ABLE TO TROLL THE GLOBAL DATABASE. If a successful match is found, the notary can then give Jane Doe a legal attestation, both physically and digitally, she's Jane Doe.

I then took this concept and applied it to less drastic use case scenarios. Like what?

Consider Jane Doe wants to do a high transaction with an enterprise. The enterprise might decide to not trust their own biometric systems, but require Jane to do to a local notary. By law, the notary must keep up with technological developments, as well as being professionally qualified by the local jurisdiction's notary laws, to obtain legal identity information plus biometrics and search the global notary database. If the match is successful, they'd not only create a legal attestation Jane Doe is whom she claims to be, but take on some form of legal responsibility for the attestation.

This rethinks the functions of old school notaries, who today are operating in a very complex physical and digital world, where proving a legal identity to then attest its them, physically or digitally signing documents, is very hard to do. It provides an independent attestation for a person, without the government having to get involved, i.e. it's privacy by design.

Design and Deployment Strategy:

Here’s my thoughts on how to achieve this:

- Don’t try to solve all the world’s notary challenges out of the gate
    - i.e. instead find 1-3 jurisdictions to work with
- First, get the rethought CRVS system into design and implementation as outlined in the CRVS section of this document
- Then, begin discussions with a committee composed of:
    - Local notaries
    - Business leaders
    - Government representatives
    - Members of the global, non-profit including the governance, business process and threat assessment team
- Get agreement on the requirements, deliverables, resource requirements, timelines and costs
- Have a funder fund this
- Break down the work into the following parallel workflows:
    - Legal changes required to local laws and regulations
    - Technical infrastructure required
    - Business processes required
    - Training/education requirements
    - Do quick POC’s to prove out the technology, security, et al
    - Then do small, very tightly controlled pilots
    - Do lessons learnt and then rapidly scale within the jurisdiction
    - Begin to assemble the team with funding to then create the global notary body
- I think the global notary body should be separate from the global, non-profit
    - However, I think the global notary body should be joined at the hip with the global non-profit regarding changes to their notary standards, especially with respect to threat assessments regarding legal identity verification
    - Without this, the local notaries can be prone to successful masquerading by criminals as another person
- **Bottom Line:**
    - First, get the CRVS system and global non-profit funded and doing initial design in 1-3 jurisdictions
    - Then fund local notary changes with an eye to rapidly scaling this to become global

Summary

It's transformational. This paper summarizes a rethink of how people, poor to rich, on the planet legally identify themselves. It gives each person, from cradle to grave, a legal self-sovereign identity (LSSI), both physically and digitally, which works within each jurisdiction, as well as globally. Each person is in control of their legal identity, choosing how much to release their identity data, biometrics and behavioral data.

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 identity problems at the global stage. As the deployments become successful, design them to rapidly scale.

Lay the foundations for maintaining the Toda LSSI infrastructure, over time, both fiscally and security. That's why the global, independent non-profit is created. Our new times we're entering, having a rapid rate of change, require new frameworks to continually address it.

It's unlikely one funder can fund all of which this document outlines in terms of costs and complexity. Thus, it makes sense for funders to come together, with each funder funding portions of the costs.

In 1989, with the fall of the Berlin Wall, a group, the Scorpions, recorded a song "The Winds of Change" (https://www.youtube.com/watch?v=n4RjJKxsamQ). They recognized the wind of change sweeping the planet. Today, 30 years later, the winds are sweeping the planet, both physically and digitally. Around us, our old walls of legally determining a person's identity now no longer work well and need to be taken down. It's time we take courage, rethinking them, allowing the "children of tomorrow dream away, in the wind of change."

About the Author:

Guy Huntington is a veteran 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 five years, he's been thinking, writing and searching for new pieces with which to rethink both human and AI System/Bot legal identities. He now has an architecture and plans addressing this creating a legal self-sovereign identity (LSSI). Guy consults on LSSI.