Proposals Paper –
Incremental Approach to Implementing New Age Legal Identity

Authors:
Guy Huntington, President, Huntington Ventures Ltd.
Michael Kleeman, UCSD

Date: December 4, 2019

Note:
The authors wish to thank Kristin Little and Diane Strahan for acting as reviewers of this proposal.

Table of Contents

Who The Paper is Aimed At:

- Government leaders and administrators
- Industry leaders

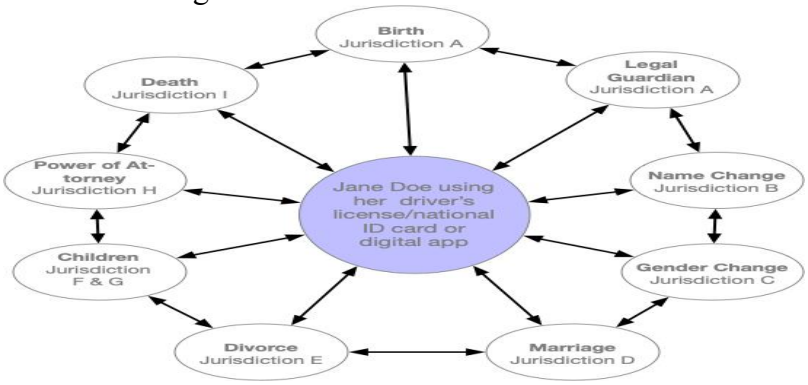
Executive Summary:

Our principal ways of legally tracking major life events, civil registration, relies on technology from the middle ages, i.e. paper. Traditionally, once legal identity is established (think driver's license), it's used in expanding business and social worlds. As we move into a digital world, businesses seek increased confidence they are transacting and engaging with the person they claim to be and not a computer generated robot or bot. Existing problems include:

- Business:
  - High cost of identify theft, and fraud to the individual and institution
  - Lack of trust in an issuing jurisdiction's documentation the person is using to verify their identity
  - Lack of confidence by businesses in confirmation that a person clicking on an advertisement, or accessing a website, is a human (and not a bot)
- Issuing Juisdictions:
  - Inability to ensure integrity of seed documents, like birth certificates, used to verify identity, prior to issuing documentation such as driver's licenses, social/medical services, passports, etc.
  - Inability to empower jurisdictions to give citizens secure control of their own legal physical and digital identity
  - How to digitize existing forms of conventional identities, e.g. driver's licenses et al, such that it works across all jurisdictions?
- Citizens:
  - How to enable multiple personas, both digitally and physically, while also being able to easily prove their legal identity digitally?
  - Inability to prove citizens legally are of age, or other specific criteria, without having to reveal their full legal identity.
  - How to empower citizens to not have to repeatedly fill in physical or online forms with sensitive identity information?

This paper proposes a new vision for legal identity- a secure, self-sovereign, and globally-recognized system of identification by:

- Leveraging existing legal identity systems, e.g. driver's licenses/national ID cards
- Rethinking human legal identity, especially for children, wards of state, etc.
- Creating this kind of architecture:



Benefits:

- Business:
  - Lower cost of identity verification via global standards for legal identity
  - Higher degree of trust a person is whom they claim to be, i.e. lower fraud costs
  - Able to determine who's a person and who's a bot in a AI/AR/VR, online or physical environment
  - Trust a legal digital signature
- Jurisdictions:
  - Create global standards for digital driver's licenses and digital legal identities
  - Improve identity verification via creating common global civil registration service protocol
  - Create self-sovereign legal identities for their citizens
  - Enable citizens to use anonymous digital and/or physical legal identification proving they're of age to enter pornographic areas and/or purchase age restricted goods or services, regardless of jurisdiction
- Citizens:
  - Easily be able to prove their legal identity which they control
  - Have anonymous legal identity proving they are human and either above or below age of consent
  - Use their digital legal identity to automatically fill in identity forms
  - Be sure their legal digital identity can't be easily stolen and then maliciously used

To begin to implement this new vision, the paper suggests::

- Partnering to fund a series of Proof of Concept (POC) and fast, iterative pilots for a rethought physical and digital driver's licenses/national ID cards
- Creating steering groups composed of the pilot jurisdictions and appropriate other organizations to:
  - Drive and stress-test the pilots, including explicit efforts to defeat the approach ("red teams")
  - Coordinate with other jurisdictions to create global standards for digital driver's licenses, civil registration data and protocols to exchange such data
  - Allow jurisdictions to select their own vendors to deliver the above
  - After successful pilots, rapidly scale the solutions globally to many other jurisdictions

Robots are now with us, both physically and virtually. The paper identifies some of the challenges for jurisdictions in legally identifying bots. A separate paper will delve into suggested solutions in more detail.

Proposals Paper – Planned Incremental Improvements Towards A Coherent Identification System

Old World to a New Digital World

Through the years, many disconnected, paper-based ID systems have evolved at local, regional and national levels. These include civil registration systems, producing paper-based documentation such as driver's licenses, national ID cards, tax numbers, social insurance numbers, etc.

Attempts to transition these discrete systems from paper to digital are falling short. For example, jurisdictions are piloting digital driver's licenses. Yet, underneath these digital identities, reside old paper-based ways of legally verifying the identity, that is then made digital.

Similarly lacking are ways we legally determine if a online person is of age of consent or not. Businesses want to be able to easily prove consumer's identities, regardless of which jurisdiction the business they're interacting with in, while at the same time reducing identity theft.

This has resulted in an increasing lack of trust in our digital ecosystem. Parents can't trust their kids will be safe, users can't trust their identity will be safe, and businesses can't trust they are actually dealing with a human being. Additionally, we now can't trust/know the identity of who is feeding us information, e.g. Facebook ads and elections.

The rise of Augmented Reality (AR), Virtual Reality (VR), Artificial Intelligence (AI), deep fakes and robots, both physical and virtual, will further complicate matters. This story, "The charge of the chatbots: how do you tell who's human online?" illustrates the problem of determing who's a human, who's a bot and if the message is real.

Business and consumers alike will want to know:

- Who they're dealing with, i.e. a human or a bot?
- Validate the person/source is who they say they are

This requires a new legal toolkit. We should be planning for a coherent, secure, legal identification system for both human and bots.

Current State of Legal Identity Across Jurisdictions

Each jurisdiction around the world has a distinct way of verifying and issuing legal physical and identity information, creating a disorderly global system. Unfortunately, many of the more promising technologes for scalable solutions have too many flaws. Here are a few of the shortcomings associated with existing regional or global identity systems:

Biometric identification

- Several national jurisdictions obtain biometrics from citizens, some starting at the age of 5 (e.g. India's Aadhar) or 15 (e.g. Estonia) which are then used to verify the identity
    - But to the best of our knowledge, no jurisdiction is currently obtaining biometrics at birth and attaching this to the CRVS registration
- Many jurisdictions political environments aren't conducive to requiring citizens to provide biometrics for civil registrations and/or physical tokens like driver's licenses
- Citizens are rightfully afraid the biometric databases might be breached, resulting in their biometrics becoming available for malicious uses
- There has been little scientific research done to confirm the use of fingerprints and iris scans or other biometrics is enough to differentiate clones from their source human

Result: Biometric confusion with different uses of biometrics jurisdiction to jurisdiction. Late capture of biometrics leads to higher risk of biometric identify theft. These leave off the table a scalable and easily applicable solution to mitigate and address identity theft.

Our current systems are inconvenient for individuals and costly to businesses

- Most civil registration services still use paper as the legal documentation of a civil service process
    - These are prone to fraud and theft, even with the current generation of anti-counterfeiting print techniques
- To mitigate risk of fraudulent seed documents, some jurisdictions within a country are able to search cross civil service databases to verify if a civil registration document being presented is valid (e.g. Australia)
- However, there is no ability to electronically search all civil service registrations across jurisdictions to verify the document's validity
- This causes a rise in Know Your Customer (KYC) software to compensate for weak identity verification

Result: Weak legal identity verification processes, high identity theft and increased costs for businesses. It creates inconvenience for individuals, given once they leave a given jurisdiction, the timeframe it takes to get/use any legal documentation requires a slow paper process.

Our current attempts at digitization are uncoordinated and vulnerable to fraud

- Many US jurisdictions are piloting or have implemented digital driver's licenses
  - Some of them have the ability to provide anonymous legal identification without having to show their name and address
  - If a phone is lost, the state's DMV (Department of Motor Vehicles) can remotely delete the electronic license
  - They use US Government 2005 Real ID standards requiring all states to have Real ID licenses by Oct 2020
  - But these tokens have limited application outside of the physical world
- Europe, Australia and some Asian countries are also implementing digital driver's licenses
- Mostly jurisdictions are based on a visual inspection of the underlying foundational documents
  - Including things like birth certificates and/or checking against a central registry service to validate the document
  - Thus, if a document is a good fraud, then a false identity will likely be accepted and created in both physical and digital identity documents

Result: Lack of global standards results in legal digital identity silos being created. This results in fraudulent identities from the start, with the ability for fraudulent data to enter other jurisdictions.

Required: A secure, global legal identity system benefiting jurisdictions, business and citizens alike

Jurisdictions:

- Ability to digitize existing forms of conventional identities, e.g. driver's licenses et al such that they are accepted globally and are usable in virtual and physical commerce
- Give jurisdiction's citizens secure control of their own legal physical and digital identity in this new age
- Enable citizens to use anonymous digital and/or physical legal identification proving they're of age to enter pornographic areas and/or purchase age restricted goods or services, regardless of jurisdiction
- Enable their citizens to legally, digitally sign documents within their jurisdiction, regionally and globally
- Improve integrity and reduce fraud risk of seed documents, like birth certificates, which are used to verify the identity prior to issuing them things like driver's licenses, social/medical services, passports and/or national identity cards
- Mitigate the risk of paying social services and/or health costs for people who aren't citizens claiming they are and/or having children they don't have
- Keep jurisdiction identity systems up to date with people who move into and out of the jurisdiction
- Lower their identity management costs amongst all their government departments and agencies
- Enable jurisdiction's citizens not having technology to use for their legal digital identity not being left behind in the digital revolution
- Electronically be able to verify a person's identity from another jurisdiction
- Establish secure biometric based identity documentation at birth

Business:

- Validate that a person is whom they claim to be
- Trust a jurisdiction's document the person is using to verify their identity
- Legally determining if an entity they're dealing with online or, in a AI/AR/VR environment, is a human or a bot
    - Confirm a person clicking on an advertisement or accessing a website is human
- Trust a legal digital signature within a jurisdiction, regionally and globally
- Be able to verify a transaction critical attribute (e.g. over 21) without needing to obtain the full personal ID
- Lower their costs of identity management and identity fraud

Citizens:

- Have multiple persona's both digitally and physically, but be able to easily prove their legal identity digitally
- Prove who legally are and of age, or other specific criteria, without having to reveal their full legal identity
- Not having to repeatedly fill in either physical or online forms with sensitive identity information
- Easily enable them to legally sign documents digitally
- Be sure their legal digital identity can't be easily stolen and then maliciously used
- Be able to cross between different legal jurisdictions and still easily prove their legal ID
- Be in full control of their legal identity physically and digitally
    - Be able to see how their identify has been used and by whom
- Enable them to not be left behind in the digital revolution when they don't have access to technology
- Confirm that they're dealing with a human in online, AI/AR/VR environments

Without addressing the above, any digital legal identification system will become disorganized and unworkable. It creates huge gaping holes, malicious criminals and/or states can easily take advantage of. Businesses end up creating their own identity verification systems to compensate. People get frustrated as their identities are stolen, while lacking an ability to easily prove who they are digitally. Jurisdictions create identity digital barriers to trade cross borders.

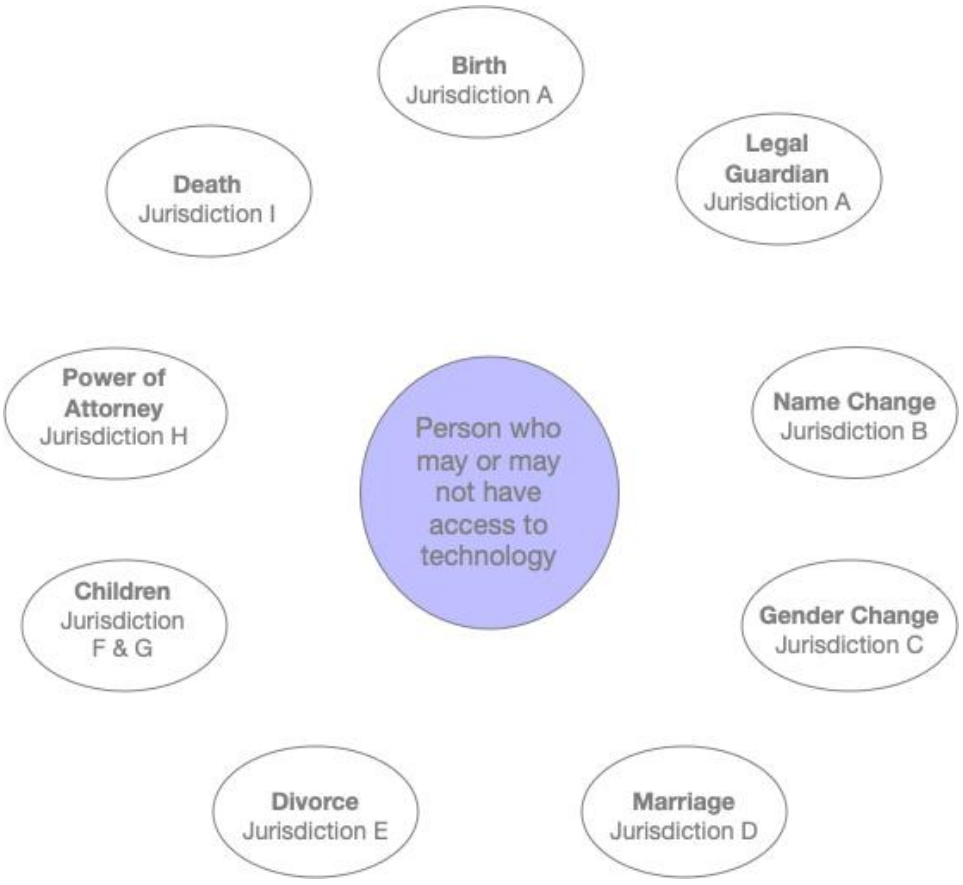
To increase ALL trust for any transactions/engagements, we need to know we are dealing with whom they claim to be and whom we think we are. If only some jurisdictions identities are known to be more legally accurate and not others, it hurts the overall trust in the digital ecosystem, negatively impacting individuals, businesses and governments.

Leverage Existing State/National Identity Systems

It makes economic, political and user sense to leverage existing infrastructure and accepted ways of identification, e.g. driver's licenses and/or national/state identification cards. People have them in their physical wallets and soon in their digital ones. Citizens, business and governments also understand how they can be used to verify an identity. So, the first recommendation of this paper is to leverage existing state/national identity systems.

There are some challenges inherent in this approach that must be addressed, regarding multiple jurisdictions issuing civil registration events for the same person. The diagram below illustrates this:

Creating a Self-Sovereign Legal Identity System – Current Design



How can a person be in control of their legal identity, both physically and digitally, across multiple independent jurisdictions? By employing public and private keys, personal control is possible, but such a system would have to address several risks…

Who Issues the Keys?

For a person who's undergoing a civil registration event, it's theoretically possible for a jurisdiction to issue a digital private key for the event. By using their private key, a person can then use this to prove who they are. Protocols like Sovrin/Blockchain leverage this approach.

Criminals Easily Obtaining Private Keys

The existing cryptocurrency markets and numerous cyber-attacks have shown it's not that hard for malicious people to obtain a person's private key either through technical or social means, and then masquerade as them. Thus, issuing a digital private key online to a person, brings with it a high degree of risk their identity might be stolen. How can this risk be mitigated?

Where to Store The Keys?

Innovative cryptocurrency-based solutions, like Ngrave, issue the private key offline. They then use QR codes to communicate information between the offline device and the app, without ever transferring the actual private key. This significantly reduces the risk of a malicious person being able to steal a citizen's civil registration private key.

How Can This Be Applied to Existing Infrastructure?

A solution framework must be low cost, secure and already used/understood by the citizen. It makes sense to leverage existing driver's licenses to do this. By using proven Near Field Communication (NFC) technology, a civil registration event private key, could be securely written and stored on an NFC driver's license. At the same time, a QR code could also be written to the NFC card.

Access to the driver's license private keys on the physical card, could be protected via use of encrypted anonymous, revocable and re-issuable biometric (as per the paper by Rud Bolle). Thus, if a malicious person does gain access to the biometric securely stored on the card, the jurisdiction can easily cancel the physical card with the authenticating biometric, and then reissue them. However, this, and all schemes with a central authority, have the issue of trust in that authority. Note that this is the default in almost all national identity schemes.

The jurisdiction would then modify its existing digital driver's license app to accept QR codes. When the phone or electronic device is near the NFC driver's license, it would enable a secure, encrypted channel to verify the QR code, and update the person's legal identity information.

Authentication access to the legal identity app would leverage the same type of technology for the card, i.e. anonymous, revocable and re-issuable biometrics securely stored on the device. Optionally, an additional 4-digit pin may be used.

If a person doesn't have access to technology, they would carry their card, and present it to readers at government agencies and business. Depending on the jurisdiction, in addition to the

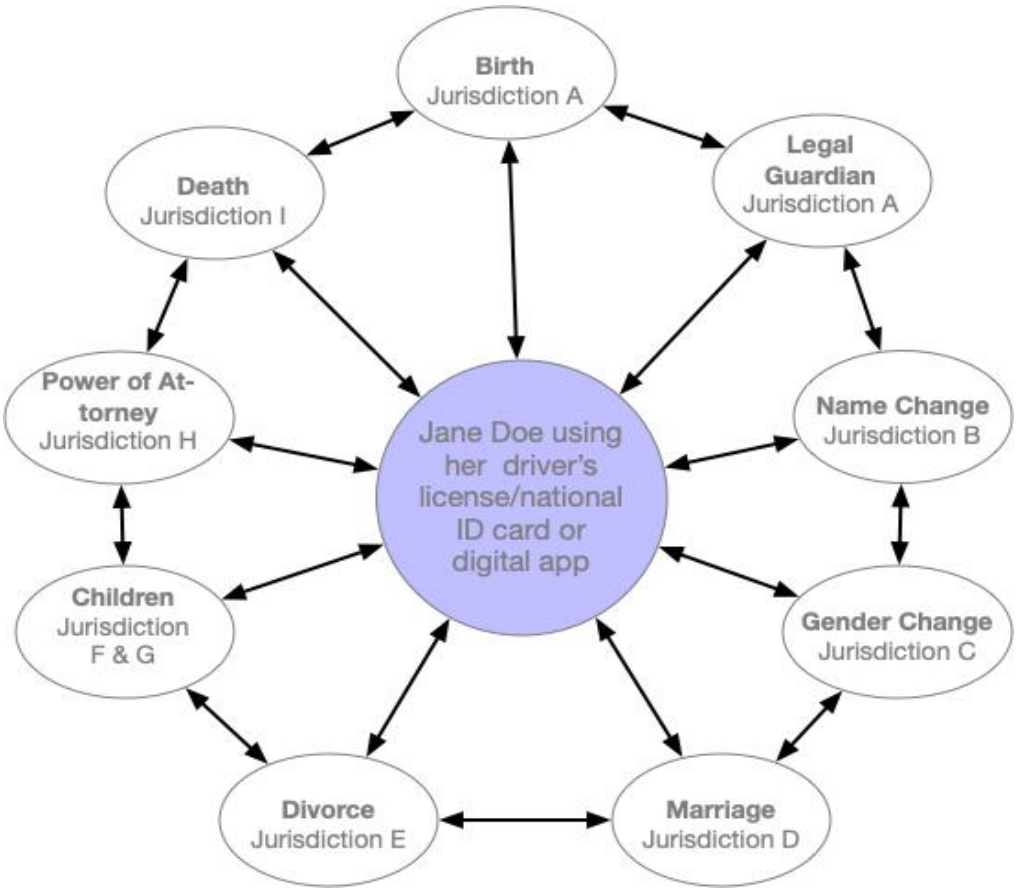
person authenticating to the card, they might require the person to enter a 4-digit pin as well to verify their identity. Thus, no one is left behind in the technological revolution we are now in. When a person wants to reveal portions of their legal identity it could be done via a QR code or some other manner.

Who Controls The Citizen's Identity?

The person is now in primary control of their legal identity, i.e. they have a legal self-soverign identity. As they move between different jurisdictions, when a civil registration event happens to them, the jurisdiction would update their card with the event. If the person has access to technology, the jurisdiction would also update the individual's legal identity app.

Conceptual Future Solution Diagram

Conceptually, here's what it would look like:



Note: The above diagram is simplified. In reality, for most civil registration events, the jurisdiction involved would be able to search all other jurisdictions, to determine if the person already exists and, based on this, if the civil registration event is allowed.

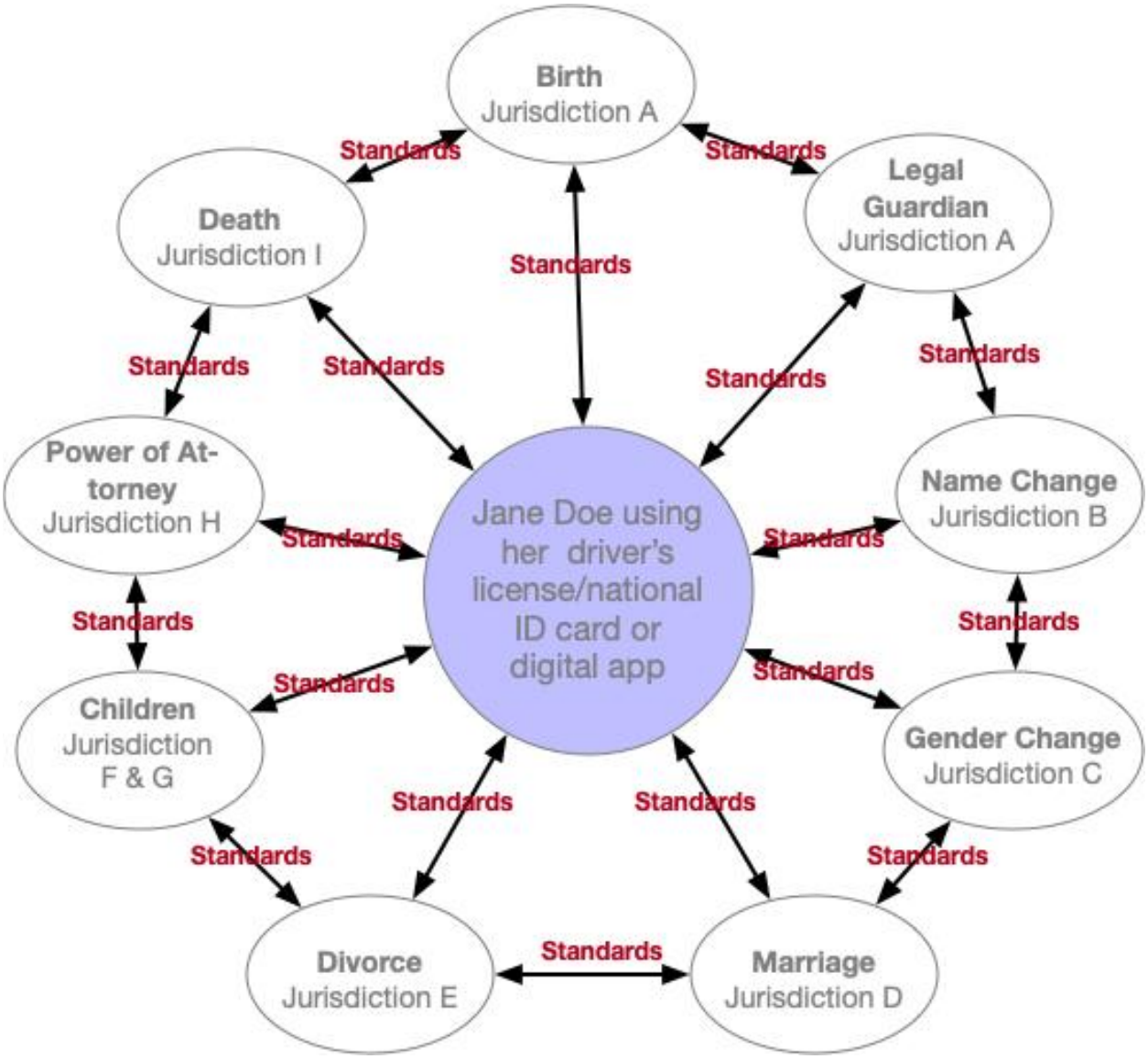
The Devil is in the Details

Anyone who's ever architected and deployed complex identity systems knows the devil is always in the details. Wonderful looking conceptual drawings, with lines connecting different groups, may flounder during implementation, where the legal, business, and technical reality can impede progress.

To counter this, there are two prerequisites to success:

- Civil registration standards/protocol
- Digital driver's licenses standards

This is what should be created by the POC/Pilots:



Proposal 1 – Rapid Proof of Concept (POC) and Iterations for a Small Pilot Group for NFC Enabled Cards Plus Digital Apps Used for Driver's Licenses and/or NFC Cards

Goals:

- POC to demonstrate NFC driver's license/national ID physical cards work in conjunction with modified digital driver's licenses/national ID cards with civil registration private keys written to the cards
- Create model digital driver's license standards
    - Show it can work cross-jurisdictions
- Create standards for civil registration services by first creating a common protocol
    - Show it can work cross-jurisdictions
- Create model standards for a legal digital identity
    - Show it can work cross-jurisdictions
    - Show it can work with a variety of business
        - E.g. banks, telcos, advertisers, etc.

Series of Iterative POC/Pilots

Do a fast POC implementation of the NFC card plus phone/electronic device app using technology which exists today.

The goal is to develop preliminary standards for the cards, app and digital legal identity, which jurisdictions can then implement, using whatever vendors they so choose. Then, rapidly scale them across multiple jurisdictions.

This includes standards for civil registration queries to be made across jurisdictions to existing systems. The reality is different civil registration jurisdictions have different forms of storing and retrieving their data. Some are mostly paper, while others may have digital storage of the information, in different forms.

The pilots should develop/prove a common protocol by which Jurisdiction A can query Jurisdiction B about Jane Doe's civil registration event. Thus, Jurisdiction A and B, would create their own internal interface to their data systems, be they paper and/or digital. The query would come in using the protocol, be interpreted into a form their internal systems can understand, and then the response back would be using the protocol.

All of which, requires citizen consent. Many of these papers recommend adoption of Kantara User Managed Access (UMA) and User Managed Access Federation. Thus, the citizen should provide their consent, via their legal phone app, and have a clear audit trail of their consent, across disparate platforms.

Governance: Steering Group

A steering group should be created composed of:

- Pilot jurisdictions
- Representatives from business, e.g. banks, telcos, advertising associations, etc.

Business must be involved in the steering group. Why? They can develop standards by which a person can digitally reveal to an enterprise they are a person, not a bot, and are either above or below age of consent. This will leverage emerging legal digital identity, such that it mitigates risk of bots acting like humans, with enterprises paying for the cost of false identities.

Working Group

It makes sense to have a small working group within the steering group that focuses on POC/pilots. This working group should then regularly communicate with the larger steering group. The steering group's purpose is to rapidly scale outwards the results of the working group.

Red Team

All systems are vulnerable to attack and it is important that any project looking to develop a global model needs to 'stress test' it and the associated technologies. Thus, we include an explicit effort to attack and defeat any proposed approach using a Red Team model.

A Series of Iterative Steps:

Rather than trying to boil the global ocean, we see it as a series of fast iterative steps:

- Propose a solution
- Pilot it within a few jurisdictions
- See what works and what doesn't work
- Redesign until we have a secure, robust, legal, business process and technical framework
- Have larger steering groups, where the results from the POC/pilots are rapidly communicated with planning made to expand it globally

Proposal 2 – Rethinking Legal Identity

The use of existing drivers licenses plus enabling existing civil registration systems to be queried, all makes sense. However, there's a need to rethink legal identity and the management of it by citizens. Why?

Challenges requiring new ways of thinking:

- When is legal and biometrically confirmed identity established, by whom and how?
- How is a parent or a legal guardian determined legally, physically or digitally, when acting on behalf of the child?
- How is a parent/legal guardian able to control their child's legal identity both physically and digitally?
- How does a parent/legal guardian protect their child's legal identity when entering AI/AR/VR environments at home, school or healthcare environments?
- How are children's legal identities management granted to others, e.g. grandparents, to manage their identity, on a time limited basis?
- How is a person's legal identity, who's a ward of the state, managed physically and digitally?
- How does a change of legal guardianship of the child make its way from the authoritative system, to the legal identity system both physically and digitally?
- How is a person's legal identity, who's now requiring power of attorney, managed physically and digitally?
- How are people under the age of consent, determined legally, physically and digitally (especially when they try to enter sex environments, etc.)?

Thus, a second project running in parallel to Project 1 focussed on rethinking legal identity is proposed.

Goals:

- Establish physical and digital legal identity methods for:
  - Managing one's legal identity for people under the age of consent, or requiring ward of state, or power of attorney
  - How digital identities will be conditionally managed with time limited consent by others
  - Providing children under the age of consent with physical/digital identities proving they are human and under age of consent
  - Protocols in the digital legal app enabling a person to show they are legally a parent, or legal guardian, or acting as power of attorney of the child/person
- Conduct POC/pilots to demonstrate and then implement the designed solutions

Governance: Steering Group

The same steering group used for Project 1 might also be used for this project

Working Group

A different working group should be formed for this project. Why?

It requires careful thought from a legal, business process and technical perspective on the implications, requirements and usage of a new thought legal identity for the digital age in which we now live. Thus, the membership of the working group should include:

- Pilot jurisdictions
- Lawyers providing legal guidance for things like delegated legal identity management, etc.
- Children's' right associations
- Etc.

Red Team

A separate, but parallel, Red Team will be created for this effort for reasons discussed above.

Suggested Steps:

- First produce a working paper outlining proposed legal, business process and technical solutions
- Revise the paper based on feedback from the steering group and other agencies/associations
- POC the proposed solutions
- Determine what works and what doesn't work
- Then pilot the solutions in jurisdictions
- Rapidly scale

Bots – Legal Identification

The arrival of both physical and virtual bots creates new challenges for jurisdictions, business and citizens including:

- Virtual bots can be created in sub-seconds
- They also can be produced in insane numbers per second
- They can also cross borders instantly, globally
- How will a bot who's operating in a jurisdiction, be legally identified?
- How will the jurisdiction X know a bot's been created in Jurisdiction Y?
- How will a court of law say that Bot 12345 did the actions it did?
- How will a court of law determine that Bot 12345 was masquerading as Jane Doe or another Bot abcde?
- How is Bot 12345 tied to ownership of Jane Doe or, an enterprise in another jurisdiction or, in the not so distant future, another bot?
- How is a bot legally determined in an online environment
- How does a human know they're interacting with a bot?
- How are bots legally identified when acting together in singularity

This paper doesn't address these important issues, but they will be addressed in a subsequent paper.

Summary

This paper began by stating any proposal for human legal identity, should leverage existing forms of identity, such as driver's licenses and national ID cards, be they physical or digital. It then presented two proposals for incrementally implementing a rethink of human legal identities:

- Rapid POC/pilots of NFC enabled driver's licenses/national ID cards with global standards being created for digital driver's licenses and civil registration data
- Rethinking human legal identity for the digital age

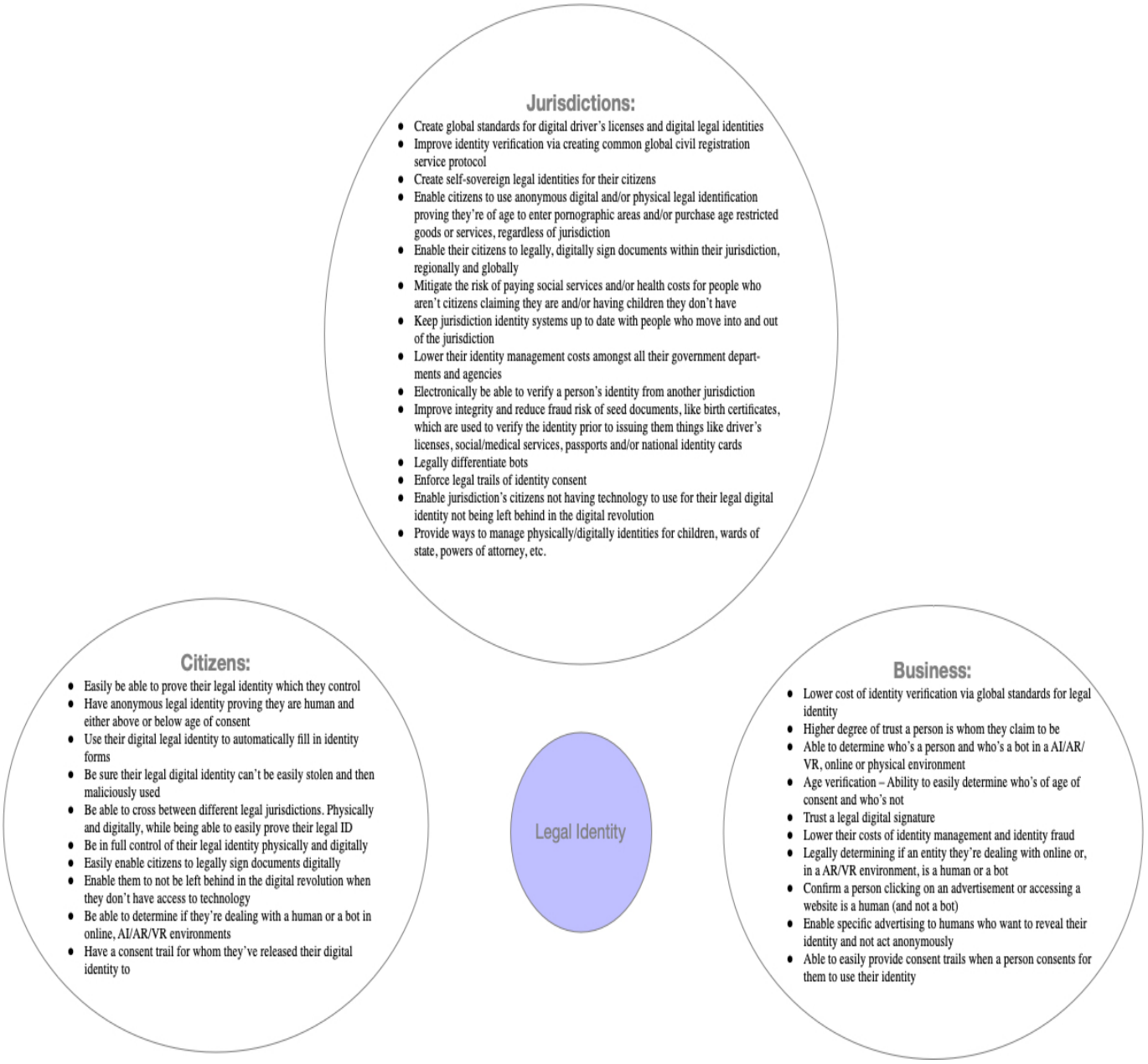
Benefits include:

- Business:
  - Lower cost of identity verification via global standards for legal identity
  - Higher degree of trust a person is whom they claim to be
  - Able to determine who's a person and who's a bot in a AI/AR/VR, online or physical environment
  - Trust a legal digital signature
- Jurisdictions:
  - Create global standards for digital driver's licenses and digital legal identities
  - Improve identity verification via creating common global civil registration service protocol
  - Create self-sovereign legal identities for their citizens
  - Enable citizens to use anonymous digital and/or physical legal identification proving they're of age to enter pornographic areas and/or purchase age restricted goods or services, regardless of jurisdiction
- Citizens:
  - Easily be able to prove their legal identity which they control
  - Have anonymous legal identity proving they are human and either above or below age of consent
  - Use their digital legal identity to automatically fill in identity forms
  - Be sure their legal digital identity can't be easily stolen and then maliciously used

To achieve the above, steering and working groups are suggested. Start with what exists and then rapidly do POC's/pilots to see what works and what doesn't work. Then adjust and rapidly scale. By doing so, the benefits to governments, citizens and business are significant.

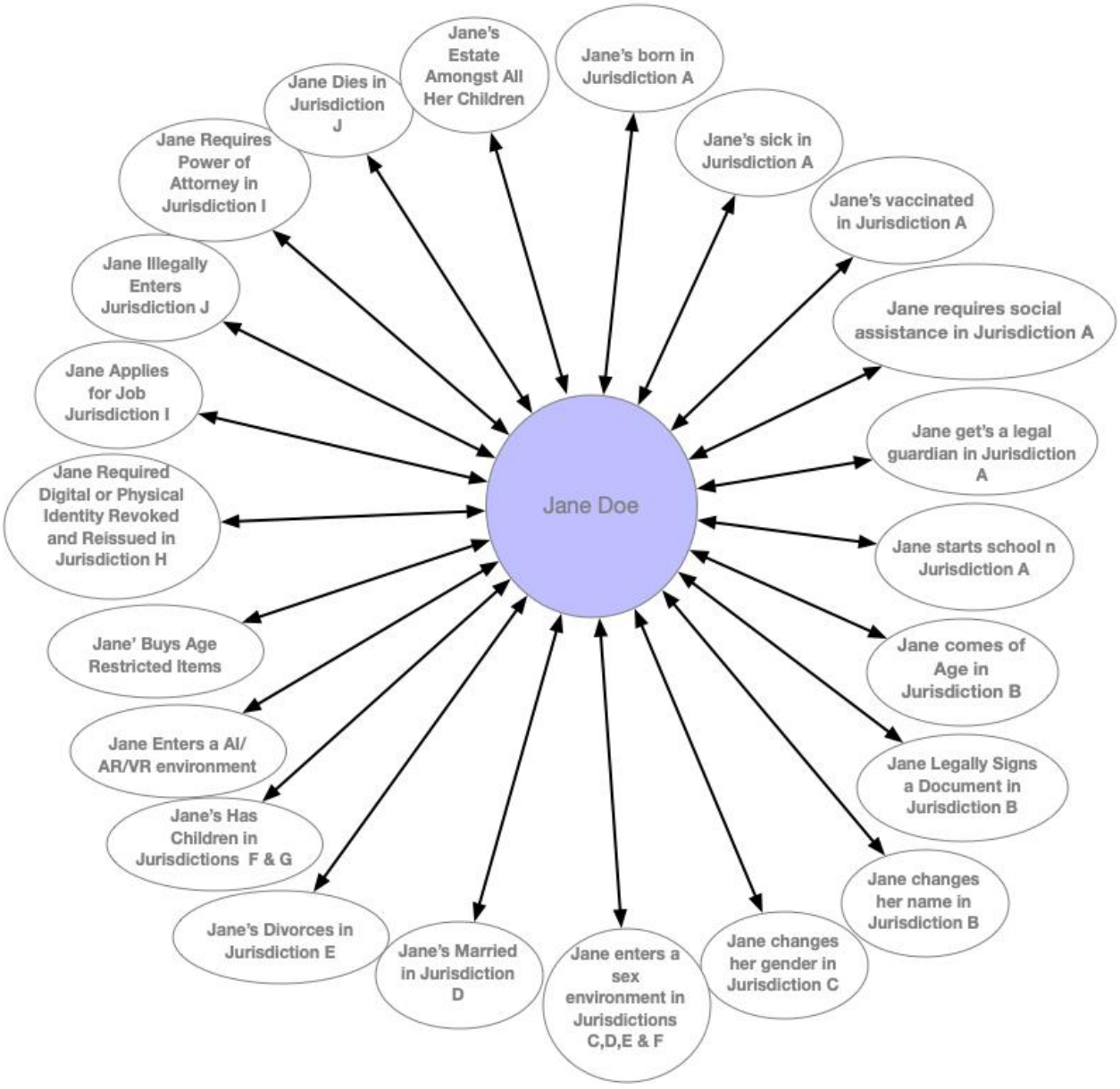
The purpose of this paper is to coalesce various jurisdictional developments in physical and digital identity. Funding should occur cross-jurisdictions for the above projects.

Benefits Summary:



Appendix A - Legal Identity Events Use Cases

People today can easily move around jurisdictions virtually or physically. This poses challenges in jurisdictions having the ability to see what the legal identity status of a person is, before granting the civil registration. Thus, the following 22 sample use cases for Jane Doe illustrate design requirements to address this:



Appendix B – Identity Challenges for Jurisdictions, Business and Citizens

General:

1. This proposal seeks to incrementally improve legal human identification within a jurisdiction, regionally and globally. It will assist in mitigating identity fraud.
2. However, it's not a panacea for all legal human identity challenges. If a malicous person is able to register a false identity at birth, or obtain such a false identity, then the person will still be able to masquerade as another. Thus, the use of good fraudulent breeder documents is not addressed by this proposal.
3. HOWEVER, the authors are working on other proposals, with others, where the use of biometrics at birth (baby fingerprints), and obtaining during first year of school an iris scan, are then attached to a person's civil registration record. This will address the use of breeder documents plus also be able to differentiate human clones. All of this is outside the scope of this proposal.
4. **The security of the entire system (business, technical and legal/regulations) is paramount.** The use of Red Teams at all stages of this proposal is therefore critical. The authors' experiences have taught them not to believe what solution design teams propose. Instead, it must be continually attacked by a friendly team, to determine what works and most importantly, what doesn't work. Thus, a continual iterative attack strategy, for business processes, technical infrastructure and user experience, must be used for all stages from POC through to pilots and broader rollout.
5. By doing fast iterative work, challenges can be identified, addressed and mitigated by adopting the learnings from the POC and pilots. This will usher in the beginnings of a new age legal identity system.

Jurisdictions:

1. Since there are no existing data standards for civil registration systems globally, the challenge is in implementing new ones. This proposal seeks to do so incrementally.
2. Many jurisdictions still use paper and/or have different underlying databases for their civil registration systems. Thus, the first step is to create a common electronic protocol which can be used across these disparate systems. This can be phased in over time.
3. The lack of a common standard for digital driver's licenses is actually a good thing. Why? It creates the opportunity to standardize human legal identity data. By agreeing on a common global standard, each jurisdiction can then implement the standard, at their own pace, within their civil registration systems. The need for interoperability of the digital driver's licenses will drive change throughout the various jurisdictions, regionally or globally.
4. By creating a common civil registration protocol, it will reduce identity fraud by being able to cross-search identities presenting themselves within a jurisdiction for a civil registration event. As a result, there is a higher likelihood the person is whom they claim to be. If the jurisdiction issues a digtal signature to citizens of age, it can then be more trusted by business, citizens and other jurisdictions.

5. However, note that until the jurisdiction implements stronger identification verification from birth onwards, i.e. biometric confirmation, then it will still be possible for malicious people to masquerade as another within the jurisdiction. Additonally, the civil registration system won't be able to differentiate human clones.

Business:

1. This incremental approach will offer the beginnings to business of having a global legal human identity standard to align business systems with. It will lower business identity management costs while also reducing identity fraud.
2. The proposed system will also enable business to reduce their costs of bots clicking on advertisements posing as humans.
3. The challenge will be ensuring the anonymous digital legal identification system is secure and easily works with business.
4. Add it all up and business must be part of steering and working groups to develop the legal identification systems.
5. Note the system won't eliminate identity fraud. As noted above, until jurisdictions adopt a biometric civil registration based system, business will still be affected by fraudulent identities. Thus, the need for Know Your Customer (KYC) systems will continue.
6. However, also note that these types of systems will now have a new improved human legal identity baseline to work from.
7. The authors see the development of a global legal human identity standard as a new underpinning in potential development of a rethought World Trade Organization (WTO) Digital Trade Organization. It offers legal identity standards that can be used, cross-jurisdictions, to enable the smooth flow of humans, goods and services.

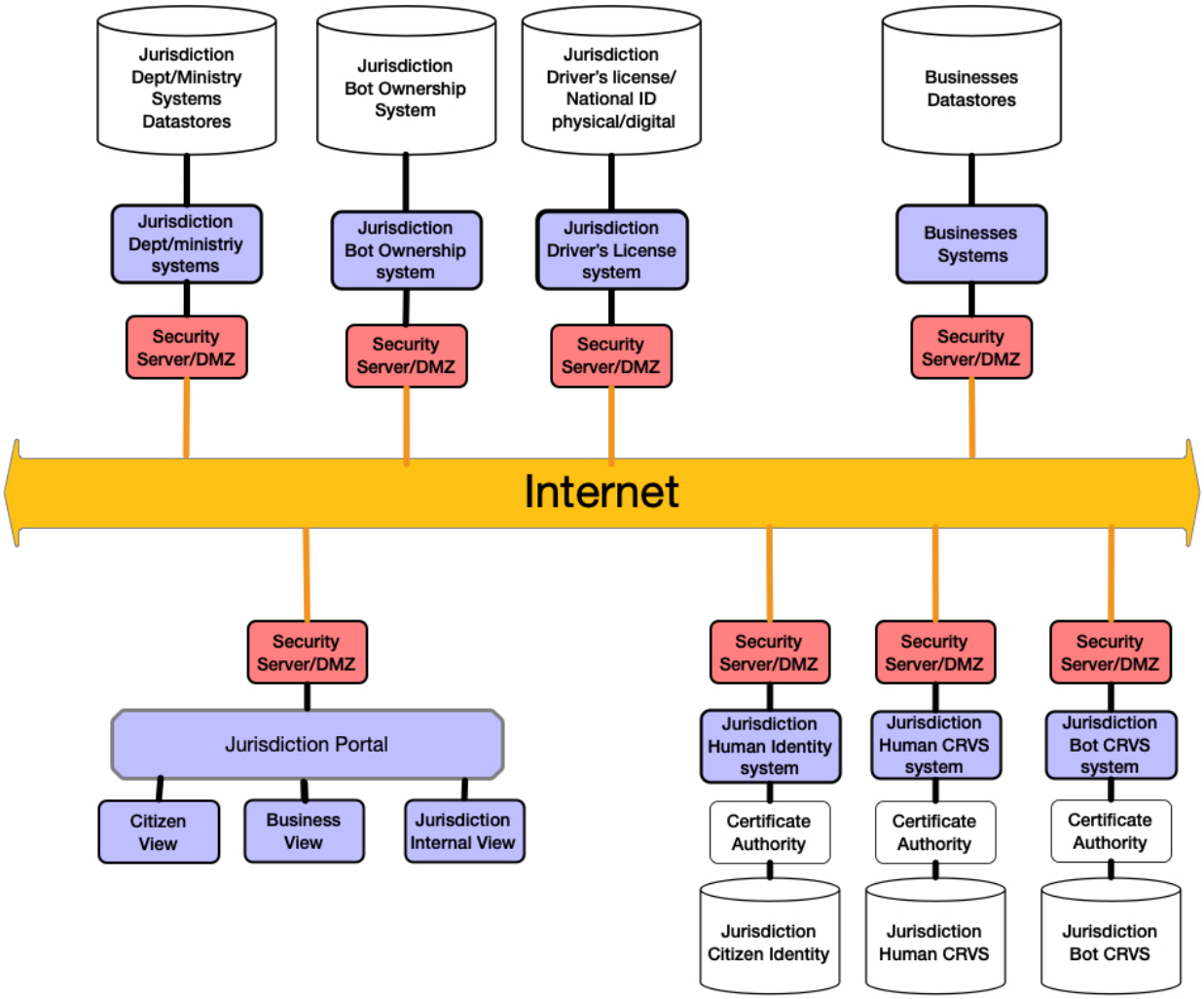
Citizens:

1. The proposed incremental system offers citizens the ability to use existing forms of legal human identification they're already familiar with, e.g. driver's licenses and national ID cards. Thus, any implementation of the solution will be readily understood by the users.
2. The proposal offers them control over their legal identity, both physically and digitally. Over time, they'll be able to use one form of legal identification for themselves, simplifying identification with businesses and jurisdictions.
3. The authors' believe the ability for a citizen to not only have control of their legal identity, BUT also control over displaying themselves anonymously, will be well received by citizens.
4. Further, we also think that having an ability to see who's a human and who's a bot in AI/AR/VR and online environments, will also be well received.
5. Citizens will want to be assured their legal identity, both physically and digitally is secure. Thus, the critical importance of the Red Teams is required, ensuring that any solution is secure.

Appendix C – Draft Architecture

Below is a preliminary draft human and bot legal identity architecture for a jurisdiction. It depicts the following:

- Jurisdiction:
  - CRVS (Civil Registration Vital Stats) systems for both humans and bots
    - These are able to issue private keys to citizens for CRVS events
    - Likely able to issue certificates for bots to be securely stored in their bot code (to be determined)
  - Separate jurisdiction citizen identity and authentication systems
    - Our premise is the CRVS should ONLY be used for identity verification and must not be a system able to identify and track people, e.g. address, etc.
    - The system would be fed updates from the CRVS when a CRVS event occurs to the citizen, e.g. marriage, death, name change, etc.
  - Driver's license system (both physical and digital)
    - This would be able to verify identities via the CRVS common protocol this paper presents in order to verify identities
    - When a CRVS event happens to a citizen, the CRVS would be able to write a private key to the citizen's driver's license
    - Enable citizens to anonymously legally prove they're a human and either above or below age of consent
  - Other jurisdiction systems
    - They would consume identities from the citizen identity and authentication system
- Businesses
  - They would be able to obtain legal citizen identities from the citizen via their driver's license (physical or digital)
  - If the identity verification risk is high, with the citizen's consent and also allowed by laws/regulations, they might be able to query the jurisdiction CRVS system
  - Able to determine if an entity they're dealing with is a human or a bot



Notes:

1. The Human CRVS system is:
   a. ONLY used for legal identity verification
   b. Able to write private keys for citizens onto their driver's license or national ID cards
   c. Able to communicate with other CRVS's to verify an identity (governed by laws)
   d. NOT able to store contact information for the citizen
2. The jurisdictions citizen identity system is:
   a. Separate from the CRVS BUT takes legal identity changes and reflects them in their system, e.g. death, name/gender change
   b. Might contain other identities for which the jurisdiction CRVS is not authoritative for, e.g. people who move in from another jurisdiction, work permits, etc.
   c. Might store citizen's contact information and/or be able to centrally authenticate a citizen
3. The ability for a jurisdiction to grant a citizen a digital signature, enabling them to use it so legally sign documents, could come from either the CRVS, or the jurisdiction's citizen identity system, or from some other system.
4. The Bot CRVS system is:
   a. ONLY used for bot legal identity verification
   b. Able to write private keys for bots
   c. Able to communicate with other CRVS's to verify a bot identity (governed by laws)

About the Authors

Guy Huntington

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."

Guy consults globally on the incoming technological tsunami wave of change. His main interest is in legally rethinking civil registration systems around the planet for legal human and bot identities. He's written 26 papers on this.

Michael Kleeman

Michael Kleeman is a technologist and strategist with more than 35 year's experience helping Fortune 500 firms, non-profits, and entrepreneurial startups globally overcome technical and business issues. He has held a variety of management and advisory roles, as a partner and senior advisor at the Boston Consulting Group, founder and advisor at Sprint and over a dozen communications firm, and as a senior advisor at Business for Social Responsibility (BSR). Mr. Kleeman is currently a senior fellow at the University of California San Diego where he works on identity and civil registration activities and is a leader of the team to develop the first accurate infant biometric device. He's also the director of the Institute for Global Production and Innovation (IGPI) which convenes researchers with multi-disciplinary expertise to study the impact of innovative production technologies on the world economy. Mr. Kleeman studied electrical and electronics engineering and psychology at Syracuse University, and he has a M.A. in Psychology from Claremont Graduate University