Guy's New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: December, 2018

TABLE OF CONTENTS

Note to Reader I

I have been writing about rethinking civil registration systems since 2006

- "The Challenges with Identity Verification"

Over the last several months, I have written 15 papers. Here's a listing of them, by subject area, with links to each one:

- Example story of an identity's lifecycle
  - The Identity Lifecycle of Jane Doe
- One-page summary
  - New Age Identity– Privacy in the Age of Human Clones & Robotics
- New laws required to do this
  - "Why We Need to Rethink Our Vital Stats Laws"
  - "Why Your Digital Consent Matters – Including Sex"
  - "Why We Need New Biometric Laws Protecting Our Privacy"
- What the new age civil registration/vital stats service does and doesn't do
  - "New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do"
- Leveraging Blockchain and Sovrin
  - **"**A Modern Identity Solution: New Age Vital Stats/Civil Registries, Self-Sovereign Identity, Blockchain, Kantara User Managed Access & EMP Resistant Data Centres"
- Protecting the civil registration/vital stats infrastructure
  - "When Our Legal Identity System Goes "Poof!"
- Separating vital stats services/databases from other identity authentication services
  - "Architecture Summary"
- Creating Estonia Version 2.0
  - "Creating Estonia Version 2.0 – Adjusting for Changes From 1999 to 2018"
- Rethinking identity assurance using new age vital stats
  - "New Age Identity Assurance – Turning it on its Head"
- Rethinking Civil Registrations in Remote Locations
  - "Where Shit Happens - Rethinking Civil Registrations in Remote Locations"
- New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision
  - "Guy's New Age Civil Registration/Vital Stats Design, Implementation & Maintenance Vision"
- Robotics, Clones and Identity
  - I'm Not a Robot
  - Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Privacy Principles

All papers are available off my website at http://www.hvl.net/papers.htm.

Note to Reader II:

What follows is my design, implementation and maintenance vision for a new age civil registration/vital stats system. As with any vision, when it hits reality many changes need to be taken. However, I feel compelled to lay out what my vision would be. Why?

It can:

- Provide the first set of "ground posts" by which to measure against participants, needs, resources, infrastructure, business processes, costs and timelines
- Assist in qualifying participants
    - i.e. it will solidify support from those who acknowledge the challenges and agree, in principle, to commit while, at the same time, might help scare off enterprises/people once they understand the type of commitment required
- Provide a document to begin discussions
- It offers potential enterprises something to use to get the ball rolling

Guy's Civil Registration/Vital Stats Design, Implementation and Maintenance Vision

Country Participants

As I see it, there are three potential patterns for a new age civil registration/vital stats deployment which countries can potentially participate in:

- One country
- Four countries meeting the geographical requirements to build and test out the biometric capture/data entry/telecommunications
- Countries in a trade area wanting to establish a common identity system

One Country

From a program management perspective, this is very desirable. Why? What is being proposed is very complicated with lots of different components requiring new:

- Research on biometrics
- Laws/regulations
- Business processes
- Technical infrastructure including biometric capture/data entry/telecommunications and EMP proof data centres, etc.

This requires LOTS of public, third-party and different levels of government consultation within the country. As well it also required constant communication between the design, implementation and maintenance team (hereafter in this document referred to as "The Team") and senior government leaders. Finally, if external Non-Government Organizations (NGO's) are used and/or third parties to develop laws, regulations and biometric capture/data entry/telecommunications devices then they too have to be part of "The Team".

Given this, there's a lot of reasons why this program can easily fall off the rails. Thus, having one willing country to do this, rather than have multiple countries involved, makes a lot of sense.

So, from a program management perspective, this is the optimal desired solution. It allows for reduction in complexity by having to work with multiple countries. Yet, for what it's worth, my gut feeling is that it would be better to have multiple countries involved. Why?

Four Countries Meeting the Geographical Requirements to Build and Test Out the Biometric Capture/Data Entry/Telecommunications

From a global deployment perspective, the paper "Where Shit Happens – Rethinking Civil Registrations in Remote Locations" lays out the requirements for a new device. From a technology perspective, this is one of the foundational pieces.

While it's possible to design the device for one country's deployment, it's better to have at least four different types of physical environments to design the device for:

- Hot
- Wet
- Cold
- Dry

For each of these, it would be even better if the locations had remote areas with no cell coverage, electrical supply and some cross-border people management issues with neighboring countries.

HOWEVER, while all of this is good from a technology design and implementation perspective, it multiplies the problems of why this program could easily fall off the rails and/or take much longer to roll out. Therefore, if this is the desired route, then the country participants MUST have stable governments, with leaders who are committed to this AND are willing to work interactively as part of "The Team" and other countries leaders.

Yet, there is a third option, which might be more desirable…

Countries in a Trade Area Wanting to Establish a Common Identity System

There are many parts of the planet where countries are in a common trade area. The free movement of people across borders results in increased trade between the trading partners and economic benefits. This requires an excellent, integrated, identity management system.

Many countries have issues with people crossing their borders illegally. As the paper "Where Shit Happens – Rethinking Civil Registrations in Remote Locations" lays out, simply solving the civil registration problem, internally within one country, doesn't solve all the identity problems. Why? People will cross borders illegally claiming to have been missed in a civil registration process.

Thus, it makes a lot of sense from a cross-border, economic and political perspective to implement a coordinated civil registration system. This means that trading partner countries agree to allow other trading partners the ability to present identities, claiming to have been missed in civil registrations, to the trading partners civil registration systems to see if they already exist.

It's my own view this type of deployment is better than the other two possible deployment patterns mentioned above. Why? It offers:

- Each trading partner's the ability to control their own civil registration system while securely integrating it with the other trading partner's civil registration systems
- The planet a working model where new age civil registration systems become the underlying identity platform used between trading partners

Hopefully, the trading partners have enough geographic and remote locations to suitably design, test and implement the biometric capture/data entry/telecommunications devices.

To make this type of implementation work, the trading partner's governments must be wholly committed to making the new age civil registration system work in a timely manner. The economic and political benefits will help keep the program on the rails as political, technical, legal and business process issues arise, between the trading partners, which need to be dealt with.

Governance, Legal Design and Implementation

The following papers lay out the high-level requirements for new laws/regulations:

- "Why We Need to Rethink Our Vital Stats Laws"
- "Why Your Digital Consent Matters – Including Sex"
- "Why We Need New Biometric Laws Protecting Our Privacy"

From a global perspective, it makes little sense for countries, on their own, to go through the high costs and time of assembling legal experts to do the research and then draft these laws and regulations. It makes much more sense to pay for the bulk of these costs once. Then have the laws/regulations in a "legal kit" form, such that other countries can quickly take this and them amend it to fit their requirements.

If readers agree with this approach, then the big question is who's going to pay for this component of "The Team"? Let's use the potential country participant deployment models to consider this:

- One Country
  - The country can find resources internally to pay for this and/or work in collaboration with external funding sources, e.g. NGO's
  - Once deployed, they could then offer the legislation in a kit package for a fee as part of services offered to other countries showing them how to successfully deploy a new age civil registration/vital stats service
    - Similar to what Estonia has done
  - The NGO's could make it a condition as part of their paying for the legal costs that the NGO retains the rights to distribute the resulting "legal kit" as they see fit to other countries
- Four countries
  - These four countries could fund the legal design and implementation costs on their own and/or work in collaboration with external funding sources, e.g. NGO's
    - The NGO's could make it a condition as part of their paying for the legal costs that the NGO retains the rights to distribute the resulting "legal kit" as they see fit to other countries
- Trading partners
  - The trading partners could fund the legal design and implementation costs on their own and/or work in collaboration with external funding sources, e.g. NGO's
    - The NGO's could make it a condition as part of their paying for the legal costs that the NGO retains the rights to distribute the resulting "legal kit" as they see fit to other countries

Time to implement is a major factor. Given this, I suggest that:

- Legal experts/firms contracted agree to enable work to occur around the clock
    - i.e. they have experts in various global locations to enable "The Team" to work in 24-hour periods
- The countries involved agree to meeting with each other and the legal experts as part of "The Team" around the clock
    - By this I mean that, if the legal experts and the countries are in different time zones, agreement is made that, on a rotating basis, meetings will be held in each of the country's time zones.
        - Thus, a country may attend a meeting during their day, then the next one occurs during their night, etc.
    - This ensures that time for design and implementation with the experts and any other country involved is kept to a reasonable length
    - Yes, I realize this is a big ask of countries and their administrators
        - It's been my experience that the governance component of programs/projects is the most critical as well as often the longest time requirement
        - Therefore, if countries want to keep the implementation times for a new age civil registration/vital stats system to a reasonable length, it's a fair ask to make

The next section discusses research required to confirm the use of infant biometrics obtained at birth. While this research is ongoing, I suggest that countries pilot the use of baby's fingerprints with laws prepared based on this as a pilot only, followed by all children having their iris scan during their first year of school.

If the research confirms baby fingerprints work long-term and, that fingerprints and iris scans are sufficient to differentiate human clones, then the country or countries can then implement changes to the new laws requiring this. If not, then modifications will have to be as to the type of biometrics to be obtained at birth.

Technology Design, Implementation & Maintenance

In almost all my past projects I first focus on governance, followed by business processes and then technology. Yet, since my civil registration/vital stats new age system heavily requires new technology to work and be maintained, long term, it becomes the second major piece of the "system puzzle".

Research

As laid out in the papers, research is required in the following areas:

Biometrics

- Confirm infant biometrics will be usable as the child turns into an adult
- Confirm that fingerprints and iris scans are enough to differentiate human clone 1, 2, 3 etc. from the rest of the population

Based on this the laws/regulations can then be fine-tuned as specified in the previous section.

EMP Proof Data Centres

Research should also be done to see if existing data centres can be modified to have EMP proof sections within them. I have no idea if this is possible at lower costs and time frames than building new data centres.

If it is possible, then the program plan should specify this as the first choice to rapidly implement in a country for their civil registration/vital stats biometric registrations. If not, then this cost centre and tasks should rise towards the top of the list to begin immediately, since there is likely long timelines and large costs associated with this.

Biometric Capture/Data Entry/Telecommunications Devices

This is another critical part of the program implementation. What I called out for in the paper "Where Shit Happens – Rethinking Civil Registrations in Remote Locations" is not trivial. Therefore, the right partners need to be assembled to create the use cases, design parameters, initial builds, testing, modification, retesting, etc. until the final design is created.

If countries and/or NGO's are paying for this, then the contracts must state that they co-own the intellectual property associated with this allowing for inexpensive licensing of the technology. Contrarily, if large commercial enterprises assume the risk and costs of building this, then the legal agreements need to be established protecting the countries from variable costs associated with the new devices.

It would be desirable if the partners doing the bulk of this work, were located around the world allowing for 24 cycles to occur in conjunction with "The Team". This would help mitigate against long timelines associated with this.

Biometric Readers Used by Different Levels of Governments and Third Parties to Confirm Higher Levels of Identity Assurance

In the paper "New Age Identity Assurance - Turning It On It's Head", I laid out that the identity has the highest level of assurance from birth. However, citizens won't be required to use this level of identity assurance unless required by law and/or risk at third parties. Given this, what are the biometric readers that will be supported?

Then there's challenges with the readers itself. In the paper "Why We Need New Biometric Laws Protecting Our Privacy" I state the potential problems associated with biometric spoofing. This is a moving target, since technology changes rapidly.

Taken together, the program implementation plan must lay out the initial testing to confirm the types of readers to be approved and then implemented. As well, it also needs to lay out processes for continual re-testing of the readers and, where defects/weaknesses are identified, the processes by which the old readers will be removed and replaced by new ones meeting the current standard.

Transmission/Endpoint Security

There will be frequent transmissions:

- Field registration devices to the central civil registration/vital stats system
- Different levels of government and third parties sending in biometrics to the central civil registration/vital stats system from biometric readers to be compared to existing biometrics in cases of higher identity assurance
- Countless people/enterprises wanting to ensure the digital signatures used by the civil registration/vital stats service are legitimate
- Different countries wanting to see if an existing person claiming they were missed in a registration process exists within another country's civil registration/vital stats system
- As well there will be transmission within the data centres and within the civil registration/vital stats system that need to be secure

Beyond the laws and regulations specifying what type of protocols (e.g. TLS 1.3, OpenID Connect, etc.) will be supported, very careful attention needs to be paid to designing, implementing and maintaining this. I always tell my teams that we will test, test and test before implementation and afterwards in maintenance mode.

Internal System Design and Administration

As the paper "Where Shit Happens – Rethinking Civil Registrations in Remote Locations" lays out, there are many different types of attack vectors, many of them within the civil registration/vital stats system. This includes all points the electrons travel through to reaching their final destination, admin privileges in viewing and/or editing data with reporting, audit and storage controls.

As the paper points out;
"A corrupt civil registration management will find ways to bypass internal and external control systems. Funding agencies, who are paying for a new age civil registration system to be implemented in developing countries, can design the civil registration's biometric readers, data collection/transmission devices, training, business processes, technical internal software processes and reporting processes to mitigate some of these risks."

Depending on who's funding the system AND the willingness of the countries involved to deploy a truly secure system, it affects the final design. Tests, tests and tests are required to ensure that the design is secure end to end. **The program plan MUST include independent penetration testing at all stages, i.e. design, implementation through various environments and maintenance.**

In the paper "Canada – We've an Identity Problem", I suggest the civil registration/vital stats security design be done in an open source type mode. By publishing the security design, it then enables wide-spread knowledge of the system with many people/enterprises testing out the design. This produces a stronger overall security system than one in which the security design is kept private. This runs counter to conventional practices.

Business Processes Design, Implementation and Maintenance

A new age civil registration/vital stats system cuts across almost all parts of a country's governance, business and social levels. The processes include but is not limited to:

- Registration/notification processes for birth, gender/name change, marriage and death
- Identity assurance processes including consent requirements for low levels of identity assurance, anonymous proof of identity, to higher levels of identity assurance
- Dispute resolution processes when claimed identities don't match registration via biometrics
- Etc.

There will be literally thousands of different business processes required to operate the system and to interact with it. Each one requires:

- Use cases
- Approved business processes for "happy path" and "unhappy paths"
- Documentation of potential attack vectors and mitigation measures
- Testing for each component of the process
- Training/education for each potential participant in the business process
- Approved processes for making any change to the existing process

The amount of work involved is very, very large, time consuming and potentially expensive. Attention to detail is very important to mitigate the risk of opening up potential security weaknesses.

The way the public and businesses are educated is also extremely important. Based on this, the public will judge the final system. The old adage "Caveat Emptor" applies. If the public finds greater ease of use and security, then they will approve. If not, it could spell political and/or economic trouble for the government.

Summary

I've led many large complicated identity projects and have also rescued some of them. As a result, this paper is the result of my experiences in doing so. As this paper repeatedly points out, there are a lot of reasons why this program could easily fall off the rails.

To mitigate against this requires:

- Continuous support from senior government leaders with "The Team"
- Strong cross-government, business and inter-government coordination
- Care must be taken to avoid what I call "silo-ization" of work and communication
    - This is the hardest task on a major identity project such as this
    - It's so easy for people to retreat within their domains, mis-communicate and then, at the last minute, realize the implementation won't work for them
- To avoid silo-ization requires the best "A team" the government and businesses can put together
- This requires strong, excellent leadership top-down as well as horizontally across the silos
    - For example, this means excellent participation by health care workers, government agencies, legal experts, businesses large and small and most citizens when the program is rolled out

The country's legal identity security rests upon the new age civil registration/vital stats system. Therefore, nothing should be rushed into in the design and implementation phases. Care and caution should be used at all stages of the program.

Attention to detail is paramount, for each business process and/or technical component is a potential attack vector. Therefore, senior levels of government and businesses need to be prepared to dive deeper into the "weeds" than the normal one- or two-page briefings they typically receive. The adage "the devil is in the details" applies.

If the program is well managed then participating countries can successfully lay the foundations for a new age economy for the next 100 years.

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."