Huntington Ventures Ltd.

The Business of Identity Management

New Age Identity Assurance: "Turning it on its Head"

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

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:

This paper addresses a new way of thinking about identity assurance starting from birth.

TABLE OF CONTENTS

Introduction

The recent Sovrin white paper "Sovrin™: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust" from January of this year, talks about technologies like Blockchain that "turns the centralized root of trust model on its head." Sovrin also does this by allowing for self-sovereign identity. This paper addresses an additional piece in the puzzle, identity assurance, which Sovrin and Blockchain don't address. It requires a new age approach. It's time we turned our old identity assurance ideas on its head too.

Old School Ways

Existing identity assurance models are built assuming that only the highest level of trust is when the identity has provided documents and verification techniques, including biometrics, to then grant the identity a high assurance level (usually 3 or 4 depending on what identity assurance scheme an enterprise is using).

At the heart of this are "foundational" documents that are then associated with the identity. One of the most common is birth certificates, social insurance numbers, drivers' licenses, passports, etc. As I have illustrated in previous papers[1][2], the birth certificate is often called a "breeder document" since, with it, one can then obtain most of the other documents. It is now easy to fraud.

Governments and financial institutions know this. So, they then build stronger levels of identity trust, i.e. assurance, by associating biometrics with the identity. This is usually done when the person reaches age of majority or their teens. That's why in Estonia, their Identity Documents Act, specifies the age as 15 when one must provide a variety of different biometrics.

However, this is like building foundations on top of quick soil. The underlying identity whom you are taking the biometrics from, may or may not be who they claim to be, i.e. Jane Doe. The biometrics simply ensure that no one else can claim to be Jane Doe BUT IS IT REALLY JANE DOE IN THE FIRST PLACE?

Then there are genetic twins and human clones. Genetic twins are rare, (about 3-4 per 1,000 births) so the frequency of this occurring hasn't been high on our identity assurance radar. Then along comes clones.

Chinese scientists announced earlier this year that they had successfully cloned monkeys. So, what was once thought of as science fiction is now on our doorstep. Our old school type documents can't verify these at birth, excepting giving them a piece of paper saying Jane Doe 1 and Jane Doe 2.

In summary, our old school identity assurance model is built on top of paper-based documents that don't actually tie the identity holding the document to the actual document. It may or may not be who they claim to be.

[1] http://hvl.net/pdf/New-Age-Vital-Stats-Services.pdf
[2] http://hvl.net/pdf/A%20Modern%20Identity%20Solution%20-%20July%202018.pdf

New School Ways

Every person should only have one physical identity. That identity should be highly verified at birth or, when a landed immigrant enters the country. In other papers I've written[3][4], I outline different biometrics that should be used for this (fingerprints and iris). I also propose that a person's parents' biometrics must also be linked to the identity from birth (fingerprints and iris). **Therefore, right from the "get-go", i.e. birth, a person has a level 4 identity assurance**.

Let's continue to turn identity assurance on its head by combing this with Sovrin identity, Blockchain and new laws for biometrics, vital stats and consent.

When the baby's birth has been registered, the parents or their legal guardians should be granted a digital attestation by the state/provincial identity verification service for their child. This attestation is digitally signed by the identity verification service. With it, by new laws, the parents/legal guardians also are granted the ability to manage the child's identity digitally. They can take the digital attestation and digitally sign it themselves. The parents/legal guardians can then present the attestation when it is required.

For example, they could immediately apply for health services for the new baby by presenting the identity verification service digital attestation. The health services would verify the issuer's claim (the attestation issued by the identity verification service) by looking up the identity verification service's public key on the blockchain. The health service would also use the same process with the parent's/legal guardian's signature. Assuming both are verified, health service now knows who the identity is (for reference refer to the decentralized identifiers (DID) section on page 10 of the Sovrin whitepaper for a discussion of this).

Note that in other papers, "New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do", I have recommended that digital attestations also be designed to be put on physical cards. Not all people will have access to digital technology and/or want to use it.

This works the same for this example, except that the parents would swipe their own card containing their swipe the card and then likely provide a 4-digit pin to verify themselves. The vital stats/civil registration digital attestation signature contained on the card would then be verified as well as confirming they are the parents/legal guardian. Then they would be able to swipe their child's card to verify the child's identity.

The state/province, with the parents'/legal guardian's consent, would also register Jane into a separate identity and authentication system using a similar process as above. This would be the repository for her address and contact information. Note that this is NOT part of the state/provincial identity verification system[5].

[3] http://hvl.net/pdf/New-Age-Vital-Stats-Services.pdf
[4] http://hvl.net/pdf/The-Challenges-With-Identity-Verification.pdf
[5] http://hvl.net/pdf/New-Age-Vital-Stats-Services.pdf

Let's say that Jane Doe is entering her first day of her first year of school. She has to be registered into the education system. So, her parents/legal guardians would provide their digital attestation for their identities, along with Jane's.

This might be the time that Jane's iris registration is obtained. The state will likely require Jane to provide her fingerprints (assuming that the work of Dr. Anil Jain and his team can be verified for obtaining baby's fingerprints).

Jane's grown up. Her parents/guardian no longer have control over her identity (excepting cases where she might be mentally incapable of this). She would likely go to the state/provincial identity verification office to provide some of her biometrics. Once this is verified, the state might take a facial recognition of her. They would then issue to Jane:

- a 4-digit pin with which she can use to digitally sign documents
    - in Estonia, the government issues a digital certificate to the citizen, which is often placed on their SIM card
    - Citizens then give themselves a 4-digit pin to legally sign documents using their digital certificate
    - This may or may not be used, depending on how Sovrin/Blockchain works in the future
- anonymous attestation
- anonymous attestation plus face
- an attestation giving her date of birth, location of the birth and parents plus photo

In the next sections, we'll see where these can be used.

Increased Risk

The identity verification service uses keys linked to their decentralized identifier on the blockchain to sign the claim so that it is tamper-evident and anyone who gets it can validate that it was issued by the state/provincial identity verification service.

Jane enters a bar. When the bar needs to see that you're of legal age, Jane can present the anonymous digital identity attestation from the state/provincial identity verification service and the bar can verify that it hasn't been changed, that the state/provincial identity verification service issued it to her, and she's the one presenting it. Everyone can use the blockchain to lookup decentralized identifiers and retrieve any associated public keys.

However, by Jane presenting the digital attestation to the bar, it doesn't mean it's actually Jane. Why not? Another person may have maliciously obtained her digital wallet, her private key and is masquerading as her. To mitigate this risk, Jane would be required to use the anonymous attestation plus digitally signed photo from the state/provincial identity verification service. The bar then physically matches up this with Jane at the door and lets her in.

Note that Jane's identity is never revealed. Gone are the days of using driver's licenses, etc. to validate our age.

Also note it seems likely that existing liquor/cigarette laws will need to be modified stipulating that an anonymous state/provincial identity verification attestation is required including facial photo digitally signed by the identity verification service.

High Risk

Let's say that Jane is wanting to open up a bank account. The risk is now higher. So, when Jane provides the bank with her state/provincial digitally signed attestation plus her photo, the bank might not accept this on its own. Why? A malicious person could have obtained Jane's digital wallet, her private key, be using a face mask and masquerading as her (refer to "Why We Need New Biometric Laws Protecting Our Privacy").

To mitigate this risk, the banking act might stipulate that Jane must also provide her biometrics. These are then securely sent to the state/provincial identity verification service, via federation.

Assuming they match, then, with Jane's consent, the bank might also federate with the state/provincial identity and authentication service to obtain her contact information.
Jane might also be required by law to digitally sign the bank account documents with her digital signature.

Identity Assurance for Robots Both Virtual and Physical

Robots, doing legal things on our behalf, or acting independently with legal implications, need identity and credential assurance. The paper "I'm Not a Robot" benchmarks current robotic industry development, while the paper "Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Privacy Principles" lays out suggested privacy principles new laws and regulations can be built upon.

The paper "The Identity Lifecycle of Jane Doe" illustrates these in the identity lifecycle of Jane Doe. Readers will note that Jane can create virtual and physical copies of herself both before and after reaching age of legal maturity. She may have one or many copies. Where they are acting on her behalf, they need to be registered for their identities in the new age civil registration system.

It's a Game Changer

The identity, from birth, has a very strong identity assurance. Their parents/legal guardians then have control over their child's identity and can use the digital attestation from the state/provincial identity verification service to apply for different services.

The citizen can act anonymously if they want to. They can even "live off the grid" by their choice. **HOWEVER, when they want to interact with government and/or financial services, there will be only one physical identity per citizen.**

The citizen, when they become of legal age, is in control of their identity. They can present anonymous attestations or an attestation providing their legal name, sex, parents, date, location of birth and photo. They can choose which to use and when, unless required by law.

The state/province stays mostly out of the way of the citizen and their identity. They provide the initial state/province identity verification service to legally verify a person and provide digital attestations which the citizen then uses. Unless there are:

- Changes to the parents, legal guardians, name change, gender change, marriage or death or,
- Laws like bank acts require a person to submit their biometrics or,
- A person's been arrested and they want to verify the identity or,
- A person has died and they want to confirm the identity

The identity verification service doesn't play a role in the life of the citizen. The citizen is in control of their identity attestations issued by the state/provincial identity service and decide when and how to use it.

This is a modern, new school way, of operating identity assurance in our digital, small world.

Summary

It's time to dispose of the old-school ways we have used to approach identity assurance. What worked in the 1900's no longer works as well today. By rethinking identity assurance i.e. turning our existing identity assurance "on its head", and leveraging Sovrin/Blockchain, we can change the way our economy works and reduce identity friction/fraud in our daily lives.

Appendix

I have written in other papers about some of the challenges with biometrics AND also about EMP events and the potential high-risk impact on the legal identity database[6][7]. I reference these here for readers who haven't read the other papers.

Biometrics Are Not All "Golden"

What I am proposing will substantially reduce identity fraud by linking the identity biometrically to the person. However, it doesn't mean that identity fraud will be eliminated. Why?
Each type of biometric has different equal error rates, i.e. where false acceptance = false rejection. Biometrics like DNA, fingerprints and retina scans have low rates which is why they are used for identity verification.
However, these are prone to attack by the readers used to obtain the biometrics. For example, in this paper "Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations" it documents how fingerprint readers can be spoofed. This paper in 2017 documents different techniques to foil biometric readers.
Thus, it is quite likely that over the coming years, government and financial institutions will play a cat and mouse game with organized crime, upgrading readers as new attacks are made. In the "Biometrics and Government" paper it calls out for independent institutions to continually test biometric readers and publish independent equal error rates.

Refer to "Why We Need New Biometric Laws Protecting Our Privacy".

New Consent Laws are Required

New laws are required regarding consent to address the following:

- Ability for a parent/legal guardian to act on behalf of their child using a digital consent and/or their physical card
- A citizen acting anonymously must grant their consent to the enterprise wanting to validate the digital signature
- A citizen granting enterprises the ability to verify their biometrics for high risk uses

Refer to "Why Your Digital Consent Matters – Including Sex".

New Vital Stats/Civil Registration Laws are Required

New vital stats/civil registration laws are required to enable what's been briefly outlined in this paper. Refer to "Why We Need to Rethink Vital Stats Laws."

[6] http://hvl.net/pdf/A%20Modern%20Identity%20Solution%20-%20July%202018.pdf
[7] http://hvl.net/pdf/New-Age-Vital-Stats-Services.pdf

A Major Technical "Gotcha" on the Horizon

As we digitize our identity verification, the self-management of our identity, establish shared ledgers and then manage our consent, the risk of losing this substantially rises, i.e. entire economies could be vulnerable. The common answer is the "cloud". That's one of the reasons that blockchain works. Yet, it might not. Why?

In 1859 there was an electro-magnetic pulse event called the "Carrington Event" which today, if it happened, would likely wipe out most of the servers in the cloud. Then in May 1921 another event called the "Railroad Storm" occurred. It wasn't as bad as the Carrington one was. If a Carrington event occurs again, then "poof!" goes the heart of the identity trust in the region/country/world, i.e. the "cloud" alone is not the solution for this.

While many enterprises will try to calculate the risk of such an event and decide if they should address it or not, the underlying identity data, e.g. vital stats, ledgers and consent, ABSOULTELY requires EMP resistant data centres. This allows us to legally recover from such an event. **However, in today's world, EMP resistant data centres are currently the exception rather than the norm.**

My premise is that governments and third parties building business cases for using these technologies MUST build into the costs EMP resistant data centres.

Refer to "When Our Legal Identity Trust System Goes "Poof!"

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."