A Modern Identity Solution:

New Age Vital Stats/Civil Registries, Self-Sovereign Identity, Blockchain, Kantara User Managed Access & EMP Resistant Data Centres

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

Note to Reader:

I have been writing about rethinking civil registration systems since 2006

- "The Challenges with Identity Verification"

Over the last several months, I have written 11 papers about:

- 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 – 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"

This paper addresses new ways of thinking about identity verification and new age vital stats/civil registration by leveraging Blockchain and Sovrin.

TABLE OF CONTENTS

Introduction

Phil Windley accurately explained the current online identity problems, earlier this year in a Computerworld article "How blockchain makes self-sovereign identities possible".

Quote:

- The proximity problem: when you're dealing with people at a distance, opportunities for fraud abound.
- The scale problem: online identity systems are based on business relationships and technical integrations to root trust authorities. All this is expensive and only done for high-value use cases.
- The flexibility problem: current identity systems are rigid, with fixed schema and use cases.
- The privacy problem: shared identifiers, like browser cookies, allow personal information to be accumulated and correlated behind our backs. Ongoing hacks convincingly show that big centralized stores of personal information are not safe.
- The consent problem: identity systems rely on universal identifiers like email addresses, phone numbers and even Social Security Numbers that make it easy for third parties to correlate behavior and keep tabs on people without their permission.

He then goes on to explain why technologies like blockchain and self-sovereign identity address this. I agree with everything he wrote except for one thing. **The digital attestations for legal identity rely upon an existing identity verification system that no longer works well.**

Existing legal identity verification is flawed

When an identity needs to be legally verified, it usually relies upon a government issued document or "attestation". Let's use Phil's example of a person walking into a bar where they have to show they are of legal age.

In this example, a driver's license is typically used. Why? It's something most individual have with them, i.e. it's portable AND it's issued by a state government. It also shows their date of birth on it, such that the bar can easily verify the age AND it has their picture on it.

In Phil's example "you can present the digital driver's license and the bar can verify that it hasn't been changed, that the DMV issued it to you, and you're the one presenting it. Everyone can use the blockchain to lookup decentralized identifiers and retrieve any associated public keys."

So, why is this flawed? It's flawed for three reasons:

- Easily forged:
  - The actual documentation required by the local government to issue you the driver's license relies upon old style documents like birth certificates, etc. Designed in the late 1800's in the UK, birth certificates were issued which were very hard to forge then. So, if you had a birth certificate in your possession, it was most likely you.
  - Today, in security circles, birth certificates are often called "breeder documents" since with them, one can then obtain a variety of different identity documents like driver's licenses, passports, etc.
  - **They are easily forged**
  - Therefore, the attestation that is sent relies upon "old-school" documents that might or might not be true in granting you the attestation in the first place
- Facial image recognition can be spoofed
  - Driver's licenses use facial recognition on the picture that's taken of you to verify it's you by comparing it to other pictures in their database
  - This technology worked well for decades
  - However, in today's world, it's now not that expensive to acquire face masks which can avoid detection
- It's not prepared for human clones
  - This was the stuff of science fiction in the 1900's
  - Then, along came Dolly the sheep in 1996 showing us that animals can be cloned
  - Earlier this year, Chinese scientists announced they had successfully cloned monkeys
  - So, the age of human cloning is now almost upon us
  - **Regardless of if this is legal or not, identity verification systems need to be able to differentiate one clone from another**

Identity fraud begins by laws for banking, health services, driver's licenses, etc. allowing a person to verify themselves using what is now considered weak identity verification. They are all mostly paper-based documents designed for the 1900's, i.e. "old school". So, while I like the concept of sovereign identity and Blockchain, the resulting systems rely for identity verification on weak technology when a legal identity is required. What's the solution?

A new age digital vital stats service

In 2005 I was considering the effects of fraud on existing vital stats services such as birth, name/gender change, marriage and death registries. I published a draft paper in January 2006 "The Challenges with Identity Verification" in which I suggested biometrics be linked to the vital stats registration identities from a citizen's birth through their entire life cycle. I took some flak from people saying that they didn't want "big brother" able to mess around with things like their DNA. **They were right**.

After spending 11 years contemplating this, I wrote a paper in Fall 2017 "Biometrics and Government" where I said that before anything could be done to rethink vital stats services, we first need to create new laws and regulations protecting our biometrics. In that paper, I laid out the underlying principles which the laws had to speak to.

In June of this year, I sat down and wrote out a paper "New Age Vital Statistics Services: What They Do and Don't Do". This paper lays out both the principles and practical examples of how a new age vital stats service should work.

Citizens must have the ability to:

- Have multiple personas
- Act anonymously if they want to
- "Live off the grid" if they so choose
- **However, when they interact with government services and/or financial ones, there should only be one physical identity per citizen**
- **Citizen's biometrics used for identity verification and/or authentication must be protected by new laws/regulations**
- With the arrival of the internet of things requiring consent and new protocols enabling citizens to centrally manage their consent across enterprises, it requires new laws protecting their consent including those where citizens provide their biometrics
- **New age vital statistics services need to be created where birth, name, gender change, marriage and death changes are tied to the identity biometrically**
- This requires new infrastructure requirements protecting the digital biometrics database from electro-magnetic pulses relied upon legally by business and governments
- Recent protocols should be leveraged allowing for businesses and government agencies to use identity federation to provide citizen biometrics, with their consent, to the state identity verification services and receive answers back

Note: I've recently updated the paper to include the use of sovereign identity/blockchain.

Now, let's revisit the bar example

A person obtains from the state/provincial new age identity verification service a digital attestation that they are of legal age. The attestation is tied biometrically to you, i.e. to obtain the attestation, you will have to provide the government identity verification service with biometrics that are then verified as you, upon which they then grant the attestation.

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.

The person enters the bar and presents the attestation. Quoting Phil but changing the driver's license DMV to the state/provincial identity verification service; "When the bar needs to see that you're of legal age, you can present the 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 you, and you're the one presenting it. Everyone can use the blockchain to lookup decentralized identifiers and retrieve any associated public keys."

Their identity is never revealed. Gone are the days of using driver's licenses, etc. to validate your age.

Use of Kantara user managed access

With the arrival of the "internet of things", my premise is that we will soon be providing our consent for hundreds of devices. This includes the use of self-sovereign identity. How can one manage consent across different enterprises, devices and applications? Answer – Kantara User Managed Access (UMA) and UMA Fed. It works across enterprise "silos" offering the user a centralized place to manage all their consents.

Last fall, while thinking about this, I realized that our existing laws/regulations were now falling behind protecting us with our consent. I wrote a paper addressing this "Citizen Consent and the Internet of Things".

The paper lays out Internet of Things Consent Principles, explaining each one in greater detail:

- End user consent must be required to use the device except those cases where it is mandated by laws and regulations.
- The chain of custody for consent must exist at all levels, i.e. from vendor through to final user or users based on risk and laws/regulations.
- The device, the system that controls it, and/or the identity management system the device is a part of must be able to use "User Managed Access" and also "OpenID Connect" protocols
    - It will also need to support emerging protocols such as blockchain and those pertaining to self-sovereign identity

- Any individual, government, or enterprise offering a centralized user consent service must be mandated by laws and regulations.
- Any consent management service must adhere to regulatory security best practices including identity and credential assurance, data storage and transmission as well as archival processes.
- Based on risk, the identity assurance and the credential assurance must be applied to obtain and/or transfer consent between the user and various enterprises and/or other Internet of Things devices.
    - This will likely need to be rethought with self-sovereign identity and blockchain
- Secure, delegated access of consent should be part of the device's consent management system.
- The user of a centralized consent management service should have the ability to transfer this service to other enterprises offering this service in a secure manner.
- When a user leaves a centralized consent management service, the service must securely store the data for a predetermined amount of time according to the timeframes set forth by laws and regulations.

UMA/UMA Fed will likely have to be adjusted to work well with self-sovereign identity as the protocols emerge.

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.

Summary

We are on the edge of a new age world where the citizen has:

- Control over their identity both physically and digitally
- Ability to act anonymously in certain situations
- Mange their consent

This paper lays out five additional requirements above and beyond what is currently being addressed by self-sovereign identity and blockchain to establish a modern identity system:

- New laws/regulations protecting a citizen's biometrics
- New age vital stats service
- New laws/regulations protecting citizen consent
- Integration with Kantara UMA/UMA Fed
- EMP resistant data centres

If we, in each of our governments and industries address this, we can build a whole new way to live where privacy is front and centre. We'll also build the requisite infrastructure able to withstand events that could otherwise paralyze governments, financial institutions, the economy and individuals.

Please contact me if you'd like to discuss this further.

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."