Huntington Ventures Ltd.
The Business of Identity Management

Creating Estonia Version 2.0 –

Adjusting for the Changes from 1999 to 2018

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

6262 Wellington Avenue, West Vancouver, BC, Canada V7W 2H4 Tel 780-289-2776 |
https://www.linkedin.com/in/ghuntington; http://www.hvl.net;

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 changes from when Estonia first introduced their ground-breaking identity architecture, in 1996, to today in 2018. It therefore proposes Estonia version 2.0 as a way to meet the new challenges.

TABLE OF CONTENTS

Executive Summary

This paper outlines the value that Estonia has offered its citizens by legislating in 1999 one physical identity per citizen. It then moves on to describe the differences between 2018 and 1999 from changes in science, protocols and fraud requiring a new updated model. The paper then outlines the required components for this new model.

It ends by describing the benefits:

- Citizens able to control their legal identity
- Governments and third parties relying on a high level of identity assurance to rapidly verify an identity
- Citizens able to centrally manage their consents with protection by laws and regulations
- Streamlining of government and third-party services
- Infrastructure that will survive an EMP event and allow for rapid identity recovery
- Rapid changes to underlying algorithms in the event they are breached or significantly weakened
- Allow citizens ways to provide their identity verification and authentication when they don't have smart phones
- Enable citizens to act anonymously

Introduction

In 1999 Estonia's GDP per capita was slightly over $4,000. They adopted one physical identity per citizen and digitized their economy resulting in a GDP per capita today of just under $20,000. It is commonly held up as an example of what developing countries should follow. However, the scientific, protocols and fraud landscape in 2018 is different than it was in 1999. This paper lays out a vision for "Estonia version 2" adjusting to the new realities for the world today.

2018 vs 1999

There are many differences between 2018 and 1999:

Scientific

- Early this year Chinese scientists announced they had successfully cloned monkeys. What was once thought as science fiction, i.e. human cloning, is now upon our doorstep
  - This means that identity verification systems, i.e. birth, name change, marriage, gender change and death registries need to adapt to differentiate human clone 1 from human clone 2 by tying the actual identity biometrically to the registration
  - This requires new laws to protect our biometrics
- Nanotechnology
  - The miniaturization of devices to almost molecular level has heralded the arrival of the "internet of things" (IoT). Everything from clothes we wear, food, medication, transportation, et al are becoming IoT devices
    - This means we will soon be managing our consent to hundreds of different IoT devices across different enterprises, platforms and applications requiring new protocols and laws
- Artificial intelligence (Robotics both virtual and physical)
  - With Moore's law still holding (i.e. each year the power of computing doubles), computers are now so powerful they are beginning to replace people who have jobs. This ranges from low technology jobs to high end jobs
    - This means that economies can't be built by modeling on other countries that have been historically successful
    - It also means that we need a new age identity framework that can differentiate humans, clones and robots both virtual and physical

Protocols

There are a number of new protocols that didn't exist in 1999. They are contributing to rapid changes in how business, governments and people interact. They include:

- Open ID Connect
  - A modern identity federation protocol used by over 1 billion people/day
- TLS 1.3
  - The most recent protocol used to protect data transmission on the internet
- OAUTH Framework
  - A framework for authorization
- Kantara UMA/UMA Fed
  - A new protocol offering citizens the ability to centrally manage their consent across many different enterprises
- SCIM
  - A protocol allowing for different enterprises to securely share identity information
- Self-Sovereign Identity
  - Protocols allowing one to store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data
  - Sovrin
  - Uport
  - Veres One
- Blockchain
  - A growing list of records, called blocks, which are linked using cryptography and are readable by the public

Fraud

Technology developments, adoption of the internet and the ability to deploy malware upon computers has resulted in the following:

- Easy identity fraud
  - Almost all identity assurance around the world still relies upon paper-based identity verification documents like birth certificates, etc. The price point to fraud these is now low with birth certificates frequently called "breeder documents"
- Masquerading as another
  - Facial recognition has been used for decades on things like driver's licenses. Additionally, different types of biometrics are now frequently built into smart phones and tablets to authenticate a person. All of these are prone to advances in masquerading as another biometrically either in person or remotely
- Encryption
  - Some encryption algorithms used in the late 1990's is now no longer secure and have been "deprecated". Additionally, some security professionals suspect that other algorithms have "backdoors" allowing for security agencies/criminal gangs access to what's encrypted

Estonia Version 2 Requirements

What Estonia did in 1999 was to create an identity documents act that required citizens, at the age of 15, to provide biometrics. This doesn't address the age of human cloning and being able to differentiate clone 1 from clone 2 at birth, nor the ability to easily produce fraudulent birth certificates. Therefore, the starting point for Estonia Version 2, is to create a new age vital stats service (i.e. birth, name change, gender change, marriage and death registry) where the identity is tied to the registration using biometrics, starting at birth.

One Physical Identity per Citizen - New Age Vital Stats/Civil Registration Service

To achieve this in today's age it requires:

- New laws and regulations protecting a citizen's biometrics:
  - Refer to "Why We Need New Biometric Laws Protecting Our Privacy"
- New laws and regulations protecting a citizen's consent
  - :Refer to "Why Your Digital Consent Matters – Including Sex"
- New laws and regulations pertaining to new age vital stats/civil registration service
  - Refer to "Why We Need to Rethink Our Vital Stats Laws"
- New age vital stats service (birth, name change, gender change, marriage and death registry)
  - Refer to "New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do"
  - "New Age Identity Assurance: Turning it Upon It's Head"
- By doing what the above papers recommend, it allows citizen to be in control of their identity
  - The identity verification service can work with:
    - "traditional identity verification cards" allowing citizens who don't use smartphones the ability to attest to their identity and to digitally sign documents
    - "Smart phones" leveraging digital attestations using Sovrin and Blockchain
    - Identity federation with government agencies and third parties to securely submit citizen biometrics, as and when required, to verify a citizen's identity using OpenID Connect

Streamline Government Services Leveraging the New Age Vital Stats/Civil Registration Service and Consent

- Change acts and regulations pertaining to identity verification requirements required to obtain government documents like driver's licenses, passports, tax, social and health services such that they use the digital attestations and, where required, obtain biometrics to then verify the citizen's identity
    - "Why We Need to Rethink Our Vital Stats Laws"
- Leverage the ability of citizens to digitally sign government documents as and when required
- Offer citizens an optional identity authentication and contact service
    - Citizens can voluntarily join, except where required by law, to centrally manage their identity contact information. With their consent, using Kantara UMA/UMA Fed, any changes to their contact information is then sent to other government agencies using SCIM

Streamline Third Party Services Leverage the New Age Vital Stats Service and Consent

- Change acts and regulations pertaining to identity verification requirements required to open bank accounts, telephone accounts, insurance, etc. such that they use the digital attestations and, where required, obtain biometrics to then verify the citizen's identity
- Leverage the ability of citizens to digitally sign third party documents as and when required
- Offer citizens an optional identity authentication and contact service
    - With their consent, using Kantara UMA/UMA Fed, any changes to their contact information is then sent to specified third parties, like banks, telcos, etc. using SCIM

Adjusting for Legal Identities of Robots Both Virtual and Physical

The new age civil registration system needs to adjust for creating and managing legal identities of robots, both virtual and real. The paper "I'm Not A Robot" outlines current benchmarks for this technology, while the paper "Legal Person: Humans, Clones, Virtual and Physical AI Robotics – New Privacy Principles" lays out suggested privacy principles new laws need to be built upon. The paper "The Identity Lifecycle of Jane Doe" illustrates the application of this for the lifecycle of an identity, Jane Doe.

Create Infrastructure That Will Survive an EMP Event

The danger in digitizing identity is that an electromagnetic pulse (EMP) event like the "Carrington Event" or "Railroad Storm" events can wipe out most servers on the planet. When recovery begins post EMP event, one of the first things is to verify you are you. If the digital citizen biometric identity database is destroyed, then this will be impossible to do. Thus, as the papers already referenced above recommend, the identity servers need to be housed in EMP proof data centres.

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

Integrate e-Governance and e-Voting with the Identity Verification Services

Once the identity verification infrastructure is in place, all e-governance services should be integrated to use the same identity verified by the state identity verification service. Everything from e-school, e-pharmacy, e-health, e-tax, e-voting, etc. should be leveraging the same citizen identity.

Complete the Citizen Lifecycle by Integrating Death Services with Automatic Notification

When a citizen dies, their identity needs to be physically verified by the biometrics. Once confirmed all government services should be automatically notified using SCIM. As well, depending on laws and regulations, third parties should also be notified. This stops the ability for others to masquerade as another using a dead citizen's identity.

Use Algorithms That Are Secure AND be Prepared to Rapidly Change Them

To mitigate against the risk of weak encryption/digital signing, governments and third parties should use published algorithms that are secure and have no suspected back doors. Governance processes should be in place that if an algorithm breach is detected and/or the algorithm is weakened, then other algorithms should be rapidly integrated.

Allow Citizens Ways to Provide Their Identity Verification and Authentication When They Don't Have Smart Phones

In many countries, citizens don't have smart phones because they are unable to afford the data packages or, they choose to not use the technology. The Estonia 2 vision offers services for these types of citizens.

An ID card or driver's license can be provisioned with the digitally issued government certificate allowing them to digitally sign documents via a card reader plus their 4-digit pin. As well, the card can contain the digitally signed attestations by the identity verification service. Thus, a citizen can choose to use these when they want to access services.

For those citizens who have access to a cell phone, they can optionally choose to register with the government identity and authentication service at a government approved office. The registration process includes them providing their biometrics to verify their identity and, once confirmed, providing their voice biometric plus selecting a 4-digit pin.

When the citizen wants to access low risk government services, they will authenticate using their voice. As the risk rises, they should then be prompted for a 4-digit pin. For high risk services the citizen will have to go to a government office to verify themselves by either presenting their digital identification card plus offering their consent to provide biometrics.

Third parties, i.e. businesses, can leverage the service by federating with the government identity and authentication service using OpenID Connect.

Many citizens use cell phone e-wallets. The optional identity and verification service with voice authentication and a 4-digit pin can be used with OpenID Connect, OAuth and Kantara UMA/UMA Fed to obtain their consent to pay for government and third-party services.

The citizen user experience should be seamless as they acquire smart phones and data packages. Thus, they can continue to use their voice plus a 4-digit pin. They now can place the digital identity attestations digitally signed by the identity verification service on their smart phones and use them as they choose to.

Enable Citizens to Have the Ability to Act Anonymously

- Anonymous identity verification when the identity requires it, with the citizen's consent
    - e.g. you're going into a bar and the bar wants to attest you are over the legal age requirement
- Option 1:
    - You'd swipe your finger at the door, or present an iris scan. The scan would then be securely sent to the registry and it would come back with a yes or no
    - i.e. your identity is never released
- Option 2:
    - You provide a digital attestation from the vital stats service, via Soverin/Blockchain that anonymously attests to who you are
    - i.e. your identity is never released
    - For more information refer to:
        - "New Age Identity Assurance – Turning it Upon its Head"
        - "A Modern Identity Solution - New Age Vital Stats, Self-Sovereign Identity, Blockchain, Kantara User Managed Access & EMP Resistant Data Centres"

- Option 3:
  - You present a physical card from vital stats/civil registration service that only has your photo on it
    - This photo is digitally signed by vital stats/civil registration service when you come of legal age
    - The bar electronically verified the signature by vital stats/civil registration and then lets you in

Summary

The world in 2018 is very different than in 1999 when Estonia pioneered the way by implementing one physical identity per citizen. By adopting the recommendations of this paper enables the following benefits:

- Citizens able to control their legal identity
- Governments and third parties relying on a high level of identity assurance to rapidly verify an identity
- Citizens able to centrally manage their consents with protection by laws and regulations
- Streamlining of government and third-party services
- Infrastructure that will survive an EMP event and allow for rapid identity recovery
- Rapid changes to underlying algorithms in the event they are breached or significantly weakened
- Allow citizens ways to provide their identity verification and authentication when they don't have smart phones
- Enable citizens to have the ability to act anonymously

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."