Huntington Ventures Ltd.
The Business of Identity Management

Architecture Summary

Copyright: 123RF Stock Photo

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 is an architectural summary of the various papers.

TABLE OF CONTENTS

Architecture Summary

Over the last not quite four years, I've been making presentations and writing papers on a new way of looking at identity verification plus a separate government identity and authentication service. For readers wanting a high-level summary, here it is…

Laws/regulations:

New laws and regulations pertaining to:

- Biometrics
  - (refer to "Why We Need New Biometric Laws Protecting Our Privacy" paper)
- Consent
  - (refer to "Why Your Digital Consent Matters – Including Sex" paper)
- New age vital stats service
  - (refer to "New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do" paper)

Biometrics:

- Conduct research on babies to see if the work of Dr. Anil Jain holds over several years
  - Begin doing pilots with babies fingerprints
- Obtain iris scans of children in their first year of school
- Do research to determine if fingerprints and iris scans are enough to differentiate human clone 1 and 2 from the rest of the population
  - For reference, refer to the recommendation section in the paper "Canada – We've an Identity Problem"

Identity Assurance:

- Change the country's identity assurance such that citizens have the highest assurance right from birth or, when they become landed immigrants
  - (Refer to" New Age Identity Assurance: -"Turning it on its Head" paper)

Vital Stats/Civil Registation (Birth, Name/Gender Change, Marriage and Death Registry):

- Create a separate vital stats service/network from other government identity and authentication databases which will contain contact information (similar to the one I helped create for the Government of Alberta)
- Store the biometric data against the citizen's birth registry or, their landed immigrant entry into the new age vital stats service
- Data only goes in and never comes out
- Use Blockchain/Sovrin to sign digital attestations from the vital stats service about an identity
  - Refer to "A Modern Identity Solution" paper
- Allow for physical vital stats cards to also be used when the citizen doesn't have access to the technology and/or doesn't want to use it
- When a citizen comes of age, they will present themselves to the vital stats service, present biometrics to confirm who they are and have their photo taken
  - The vital stats service will then digitally sign the photo

    - The citizen will be given two digital claims
        - One is an anonymous claim with their photo
        - The other is the birth certificate information
    - The citizen is now in control of how and where they use these claims, excepting where required by law
- When a person dies, biometrics, if obtainable, will be used to confirm the death identification
- The service will use TLS1.3 to communicate with biometric readers
- Biometric readers must be approved by vital stats before any third party or government agency uses this to collect a biometric and send it to the vital stats service for identity verification
    - Refer to "New Age Vital Statistics/Civil Registration Services: What They Do and Don't Do" paper

Government Identity and Authentication Service:

- This should be either voluntary or required by law when the citizen wants to access government services
- The citizen will register with the service using their vital stats claims
    - Children can be registered by their parents who have legal consent to do this
- Voice will be one of the authentication methods used
    - This allows citizens to use technology they have in their pockets, e.g. a cell phone to interact with government services
        - As risk rises, they also might have to enter a 4-digit pin
- Open source identity and access management software will be used
- The service will use OpenID Connect, Oauth2, SCIM, TLS 1.3 and BPEL
- Citizens will have the choice whether or not to have the service send out contact information changes to other government agencies and/or third parties excepting those required by law
- Refer to https://www.slideshare.net/ghuntington/overview-of-my-various-national-ict-strategy-presentations for an overview of what we've been proposing for the last few years

Infrastructure:

- Vital stats:
    - The vital stats service needs to be run in EMP proof data centre
    - All endpoints must be hardened and continuously tested
    - The service must be available, at 99.999% availability
    - Internal processes need to be in place and continually tested regarding admin access and/or changes to the underlying data
    - Audit and reporting needs to be secure and activated depending on admin actions

- Citizen Identity and Authentication services
    - It's likely, but not mandatory, that these services should also be in EMP proof data centres
    - All endpoints must be hardened and continuously tested
    - The service must be available, at 99.999% availability
    - Internal processes need to be in place and continually tested regarding admin access and/or changes to the underlying data
    - Audit and reporting needs to be secure and activated depending on admin actions
- For EMP references refer to "When Our Legal Identity Trust 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."