

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

THE CHALLENGES WITH IDENTITY VERIFICATION

PROBLEM

“How does one verify a physical person?”

INTRODUCTION

As an identity management consultant, I am always wrestling with identity verification i.e. matching up an individual to their true legal identity. While there is much fascinating work going on in the area of digital identities/personas and identity federation, my own feeling is that the underlying mechanisms of linking a real person to their legally defined identity is very weak.

The stopping of using social security numbers in employer data stores, which was a poor attempt at matching a person to a government approved identity, has made the situation even worse. Now enterprises are scrambling trying to obey the law yet having very weak identity verification information. The question that most often goes unanswered or unchecked is “how do you know the person standing in front of you is who they claim to be?”

I have thought lots about this problem. As a result, in this paper, I will deal with the challenges of verifying a physical person and propose a solution to the current problems. There needs to be a globally recognized way, legally approved by governments, to verify the identity of each of their citizens which also protects the individual’s identity privacy. What I have proposed could be the foundational building block for doing this.

I welcome your comments, criticisms and suggestions.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

BACKGROUND

During the last six hundred years, governments have dealt with verification of physical people. Birth, marriage and death registries were established attesting that a person entered the world, their name, whom their marriage partner was, their children and when they died. National census was developed in order to count the individuals living in a country recording the names and addresses of each individual. Passports were also developed to identify people moving between countries.

During the last one hundred years, further forms of identifying individuals were developed. These include social security numbers and driver licenses. Internally within governments, tax numbers were also assigned to individuals as a way to identify a person.

As the movement of people increased, business and legal requirements developed requiring tokens of these identity verification systems e.g. drivers license. Merchants and governments developed systems recognizing these tokens. It became common for individuals to carry with them these tokens and to use them in dealing with merchants, prospective employers and government officers such as police.

The justice systems in many countries have been evolving ways of better identifying a person physically. The need for this arose when the tokens could be relatively easily counterfeited and/or where an individual needed to be identified without identity tokens.

These systems used physical identification. Fingerprints have now been supplemented by DNA and the evolution of other biometric systems such as retina scans. However, these systems are only used in special cases such as for convicted criminals, establishing the physical presence of a person at a crime scene, and in instances when an identity is checked against a pre-established data store that the individual has normally consented to be in e.g. a retina scan for customs clearance. There is no common data store for all individuals living in the country against which these methods can verify the individual to.

Over the last fifty years commercial tokens were also developed attesting to an identity. Credit cards are now common ways, in developed countries, of identifying to a merchant the identity of an individual. However, these tokens also can be counterfeited and/or stolen and used by others masquerading as the identity. Credit cards developed hand written signatures as additional verification for the merchant of an identity. However, these means are relatively easily bypassed through forgery by the person masquerading or failure of the merchant to check the signatures while the individual is at the cash register.

The rapid movement of people via modern transportation systems has increased the challenge of verification of physical identities. Immigration, customs and police officers are now trying to keep track of the movements of hundred of millions of people or more. Merchants are also trying to identify a person standing in front of them claiming to be someone and carrying a commercial token attesting to their credit worthiness.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

During the last ten years, “identity theft” has increased. This is due to criminals being able to obtain identities via “dumpster diving” all the way through to hacking into government and commercial identity data stores. As a result states and nations have developed laws attempting to protect the “identity” of an individual. The use of social security numbers is now generally restricted. Passing data on the identities between commercial entities and between governments is now restricted to varying degrees in certain countries.

The challenge of verifying an identity has increased even more for multi-nationals operating in hundreds of different countries. How does a company know that a prospective worker is who they say they are and then verify it? Most nations don’t have birth data stores available on line to verify an identity. The social security number may or may not be searchable. Passports in some countries are relatively easily forgeable. Many financial institutions do some kind of criminal background check which is only as good as the data store which they are checking against (and which in many countries is not online, poorly kept up to date or fragmented in localities).

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

CHALLENGES

Today, the challenges of verifying an identity of a person standing in front of you are:

1. Verifying existing physical tokens the person presents to you.
2. Verifying with recognized legal data stores the identity.
3. Verifying the physical identity as separate from another individual.

The needs for authenticity in the above vary based on commercial risk and legal requirements. For example, a store clerk may only require seeing a driver’s license or birth certificate to verify the age of someone wanting to make a liquor purchase where age regulations apply. The clerk may only care that you have the token to present and that it “looks” reasonable. The state however may care that the token is legitimate and that the individual carrying the token has not obtained it fraudulently.

A bank manager will need more identity verification in order to create a bank account. This can include social security number, local address, driver’s license, employer’s name and birth certificate. They may also ask for commercial token information such as credit cards which is likely to be checked by the bank depending on the risk to the bank of potential transactions.

An immigration officer will need to see a passport as well as ask personal questions before allowing a person into their country. Based on this, they may be able to see other information about the individual from the immigration officer’s country’s data stores or, perhaps from other countries.

All of the above rely upon national or state government issued tokens. The issuance of birth, marriage and death certificates is the underlying basis for most other physical identity verification systems. There are a number of challenges with the current birth and marriage certificate systems:

1. People now frequently move around the world. This is causing challenges with governments and commercial institutions trying to verify a birth or marriage certificate the person is presenting.
2. It does not necessarily tie an individual to the person standing in front of you. The reason is the actual certificate being presented is tied to forms submitted to a recording institution. The person signing the form makes an attestation that the information is correct and accurate. Thus a medical doctor or hospital or parent or government official may make an attestation that the person named “Guy Huntington” was actually born on July 26, 1957 in Calgary, Canada.

It is the supposition of the token that the person signing the form actually saw and/or witnessed the birth of Guy. There is no information within the birth certificate of Guy Huntington actually linking Guy Huntington to the token other than he is holding it and presenting it to you. There is no information within the

Author – Guy Huntington, Huntington Ventures Ltd.

guy.huntington@hvl.net, www.hvl.net

Date: January 11, 2006

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

Government of Alberta’s birth registry actually linking the physical Guy Huntington to the entry. It is based off of forms, which in turn is based on the attestations of the people signing the forms.

The premise of this paper is that the current birth and marriage paper certificates, as they currently exist are no longer adequate for today’s identification challenges. Why?

1. “Forge-ability” – The paper certificates can be easily forged. The ease of doing this has increased over the last several years. The reason it’s now a problem is that many government and commercial institutions rely upon presentation of this token with which they then create their own tokens, many of them used digitally. The challenge is that most of these institutions don’t or can’t do searches on the birth or marriage registry to verify the identity. Thus the digital identities may be fraudulent.
2. “Silo-ized” registry data stores – Normally each state and/or city maintains its own birth and marriage registry. The challenge is in communicating with and paying for a search to be done in a timely manner.
3. Notification – Currently, the searching of a birth or marriage certificate is open to anyone with no notification to the identity that their birth or marriage certificate is being searched. In some instances, individuals may want to authorize a search to be made verifying their identity or perhaps refuse the search to be done protecting their identity privacy.
4. Lack of tying the identity to the birth, marriage or death certificate. The certificate is only a token. It does not tie the bearer to the actual token other than having it in their possession.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

SOLUTION

This paper presents the following suggestions for change.

1. A biological sample of the person be taken at birth and used for DNA identification. Currently, this is the best scientific means of determining the identity of an individual.
2. The biological sample be analyzed and converted into a DNA digitization.
3. The DNA digitized sample is securely stored in government approved national identity data warehouse while the physical sample is destroyed.
4. Very strict laws and regulations be developed protecting the government identity data warehouse. At no times should the digital DNA be ever released or transferred out of the government identity data warehouse. The digitized DNA portion of the identity data should only be used for identity verification within the national identity data warehouse.
5. Identity search notification – A person whose identity is being searched must have the option of being notified requesting their authorization for their identity to be searched. If the person is unavailable for notification or, incapable of giving approval, then legal approval needs to be given to have the search done. This information needs to be stored in the national identity data warehouse. The identity being searched should have the right to a report at any time on who has searched their identity, when this occurred and, if approved legally by others, who this was.
6. Search-ability – Other government and commercial institutions should be able to have searches done on the identity data warehouse, with the written or digitally signed consent of the person whose identity is being searched. The way a search would be done is as per the following example:

Say you are applying for a driver’s license or marriage certificate. You would either provide the state with a sample of your DNA to be tested or, go to a government approved DNA testing organization. They would take a biological sample from you to do the DNA testing with and, by law, destroy the sample immediately after testing. They in turn would digitize the sample, take the digitized DNA sample, encrypt it and securely send it to the national identity data warehouse.

There the incoming digitized sample would be compared to the digitized DNA sample taken at your birth. If the national identity data warehouse matches to the proposed identity, then the national identity data warehouse would securely send a digitally signed statement attesting to the verification. This digitally signed

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

search result would then be hashed by the state driver’s license authority and then digitally enclosed in your driver’s license. The state would destroy their digitized version of the DNA sample after receiving the results from the national identity data warehouse.

The driver’s license then could be read by digital readers with the ability to unhash the driver’s license and see the verification of your identity. In order to do so, you must provide the encryption routine to unhash the identity on the driver’s license.

In instances where the person is incapable of giving permission or incapable of providing the encryption routine to dehash the identity verification, then legal processes must be used to do so. These processes must then be recorded in the national identity data warehouse and be made available to the identity at any time they request it.

7. The same process as above would apply for a death certificate. In this case the coroner would take a biological sample of the dead person, do a DNA test on it, securely send the digitized DNA sample to the national identity data warehouse, confirm it is the person, obtain a digitally signed copy of the search result and digitally insert this into the death certificate.
8. Your own birth certificate – You would receive a birth certificate with a digitally signed attestation by the national identity data warehouse of the date the entry was made into the data warehouse.

The birth certificate would allow your legal guardians the ability to unencrypt the signed attestation when they are using the birth certificate to apply for other government documents on your behalf. At the legal age of consent, the national data warehouse would revoke the privileges for the legal guardian to unhash the attestation and pass those privileges to the person whose birth certificate it belongs to.

9. Immigrants – Immigrants should use the birth registry of their home country with similar operations as described above. For those whose country lacks a national identity data warehouse, they would then apply to be inserted into the national identity data warehouse in the country to which they are immigrating.

After suitable background checks, their DNA should be taken and then a digitized sample inserted into the national identity data warehouse, their DNA sample destroyed and a national identity card being given to them. The national identity card would have the same features as the birth certificate with the ability to have a hashed digitally signed copy from the national identity data warehouse attesting to their identity within the card. The immigrants would have the rights to decrypt the hash on their card.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

10. Ability of the national identity data warehouse to do a one to many search – Any new entries must have the ability to have a one to many DNA search done within the national identity data warehouse. This will prevent the use of human clones in the future.

This system has the following features:

- Provides a way to tie the individual physically to an identity token
- Secure the storage of the digitized DNA without ever transmitting the original digitized DNA contained in the national identity data warehouse
 - Enquires can come in with digitized DNA samples securely sent for searching but no digitized DNA from the original sample is ever sent out
- By law require all DNA samples to be immediately destroyed after testing – this will become important in years to come as cloning becomes possible
- Puts control over the identity in the hands of the identity token holder
 - They can chose who they will allow to decrypt the identity attestations of the national identity data warehouse to
 - They can receive notification and/or reports over who has accessed their identity in the national identity data warehouse and when this occurred
- Still provides physical tokens e.g. birth certificates, marriage certificates, driver’s licenses or death certificates
 - The tokens can be used to provide age authenticity
 - Has the ability to provide the birth verification from the national identity data warehouse with approval of the token holder e.g. on their birth certificate, marriage certificate or a driver’s license

Employers, merchants and financial institutions may chose to continue by accepting traditional information from the identity or by requesting the identity to agree to a search of their identity in the national identity data warehouse. For commercial or employer identity requests to the national identity data warehouse, the laws should be explicit that:

- DNA sample be done by a government approved institution
- DNA test be prior approved by the identity
- Physical sample be destroyed after testing
- DNA digitized sample be destroyed as well. The digitized DNA sample by law should not be able to be stored in the commercial or employer database. What can be stored is the digitally signed attestation by the national identity warehouse confirming the identification.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

This solution addresses the existing problems with respect to identifying individuals to a token. It eliminates the need for use of social security numbers as a way to tie an individual to a government approved identity. Rather than use government numbers which are widely used in other sensitive data stores, a government digitally signed attestation is used. If someone steals your birth or marriage certificates, the damage can be contained since you still hold the encryption routine to decrypt the hash of the attestation.

This also sets the stage for digital identities where some kind of legal verification of the identity is required. Centralized digital identity repositories, be they government or commercial, may use the digitally signed identity attestation of the national identity data warehouse (with the user’s consent in advance) as the underlying verification of the identity to a legally defined real person.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

CONCLUSION

Current challenges in implementing the proposed solution include:

- Legal law changes at state, national and international levels
- Regulatory standardization at state and national levels on birth data
- Deciding on how to digitize DNA samples in a standard way
- Size of the digitized DNA sample files
- Search algorithms to do a digitized DNA search
- Computing power required to do a one to many search on hundreds of millions or more of digitized DNA samples
- Creating government approved DNA testing laboratories
- Reducing the costs and times for doing DNA tests
- Costs of issuing new birth marriage and death certificates containing digitally signed attestations from the national identity data warehouse
- Regulatory checks on commercial and government identity data warehouse stores to ensure no DNA digitized samples are kept
- Security around the national identity data warehouse
- Providing high-availability of the national identity data warehouse

Some of these challenges are large i.e. standardizing how DNA will be digitized, the search algorithms and computing power to do a one to many search. It is the author’s own personal belief that these challenges are addressable under a national and international framework.

The solution proposed is not a panacea for all identity verification problems. For example, it won’t prevent forgeries of birth certificates. It will however limit the damage that this can do without a digitally signed attestation attached to it that the government has provided and the identity controls. It won’t prevent the use of false government identity numbers on forms. However, it will provide a new framework where the need and thus the value of obtaining these numbers is reduced.

What is proposed is a new modern framework that takes into account the identity privacy needs of individuals while at the same time putting in place nationally and internationally agreed upon standards for verifying people.

In this digital age, it is important to allow for relatively quick searches to be made legally linking a person to a government approved identity. The challenge is in making this possible without giving “big brother” too much latitude but at the same time giving the government and the individual enough information to conduct legally approved searches with prior approvals.

**Draft “The Challenges With Identity Verification” –
Comments and Criticisms Welcomed**

ABOUT THE AUTHOR

Guy Huntington is an independent identity management consultant. He has been the lead consultant on projects such as Boeing’s global single sign on, Capital One’s single sign on, Capital One’s provisioning project and Kaiser Permanente’s web single sign on. He has wrestled with the challenges of identity verification for off-shore call centers as well as for contractors, consultants, temps and business partners. He is extremely interested in identity verification, digital identities, digital personas and identity federation. Guy can be reached at guy.huntington@hvl.net, www.hvl.net and at 604-861-6804.