Identity Federation:
Governments & Economic Growth

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: September 2017

Table of Contents

Executive Summary 3
Introduction 4
Examples 4
Net Effects 7
What about Immigration and people working on visas? 9
Requirements 10
Summary 12
About the Author 13

Executive Summary

This paper illustrates how identity federation rethinks citizen interaction with government and third parties. It provides examples for finance, health, social services, drivers' licenses, passports, different levels of governments, citizens' changing addresses, and schools.

The net effects of identity federation are:

- A rapid increase in the speed of servicing a citizen via their cell phone
- Seamless interaction from the national identity verification service with governments and third parties
- Lower cost of service
- A citizen's privacy is protected with their consent
- Economic growth

Using biometrics taken at birth, one physical identity per person is required. When coupled with creation of new laws and regulations to protect a citizen's biometrics it offers economic growth. Estonia's successful e-residency program is discussed, highlighting nearly 4,000 new companies being created by the program.

The paper identifies the high level requirements to make this happen:

- Laws and regulations
- Creation of a national identity verification service
- OpenID Connect

Introduction

If you have ever logged on to Google, Facebook, or PayPal and then clicked on a link to another website, which automatically accepted your existing authentication/authorization, then you have used identity federation. Without knowing it, approximately one billion people use OpenID Connect (the actual identity verification protocol) daily. Released in 2014, OpenID Connect is causing a rethink of how enterprises interact with their users **and governments are no exception**.

Examples

Finance

A citizen wishes to open a bank account. In some countries, it is possible to electronically create a bank account in only minutes online!

The citizen accesses the bank's website using their cell phone. They click on a link to open a new account and are immediately redirected to the government's national identity verification service. The citizen presents their national e-identity credentials issued by the government along with a password. The citizen's credentials are electronically verified and then, with the citizen's consent, their identity information is sent to the bank. The bank trusts the credentials because the government has a high degree of identity assurance associated with the citizen. The bank instantly receives the citizen's current address from the government. The citizen digitally signs the documents using their government issued digital signature, and the bank account is created.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the bank's internal network.

Health

A citizen uses their cell phone to call a toll-free number offered by the government to obtain health advice from a medical professional. They authenticate by providing a biometric via their cell phone plus a password. Next, they give their consent for the medical professional to view their health record. The professional then conducts a diagnosis, updates the citizen's e-health record, and the citizen then proceeds to use the diagnosis.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the government's internal health network.

Social Services

A mother and her two children appear at a government social services office claiming support. The social service worker verifies the family's identities by obtaining their biometrics. With the mother's consent, the worker is able to access their identity information including their most recent address, as well as pulling up social services, health, and education information about the woman and children. The social worker then offers social service support. The mother is happy she is able to access the support she needs quickly and did not have to fill out multiple forms providing information about who she is.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the government's internal social services, health, and education network.

Driver's License

A citizen wants to obtain a driver's license. They access the government's driver's license website via their cell phone, log on using their national e-identity, book an appointment for the driver's test, show up for the test, and pass. With the citizen's consent, the government agent then takes their picture, the driver's license is produced, and the person then digitally signs for the driver's license using the digital signature issued by the government. The citizen is happy they did not have to produce all sorts of information validating their identity.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the government's internal driver's license network.

Passport

A citizen wants to apply for a passport. They log on to the government passport site using their cell phone, and authenticate themselves using their government issued national e-identity. With their consent, the passport site receives their identity information. The citizen then digitally signs the form using their government-issued digital signature. If any other biometric is required to be attached to the passport, an appointment is made for the citizen to provide this with their consent. The citizen is happy the entire process was fast, easy, and didn't require them to fill in any forms with their identity information.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the government's internal passport network.

Regional/Municipal Governments

A citizen wants to access a regional or municipal service. They access the region/municipality website from their phone, log in using their national e-identity, give consent for their identity information to be passed, and then receive local services. The citizen is happy with how easy it is to deal with governments, and happy that they didn't have to enter all sorts of identity information.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the regional/municipal government's internal network.

A Citizen Moves

A citizen has changed residence. They log on to the national identity verification service using their national e-identity plus a password. They then are able to change their address. With their consent, the government is now able to send out the address change to not only the government's internal ministries but also to any other level of government and/or third party the citizen specifies. The citizen is happy because now all enterprises they deal with have an up to date address.

The citizen is also happy because they have the option of not updating other enterprises, except where required by law. Privacy is built into the system.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the government's internal network.

Schools

A child enters the school system. On their first day, their parents/legal guardians and the child provide some biometrics which are verified against the national identity verification service. Instantly, a lifelong e-education account is created for the child. The parents/legal guardians receive regular SMS reports about the child's progress. The child authenticates to the school's systems using a biometric which is verified by the national identity verification service.

Parents/legal guardians are happy because they now get regular reports on their child's progress. The child is happy throughout their life since their education record is automatically updated. Governments are happy since it reduces operating costs and also mitigates the risk of students who are enrolled but don't actually exist, i.e. ghost students.

How is this transaction conducted? By using identity federation, the national identity verification service, the Internet, and the government's internal education network.

Net Effects

The net effects of identity federation are:

- Rapid increase in the speed of servicing a citizen
- Seamless interaction between the national identity verification service and governments and third parties
- Lower cost of service
- Citizens' privacy is protected with their consent

What is at the heart of this?

A trusted national citizen identity with biometrics is created when they are born. As this paper describes "Identity Federation: Biometrics and Governments" (https://www.slideshare.net/ghuntington/identity-federation-biometrics-and-governments-sept-2017-80192336), it requires that governments create new laws and regulations protecting the biometrics used to identify a person (fingerprints, iris, and DNA). It also requires the national identity verification service to be run separately from other traditional government ministries responsible for things like drivers' licenses and passports. Why?

The answer is the national identity verification service is a request only system where a biometric is provided and a match or non-match occurs with the underlying database. There must be no transfer out of any biometric from this database. This is how citizens can be assured their biometrics, like DNA, used for national identity verification, are protected from any potential misuse.

The paper outlines that the underlying identity database, responsible for the national identity verification, must be run on its own network, as well as only contain minimal information to identify the citizen. It clearly states that there should be no creation of the "mother of all citizen identity databases." This reduces the risk of attackers trying to penetrate the database.

Further, the national identity verification service will be accessed by the government, its ministries/departments, by regional/municipal levels of government, and by third parties via the internet. That is where identity federation comes into play. It leverages the Internet and also the cell phone. OpenID Connect was built with mobile devices in mind.

If and when a citizen wants to apply for things like a passport, then they will use their national e-identity (even children will have one). The first step is for a citizen to verify themselves against the national identity verification service. Assuming the verification is successful, then the citizen gives their consent for the identity information to be transferred seamlessly and securely to the drivers' license or passport systems.

The same scenario also applies to third parties. To accomplish this, third parties would comply with the new laws and regulations the government creates according to the identity and credential assurance principles laid out in the paper. The citizen gives their consent. Any biometrics used for authentication are securely stored and managed. The citizen can inform the third party at any point that they want to withdraw use of their biometric from the service, and the third party must comply using processes specified by the laws and regulations.

What about Immigration and people working on visas?

In today's world, many people cross borders without documentation, claiming refugee status. Governments must then deal with trying to identify these people and decide what to do with them. Today, many countries adopt biometrics as a way to at least identify these individuals when they are at the border.

The long-term solution is to force all countries to move beyond current UN regulations for registering the birth of every person and extend this to biometrics. Then countries must adopt legal agreements to be able to cross-search other jurisdictions' national identity verification services to validate the claimed identity of the person.

The same process applies to people who are legally entering a country seeking to work, study, or live. Countries adopting what this paper suggests will create a national e-identity for the person with links to the home country where the person comes from. The foreign person will now be able to deal online with government services, as do residents.

In Estonia for example, they are working at creating e-residents for foreigners aimed at taking their existing population of 1.3 million to over 10 million by encouraging foreign people to invest in their country. The result is that already nearly 4,000 companies have been created (https://e-resident.gov.ee/).

Requirements

Laws and Regulations

The very first step is to do a legal gap analysis to determine the legal and regulatory changes required to enable this vision. Laws and regulations must be created to:

- Establish how any citizen biometric used for the national identity verification service will be protected and not used for any other purpose than identity verification, nor will it ever leave the database and be exported to any other government ministry/department or third party
- Mandate the collection of biometrics used for national identity verification:
    - At birth – Fingerprints and a DNA sample
    - First year of school – iris scan
- Specify under which conditions the ability to verify an identity will be done with citizen consent as well as without citizen consent
- Mandate how any other biometric collected by the other government ministries/departments, different levels of government, and third parties should be:
    - Obtained with citizen consent
    - Properly stored
    - Usage of the biometric for authentication
    - Processes whereby the citizen can request removal of their biometric from the database
    - Citizen consent required to use the biometric for any other purpose than authentication

With this, citizens will buy into the national identity verification service using their biometrics.

Creation of a National Identity Verification Service

There are several components to this including:

- A unified birth, name change, marriage and death registry service using the same underlying database
- Biometric collection processes for newborn infants for:
    - DNA
    - Fingerprints
- A biometric collection process for an iris scan during a child's first year of school
- Collection of the parent's or legal guardian's identity information and links within the national identity database to them
    - This also involves ensuring that any legal change to the underlying legal guardianship of the child is securely sent from the authoritative legal source to the national identity verification service
- Creation of the national identity verification service on its own network with multiple layers of security
- Read only access to the underlying data except with legally approved changes
- No biometrics stored within the database can be exported

- All access to the national identity verification service will be via the Internet for all government ministries, different levels of governments, and third parties
- Ability of the national identity verification service to provide anonymous verification of the identity where applicable by laws and regulations

Create Identity and Credential Assurance Levels

In today's age, central to the heart of functioning governments and third parties are well thought out identity and credential assurance levels. These are measures of trust given for identity and authentication based on risk.

Government ministries/departments, different levels of government, and third parties all need to legally and technically know what the assurance levels are for a given transaction. This should mesh up with other countries the government interacts with. It allows seamless citizen and business flow across country boundaries physically and electronically.

Adopt OpenID Connect

Governments should then adopt usage of OpenID Connect. HOWEVER, it is not "one thing" AND there are many risks and potential liabilities that need to be mitigated via legal agreements, business, and technical processes. The government must create legal frameworks for trust circles to be built with their "identity federation partners" such as third parties, crown corporations, and other levels of government. It is the heart of a government security system so appropriate attention must be given in the planning, deployment, and maintenance of it.

Summary

Most government leaders are not aware of the potential impact that a national identity verification service coupled with the cell phone, identity federation, and the Internet can have on their country or jurisdiction. Instead, it gets lost in ministries/departments associated with things like immigration, passports, drivers' licenses, voter registration, education, health, and social services. Each of them is trying to solve their own problems using different vendors as best they can.

Leaders in the government need to realize that this is quietly causing an economic revolution on which their country can benefit or suffer is they don't position their country for it. That's what this document is about. If you are a government leader, then you need to take control of all your various departments and provide them with a vision and leadership crossing their existing departmental silos.

The solution this paper presents is vendor agnostic. There is no one vendor who is able to come into your government and create what this paper presents. Yes, they can contribute some of the solution but they are not able to provide the complete solution. Why not?

The identity federation protocol, OpenID Connect, is a protocol adopted by thousands of different companies. It is not something that one vendor "owns".

Then there is the technical solution and business processes driven by the laws and regulations that need to be created to solve this. To make all the "magic" work it requires a strong legal framework, as illustrated by examples given at the beginning of this document. This includes new laws and regulations pertaining to biometrics as well as legal frameworks to create identity federation agreements.

To give you an example of the complexity of the identity federation agreements required, see this paper "Enterprise Identity Federation: Mitigating Risks and Liabilities" (https://www.slideshare.net/ghuntington/identity-federation-mitigating-risks-and-liabilities-79942481) and then have your government legal, business, and IT personnel read it thoroughly. I've worked with many large enterprises, both government and Fortune 500, where they didn't understand what it takes to deploy identity federation.

If you take this message to heart, then you can effectively steer your country onto the pathway of economic growth.

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."

Guy has worked with many different identity and access vendor's products as well as with many different consulting companies on projects he has managed.