Botswana National ICT & Healthcare Strategy

Huntington Ventures Ltd.
The Business of Identity Management
June 2016

This Deck…

- Lays out existing healthcare delivery problems Botswana currently has
- Presents a high level framework for an ICT health care strategy leveraging the national identity and authentication infrastructure which:
  - Unifies the citizen's identities between the numerous existing ministry health applications
  - Provides an national eHealth software
  - Combines the Omang with citizen health care cards for remote locations
- Presents new, low cost ways of reminding citizens about vaccinations for their children as well as innovative ways of tracking moms to be
- So who am I?

Guy Huntington

Guy Huntington is a very experienced identity architect, program and project manager who has led, as well as rescued, many large Fortune 500 identity projects including Boeing and Capital One. He recently completed being the identity architect for the Government of Alberta's Digital Citizen Identity and Authentication program.

Botswana HealthCare Delivery Challenges

- Too many health care systems/applications currently delivering health care
- Lack of a unified health identity per citizen that commences when they are born and stays with them until they die
- Some remote places lacking connectivity are difficult to deliver health services cost effectively

Technology Citizens Have

- Most citizens in Africa DON'T have internet access
- What they do have is:
  - Cell phone
  - e-wallets
- Some have debit and credit cards

Solution: Leverage Identity & Cell

- Create a national identity strategy leveraging citizens use of cell phones using their voice to authenticate
- The architecture behind this has been used by large global enterprises and a few countries like Estonia since the late 1990's….so it's nothing new
- It also leverages interactive voice response, which has been used in industry for the last 20 years as well
- It provides a seamless user experience when the citizen acquires a smart phone, tablet or laptop
- It leverages the same infrastructure that ALL government ministries will use
- Additionally, the same infrastructure can be used by crown corporations, municipalities and third parties like banks, telcos and insurance companies

Before We Get To Health…

- I will show you how other countries are using a similar infrastructure to create more than 1,000 online services for their citizens (Estonia)
- To begin, let me first talk about the lifecycle of a citizen's identity

It Starts When A Citizen Is Born…

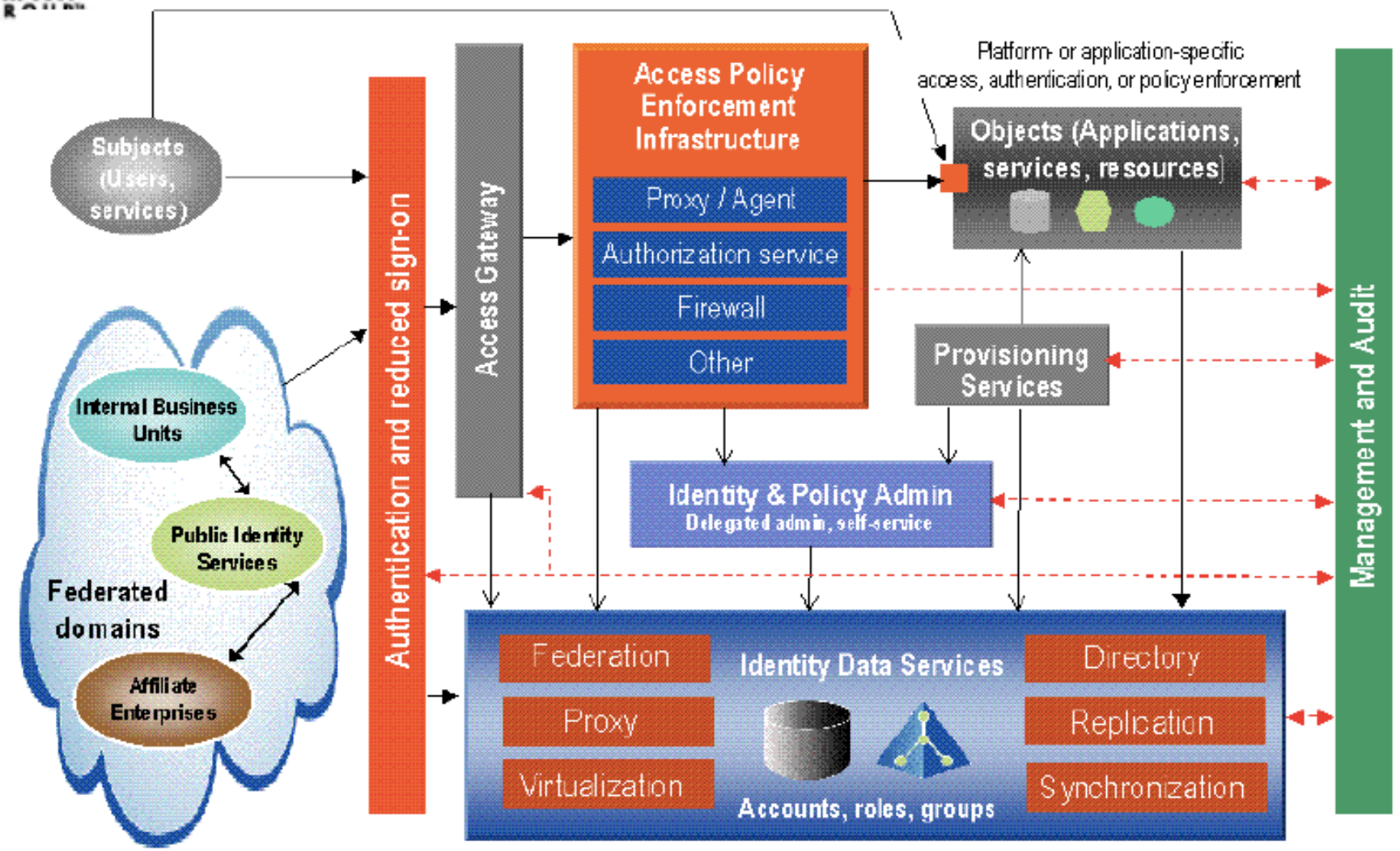
- When you are born, in addition to the traditional information being captured, the health worker will also take a biometric from you, e.g. a finger scan and/or a retina scan
- As well, the health worker will also obtain your parents national identities from their national ID card
- There is one important addition to the national ID….it now captures the citizen's cell number in the national ID directory
- So, in the national directory, your electronic identity begins at birth. There is also a relationship between you and your parents or legal guardians
- Let's look "behind the scenes" at how this will work by first understanding a bit about the architecture...

Nearly 20 Years Ago…

- Many Fortune 500 companies and only a few governments realized that single identity was a critical cornerstone piece of their digital strategies
- **Without this, no SOA and portal strategy would work, since having multiple identities for the same person would not allow for seamless digital and in-person services**
- **Further, they also realized that having a common access service is dependent upon having a unified identity**
- In my own case, at Boeing, in the early 2000's, we implemented a unified identity and access management infrastructure and then integrated into this several large portals with more than one million users as well as 1,500 applications. In parallel, they then developed a SOA architecture based on the identity infrastructure
- To illustrate this, the next slide is an old Burton Group target identity architecture, now nearly 20 years old, showing the basic components of an identity and access management system

Roadmap of IdM Terms & Tech

Putting it together – Burton Group Reference Architecture Template for IdM



The Point I Am Making…

- For the last 20 years, all identity and access management systems have the following components:
  - **Identity Management Server**
    - In today's world this is a combination of the Provisioning and Identity & Policy Admin from the previous slide
  - **Directory**
    - This is the large box at the bottom entitled "Identity Data Services
  - **Access Manager**
    - This is the box titled Access Policy Enforcement Infrastructure
  - **API/Internet Gateway server**
    - This didn't exist 20 years ago
    - You will see this in some slides in this deck

Estonia…

- In Estonia, in the late 1990's they too realized that identity is the key component
- They realized that a common identity for each citizen was required
- They also realized that citizen event life triggers were also important to streamline government services
- Finally, they too also adopted a SOA web services architecture

Single Citizen Identity

- One identity per citizen
- Any changes to the identity are then shared with other apps/services consuming them
  - One place for a citizen to change things like addresses and phone numbers
  - Citizens don’t have to fill in the same information over and over in forms for different apps/services
- Same identity used for access management

Identity - Foundation of e-Governance

Citizen

Accesses via their phone or the internet

Citizen Identity Access Management System

Government Portal

Ministry Apps/Services

Ministry Apps/Services

Ministry Apps/Services

Crown Corp. Apps/Services

Municipalities Apps/Services

3rd Party Apps/Services

Single Citizen Identity

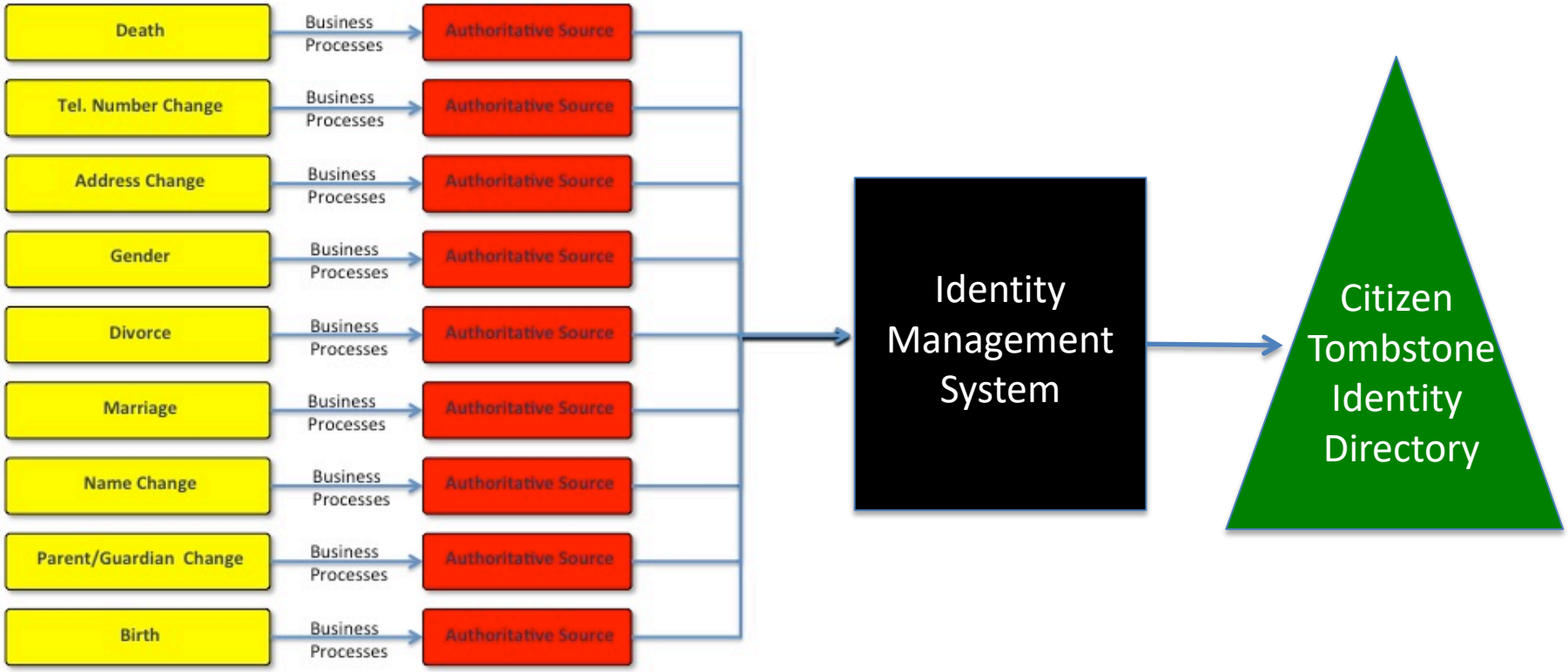
So Why The Green Triangle?

- A “Directory” is a special type of database
- More than 20 years ago, large enterprises realized that if they were going to use the database for authentications, it could take hundreds of thousands or millions of concurrent hits per second
- Since the old databases couldn’t perform, they created a tree type database which could easily perform and scale
- This is called a LDAP directory (Lightweight Directory Access Protocol) and is depicted using a triangle

Now Let's Look At Authoritative Sources

- In the lifecycle of an identity, there are several main identity "trigger" points
  - These are depicted in the yellow boxes in the next slide
- For each one of these, there are associated business processes, usually determined by laws
  - These are depicted by the red boxes in the next slide
- Once the data is entered into the authoritative source for the identity lifecycle, it then flows to the national identity management server
  - The black box in the next slide
  - This is the smart brains of the identity management system
- It then creates or modifies an identity in the citizen tombstone identity directory

National Citizen Identity Lifecycle



Why Is It Called “Tombstone”?

- The national identity and access management infrastructure only stores high level “tombstone” identity information
  - Similar to what is often entered on a person’s tombstone
- This includes things like legal name, place of birth, gender, address AND CELL NUMBER
- The directory is not the “mother of all identity databases”
  - So sensitive information such as tax numbers, etc. stays in the respective ministries databases
- This is good privacy design

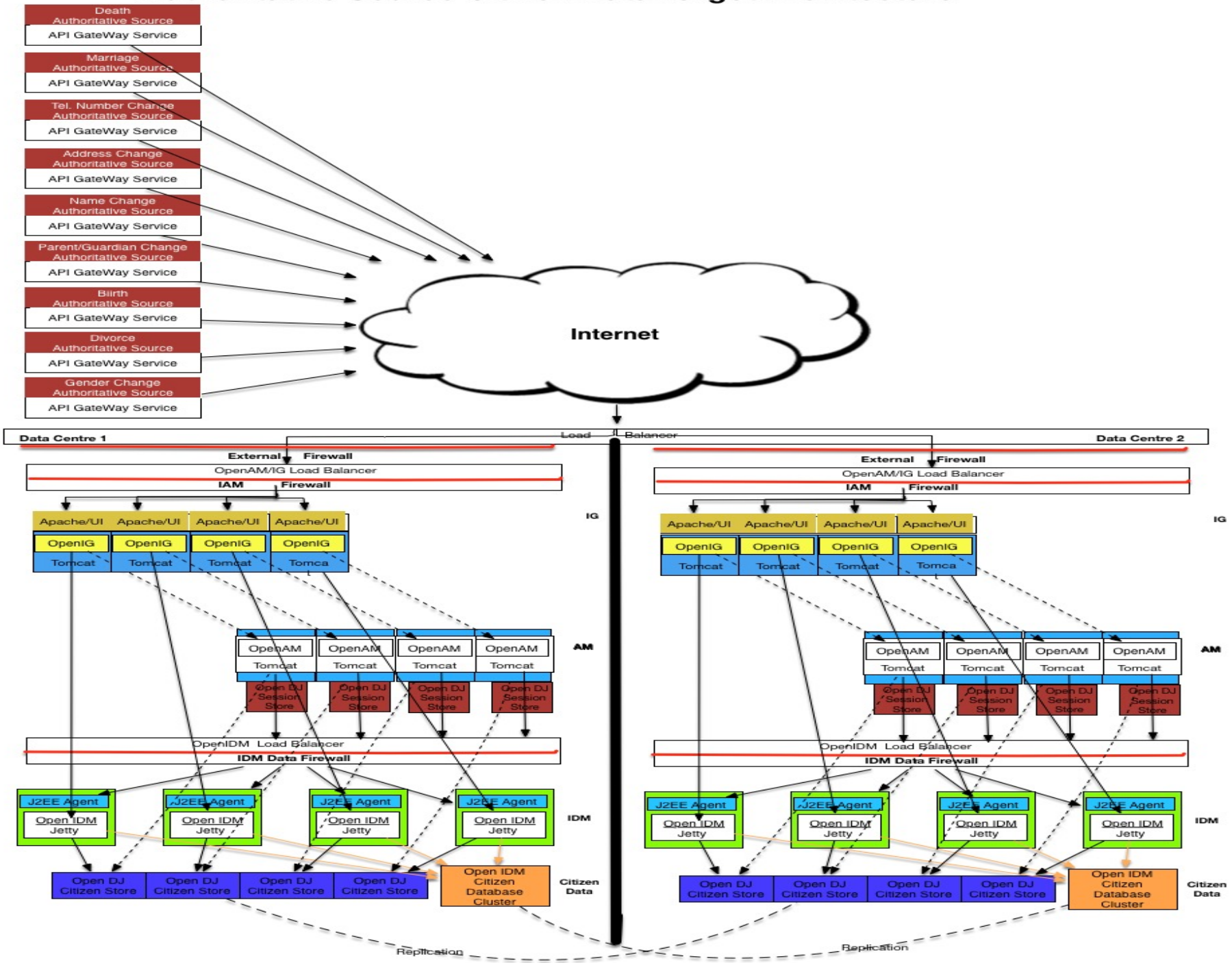
Leverage Open Source Software

- The strategy leverages open source software identity and access management from a company called “ForgeRock”
- Governments using this around the world include Canada, Norway, New Zealand, Australia and the Province of Alberta
- Large companies like Toyota also use it
- So this is proven and you won’t be the first to use it
- Let me show you what really happens “underneath the hood”…

The Actual Architecture…

- The following slide shows the actual architecture used
- To simplify this let's pretend that you've just been born
- The birth registration, including your biometric, plus you parents identity information is sent from one of the red boxes on the left titled "Birth Authoritative Source"
- It flows out via an API (Application Programming Interface), securely through the internet (3 types of encryption used) and into one of Botswana's data centres
- It then flows to a box called "Open IG". This is the internet gateway server mentioned previously
- Open IG then passes the information to the Open IDM server (this is the identity management server mentioned previously)
- Open IDM then realizes you are a new entry and then creates a new identity in the directory with links to your parent's/legal guardian (this is the LDAP directory mentioned previously)

Authoritative Source Citizen Data Target Architecture



So Why Am I Showing You This?

- You are about to see how the same underlying national identity management and authentication infrastructure can be used to create new accounts in open source healthcare and education management software
- It will also be used to authenticate against

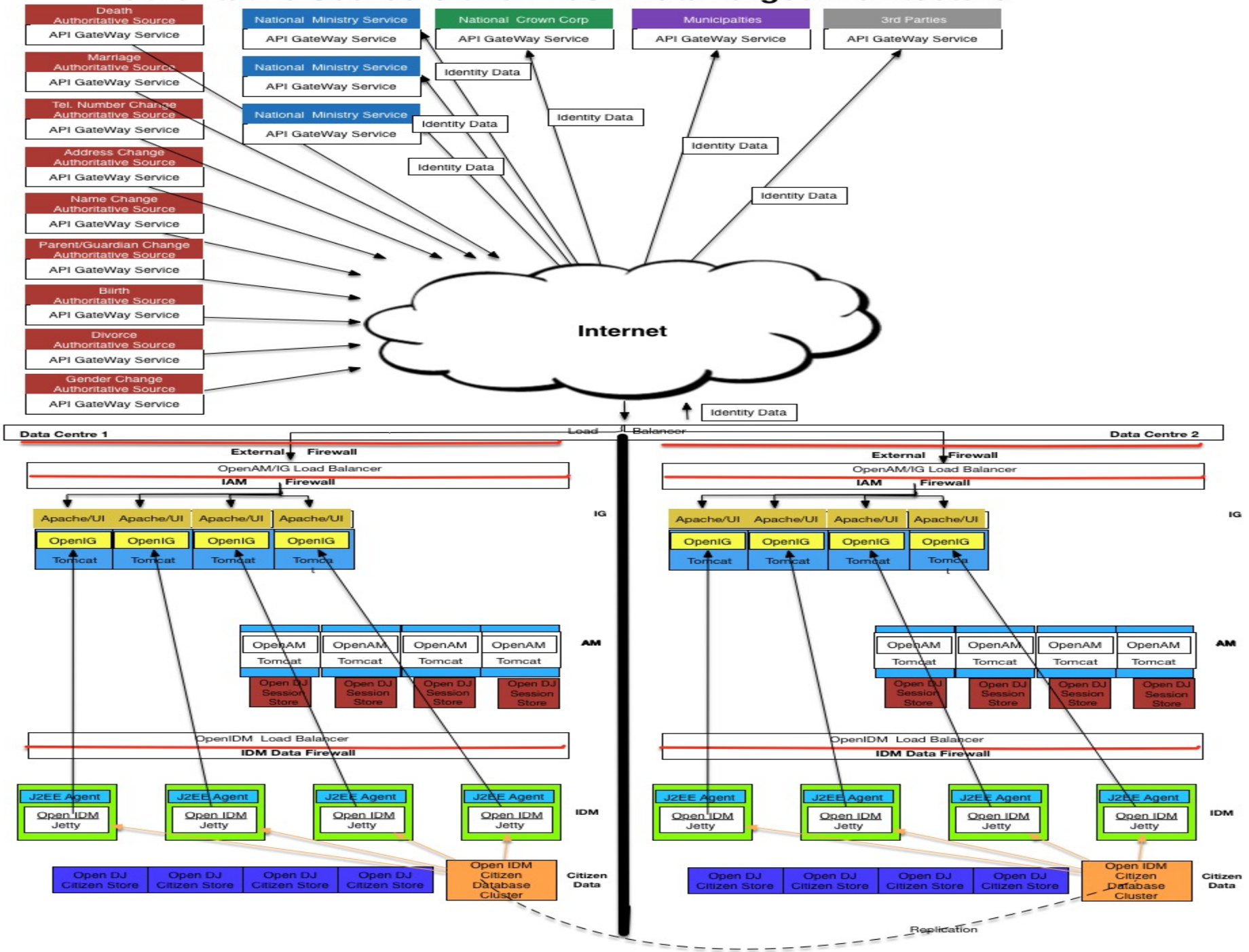
Automatically Create A Healthcare Account For The Infant

- The identity management server can be used to send your new birth entry, along with your parents/legal guardian information to a open source health care software (which also exists today)
- Included in this is your parents/legal guardians cell phone information
- Here's how this happens "underneath the hood"…

Changes To The Citizen's Identity

- The value of using this architecture is that all government ministries, crown corporations, municipalities and 3rd parties consume the same identity
- So now let's see how an identity change then flows from the identity management server (OpenIDM) to these entities…one of which is to the Open Source Health Care application to create a new identity for you
- In the next slide you'll see the identity management server, sending your identity information, via Open IG out to numerous ministries, crown corps, municipalities and third parties
- In this case, one of the "National Ministry Services" would be the Ministry's of Health Open Source Healthcare Management Software

Authoritative Source Citizen Push Data Target Architecture



Let's Say You Don't Immediately Implement Open Source eHealth…

- If it takes time to implement the open source eHealth software, then an interim step is to first set up each of the existing healthcare applications with the same identity and any changes to the identity, from the national citizen identity and authentication infrastructure
- This will eliminate any possible confusion or costs arising from identities that are out of sync between the different systems as well as assumptions the identity man be more than one person
  - E.g. In British Columbia, several years ago, they discovered they had 9 million health care cards for 4 million citizens. This lead to the creation of a unified citizen identity system

When You're Vaccinated Your Biometrics Are Updated…

- Since your finger biometric changes, the vaccination point in your lifecycle is an excellent opportunity for the local health care worker to update it

Use Voice To Service Citizens Via Telemedicine

- In remote areas where there are no or poor access to health care professionals here's what not could happen…
- A citizen could call a toll freee healthcare number
- They are authenticated using their voice
- The authtentication services then sends a PAI "Persistent Anonymous Identifier" to the helth portal
- The Health portal then maps the PAI to your identity
- With your consent, the citizen grants acces to their ehealth record to the health professiona; on the phone
- The medical profession treats them and then updates their health record

Why Use A PAI?

- The architecture values a citizen's privacy
- Therefore, it mitigates against the risk that a malicious person, who has access to a ministry server can then obtain your unique ID and then masquerade as you on another ministry's server
- So, let's use an example…
- You the citizen are interacting with two different ministry services "A" and "B"
- When you successfully authenticate, Ministry A gets a PAI of ABCDE for you, which they then map to your identity within the database
- Ministry B gets a PAI of MNOPQ
- So a person who maliciously obtains ABCDE can't use this on other different ministries databases

All Apps/Services Leverage the Same Access Management System

Citizen

Accesses via their phone or the internet

Citizen Identity Access Management System

Government Portal

Ministry Apps/Services

Ministry Apps/Services

Ministry Apps/Services

Crown Corp. Apps/Services

Municipalities Apps/Services

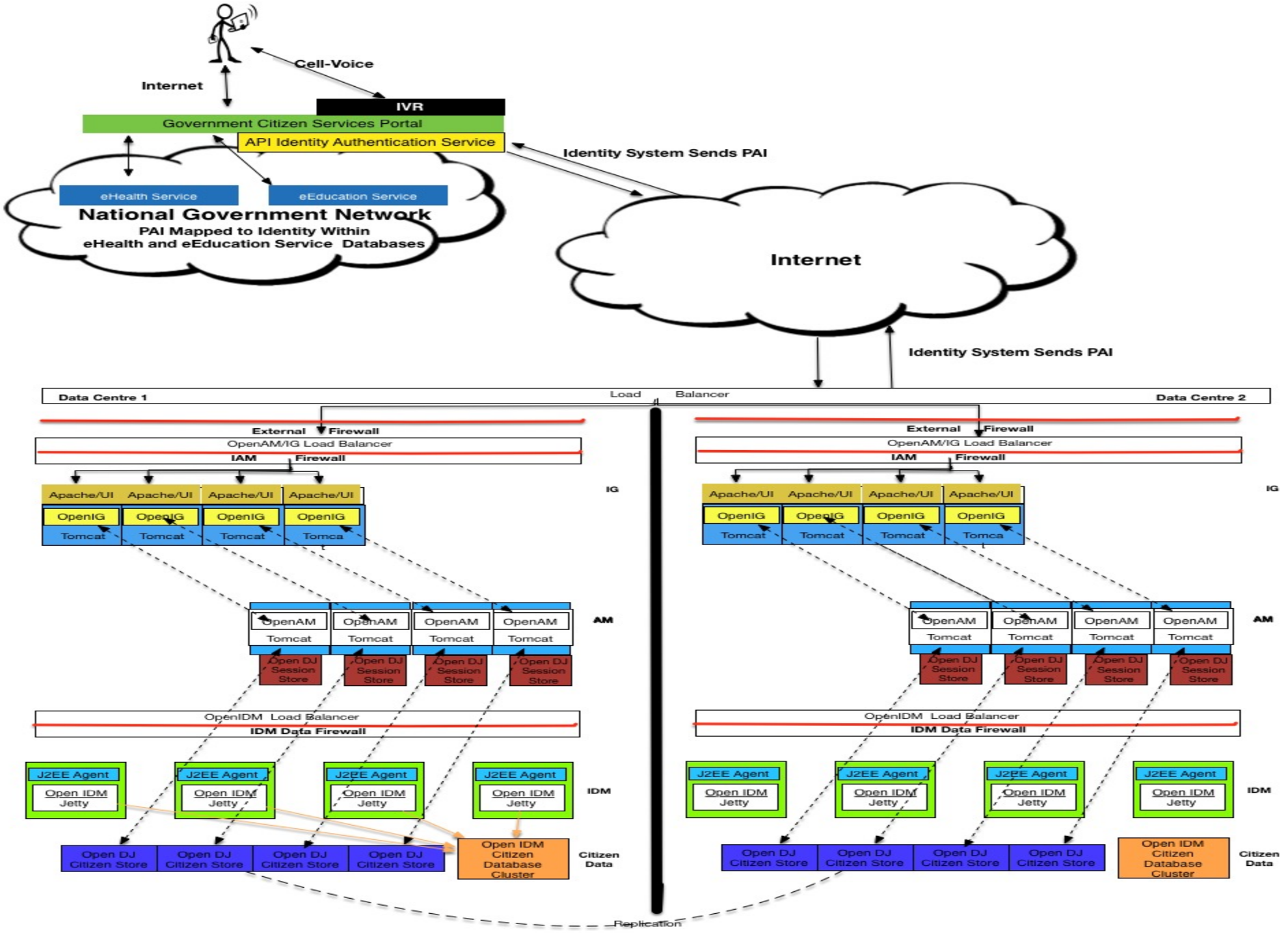
3rd Party Apps/Services

Single Citizen Identity

Let’s Follow The Electrons…

- The sick citizens uses their voice to authenticate by calling a toll free health number and then saying their name
- The IVR takes the voice and then passes it, via the internet to the same infrastructure you saw before in previous slides
- It goes through the Internet Gateway server and on to the Open AM (access manager server)
- This then verifies the voice against the directory or a related biometric server
- If successful, the Open AM server then generates the PAI which is then sent, via Open IG to the Health portal
- The portal then maps the PAI to your identity and the open source health care software then takes over

eHealth and eEducation Target Architecture



What Happens When There's No Connectivity?

- In certain parts of your country there may be no or poor connectivity
- You, the infant, will also have a national identity card
  - Malaysia creates youth identity cards MyKid
    - http://www.malaysiacentral.com/information-directory/mykid-identity-card-of-malaysia-for-children-below-12-years-old/#sthash.ZXp3bJOb.dpbs
- On the card will securely be stored some of your medical information
- If your parents are in a remote area, the health care worker will scan the card using a portable unit, treat or vaccinate you and then update the card
- When the healthcare worker reaches connectivity, they will upload the information to the healthcare system

So The Next Time You Show Up For Treatment…

- You would present your or your child's national OMANG.
- The health care field worker would use a portable unit to scan the card and upload medical information contained on the card
- After treatment, the health care worker updates the card and then, when they reach connectivity updates the national system

When You Need A Vaccination…

- The open source eHealth software has your parents/legal guardian's cell numbers from the national identity and authentication infrastructure
- So…it will be able to send them a SMS message telling them you need a vaccination
- This leverages what the citizens have in their pockets and the national identity and authentication infrastructure
- You, the citizen, have to go to only one place to change things like your address and your phone number so the information is up to date in all the different services you interact with

When The Citizen Changes Their Address Or Phone Number…

- They only have one place to go to change this information with the government, i.e. via their cell, smartphone, tablet, computer or, an actual office
- After authenticating, the citizen may be required to enter a 4 digit pin to provide stronger authentication that they are whom they claim to be
- The change makes its way through the architecture seen previously and then the identity management server automatically sends it out to pre-approved apps in ministries, crown corps and third parties

Change in Guardianship to Infants…

- Whenever there is a legal change in parent/guardian status, it will be recorded via legal business processes in a authoritative source
- The national identity management server would then automatically update the record in the directory as well as updating ministry apps, including health, social services, education and municipalities etc. for which a policy has been created.
- This will aid front line people who may be dealing with different people claiming conflicting parenthood/guardianship for a child

Innovative Treatment Programs

- At a recent African conference I attended, I came across people who were using SMS to assist mom's to be with a treatment program in West Africa
- They were very existed in the national identity and authentication infrastructure this presentation covers
- This architecture and strategy presented seeks to leverage cost effective ways of treating and following up with people using something they have in their pockets…a cell phone.

Integrating Private & Public Healthcare…

- Private health care providers would be required to integrate the national citizen identity and authentication service into their systems
- They would then be using the same underlying citizen identity as would a public healthcare system
- Let's uses ACME Medical as the third party. ACME medical would create their apps to access the national authentication system using patient's voices as well as some other biometrics where the voice isn't available
  - The fancy term for this is ACME's authentication system would abstract out its trust to the national identity and authentication system
- Acme would receive a PAI from the national identity and access management system which it twould then map to the identity within their own data systems
- As open source medical data systems, like HL7, etc. are adopted citizen health data could then flow between the private and public systems

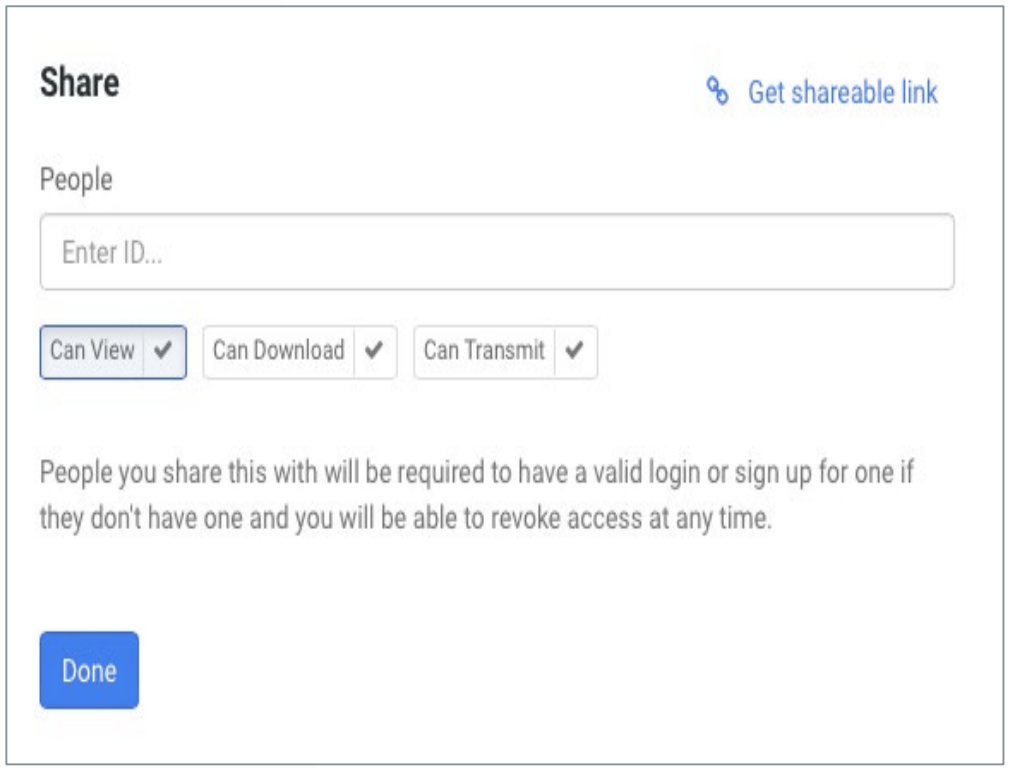
So What's This About "Citizen Consent?"

- As the world and your country digitizes, citizen consents will be required for numerous things
- In the past, you gave you consent in silo-ized applications
- What if you could centrally manage all the consents you have to governments, third parties. Municipalities, etc.?
- Today you can using a emerging protocol "User Managed Access"

Privacy & Consent

User Managed Access (UMA)

- Standards based privacy and consent
- Giving people the right to control access to their data across providers
- Interoperable OAuth2-based protocol
- **Shipping as an integrated feature of OpenAM and OpenIG**



Does This Solve All Health Problems…

- No. HOWEVER IT:
  - Provides a e-health framework leveraging national citizen identity and authentication infrastructure
  - Leverages existing technology most citizens have access today
  - Provides a privacy and consent framework which is required in health care
  - Enables the Ministry to use the same identity with all the applications currently running in the health ministry
  - Rethinks the OMANG such that it becomes also a national health card as well containing some medical information, securely stored, and available to health care workers out in the field

National ICT Identity …

- Is one of the critical building blocks to create an e-health framework
- The same investment used by other government services can be leveraged by the Health ministry
- The same privacy and consent services the national identity service implements can be used by the e-Health software

This Could Be Botswana…

- Botswana can become a digital leader in Africa
- HOWEVER, to do this requires all Ministries to work together leveraging the same underlying national identity and authentication infrastructure
- Finance, Education and Health should be involved in the creation of this infrastructure in addition to the traditional ministries who look after identity lifecycle events

Summary

- **Botswana could become the Estonia of Africa – a innovative nation that leveraged the digital world to rethink itself**
- **Please contact me:**
  - 1-604-861-6804
  - guy@hvl.net
  - www.hvl.net