PUBLIC

Research & Development Proposed Investigation

V.00.11

4205 S. Miami Blvd
Research Triangle Park 27703
USA

redpath@us.ibm.com

IBM Digital Identity Deployment and Proofing addressing NIST proposals

Prepared for: IBM Mobile Identity Project

Prepared by: Richard Redpath
IBM Mobile Identity Emerging Technologies

March 10th 2017

Description

This document outlines a digital identity deployment and proofing solution that does not require a connection for authentication compared to NIST proposed digital identity guidelines and enrollment/proofing that requires scale and financial resources of a connection as well as unneeded vetting. This is a disruptive technology that provides financial benefits to issuing institutions, scaleability, and limited access for increase security of the owner of record for authentication of a populus. The intent of this document is a Point Of View (POV) for NIST to learn about the new industry innovation.

Proposal Number: N/A

Table of Contents

Background

NIST is providing Digital Identity Guidelines over a public period from January 30- March 2017 and what NIST has learned about the industry innovation.

https://pages.nist.gov/800-63-3/

The initiative is not aware of the recent disruptive technology that IBM has invented which enables Digital Identity to work like thermal plastic in a disconnected network. Furthermore the IBM Ecosystem of enrollment and proofing is more disconnected from requirements of maintenance period and enables this control by the relying party (issuing institution).

Executive Summary

Identity today is a disconnected environment through Thermal Plastic cards. The owner (applicant) is not enrolled in a subscriber system but obtains the identity material from an Institution (origin, owner of record) such as the DMV or Provider such a membership club or Insurance company directly.

Digital Identity is under construction (DRAFT NIST publication 800-63-3, 800-63-3A) to have a Credential Service Provider (CSP) to the relying party (RP) for the Verifier to validate in a connected environment. This work is reflective of what NIST has learned about industry innovation for enrollment and identity proofing. “These guidelines provide technical requirements for Federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose.” Guideline 800-63-3A focuses on the enrollment and verification of an identity for use in digital authentication.

Unfortunately this work is not aware of the IBM innovation which is designed to work in a disconnected environment like thermal plastic today as well as less contrained provisioning of security as privacy information has been de-weaponized. The origin (owner of record) of your identity remains with the issuing Institution and is not subsetted to some form for a central Credential Service Provider (CSP) to service requests for proofing. The solution also prevents massive transaction processing in order to authenticate identity as well as prevention of financial burden for infrastructure, distribution of your privacy information to another source (weaponizing), and the avoidance of new security conduits into a highly valuable target. Additionally the disruptive technology for the industry has provided a means for privacy control that has never been envisioned before possible through a DSA Group Homomorphism for traits that seamlessly works disconnected and is essentially a hybrid blockchain.

$$G \rightarrow H$$

$$\varphi_x(u+v) = \varphi_x(v) + \varphi_x(u)$$

IBM has designed a Digital Identity system which works like thermal plastic in a disconnected network with no transaction security vetting requirements that get dragged along for designing a digital identity system that is unaware of the new innovations by IBM that require connectivity.

The Identity assurance level (IAL) is controlled by the Issuer (Institution) which has the prerogative to apply the latest assurance technique such as fingerprint and biometric information and remains with the issuer for the owner of record. The IALs do not require a CSP to contact the RP (origin of identity) to fulfill a request in context of authentication needed for an owner.

Futhermore for completeness the Digital Identity Guidelines do not faciltate a means to use multiple identity instruments required by some scenarios (eg: Pharmacy, Medical Provider). The IBM Digital Identiity system provides this means.

Introduction

Identity is a real life interaction of individuals to establish that a subject is actually who they claim to be. This interaction in terms of digital concepts is peer to peer. Imagine 10,000 bars and restaurants open in North Carolina every Saturday night and are required to proof people for privileges controlled by the state. Envision the financial infrastructure and security if the state were tasked for vetting each proofing. These peer to peer interactions happening every day are the norm and go on without an engineering task force behind them for a communication infrastructure. Identity today is a disconnected environment through Thermal Plastic cards as a Driver's License or Identity Card. The owner (applicant) is not enrolled in a subscriber system but obtains the identity material from an Institution (origin, owner of record) such as the DMV or Provider a membership club or Insurance company directly. These Thermal Plastic cards have security features to make it difficult if not impossible to copy.

Digital identity is a subject engaged in an online transaction and does not uniquely identify the subject for a digital service that does not mean that the physical representation of the underlying subject is known. Your son could use your loaned credit card online for a transaction and as long as all the information presented is correct the transaction is completed for the recognized digital identity engaged.

A Mobile Driver's License (mDL) is intended as a digital form of the Thermal Plastic Card to be on your mobile device seamlessly replacing the printed card. Digital form has the opportunity for complete privacy control of information verses a printed fixed document. Today we hand over all our information with our Thermal Plastic card to a restauranteer for privileges but mDL can change that. Digital form can also create an ecosystem that is cost effective for the issuer as well as the legislative statutory enforcement of privileges that can be taken away at any time in an instant. Additionally an mDL can de-weaponize your privacy information for its stored form; a thermal plastic license is in the clear for anyone to read if stolen. Futhermore the authentication by officer for maintaining law can be safer.

An mDL must have considerations for Use case scenarios, Privacy, security, financial impact, and scale considerations for the sublimation of a Thermal plastic card. The most common use case peer to peer disconnected must be addressed to be seamless. Privacy should be an opportunity taken and fixed for the current material card as well as security of the information. Today the Issuer of your identity does not have a financial investment in infrastructure for you to establish who you claim to be and that burden should not be created. Tens of thousands of bars and restaurants open on Saturday night in the USA and the populus should not be concerned with servicing response for scale to prove who they are.

Privacy, Security, Financial, and Scale Considerations

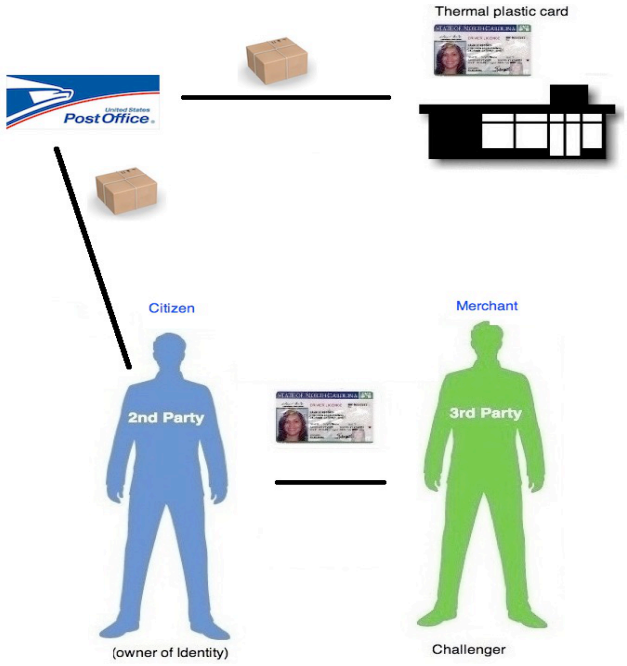
- The authentication process for thermal plastic driver's license today is peer to peer and is not to be translated into server transaction based solution (scale)
- The owner of record remains the same with no introduction of financial burden of authentication processing (financial)
- Do not create new conduits, a security issue, into the owner of record to authenticate (security)
- Work disconnected anywhere (security)
- Do not weaponize privacy information and distribute it to another source outside the owner of record for handling requests. (security)
- Provide complete privacy information control by the owner of the identity. (privacy)
- Do not create new and larger population threat targets. (security)
- Provide a means for multiple identity instruments for a privilege such as Class 2 drugs from a pharmacy.

Discussion

Digital Identity requires deployment to devices which makes it ephemeral and a security issue for copying unlike today's process of US mailing a thermal plastic card for your wallet that has security features to make it difficult if not impossible to copy.

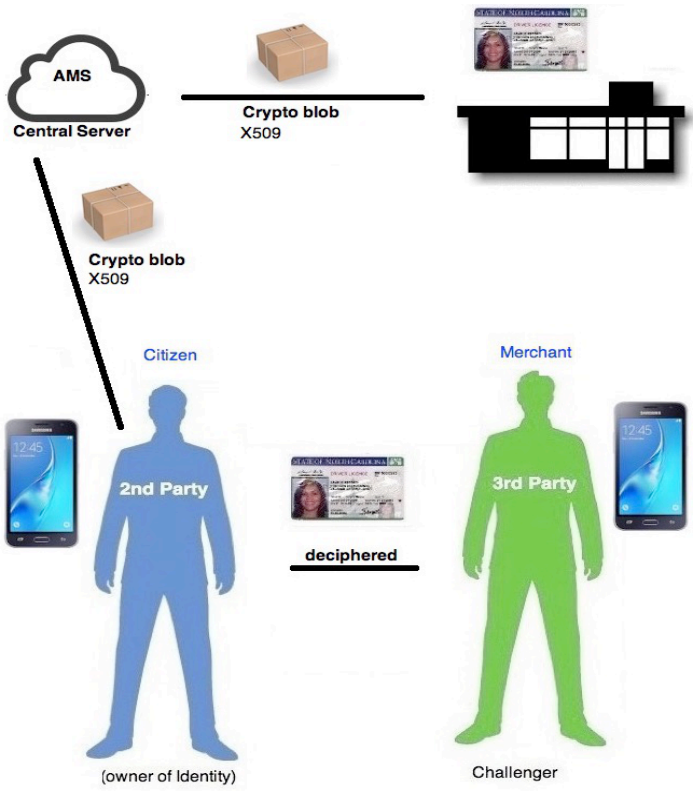
IBM has designed a Digital Identity system which works like thermal plastic in a disconnected network with no transaction security vetting requirements that get dragged along for designing a digital identity system that is unaware of the new innovations by IBM that require connectivity.

To best describe this system and its simplicity the current thermal plastic system will be compared to the IBM system with analogies. Today the Post office is tasked to deliver your Thermal Plastic Driver's license just like any package for delivery. The Post Office is not in the know of what's in the package to deliver and there is no reason too. The owner (citizen) is not required to be vetted to register to the Post Office for delivery other than the Post office knowing the address.



The owner doesn't need a digital connection to be vetted by a Merchant. The Institution has security constraints already built into the issuing system and more being added everyday to vet the owner (citizen) to provide identity material for a Merchant.

The IBM solution is very much the same and leaves in place the control and experience of issuing by the Institution. A picture is shown below from a high level perspective of the owner who has purchased an Identity instrument.

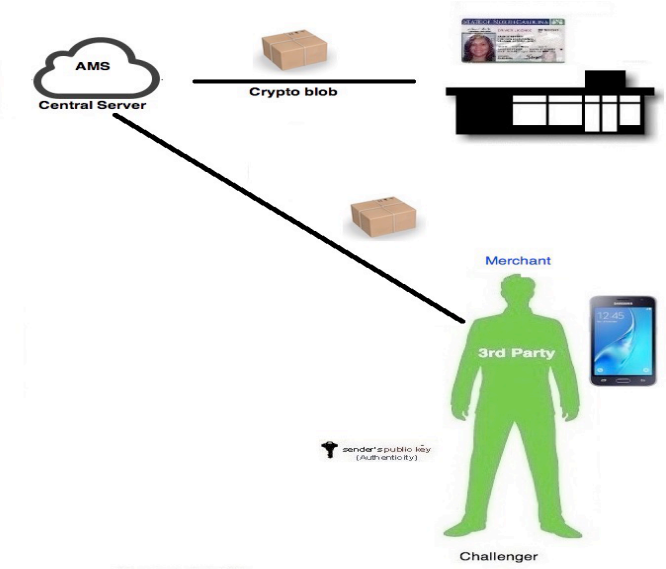


The Owner can register the device with the Central Server, essentially registering your address for delivery. There is no need to authenticate the user to subscribe other than providing a subscription credential (address) that can be used by providers (Institution) to know where to deliver the package. This is pretty much the same as iTunes, anyone can join and purchase products. Very much like Amazon is to purchasing products and shipped delivery. The central server shown above has a store of acquisition URLs to obtain products. The owner is redirected to the product site and vetted by that institution who will know where to send the identity instrument.

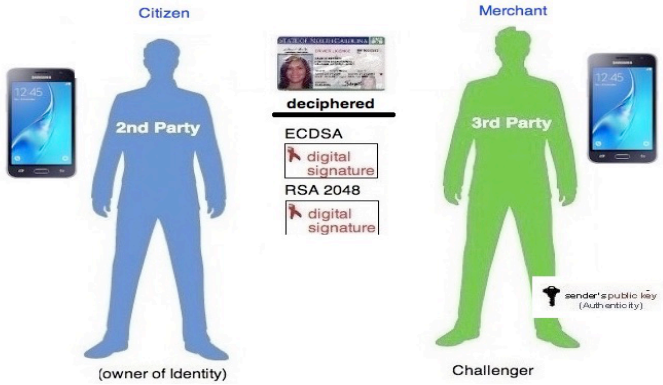
The merchant can validate the owner directly. There are no new conduits or financial infrastructure needed into the issuing Institution. The owner has complete control of the privacy information that is shown to the merchant directly. Authentication is peer to peer and involves no services and is disconnected from the Relying Party; very much like thermal plastic today.

The owner information is uniquely encrypted to a device and that encryption private key is only known by the owner. The package is called the Cryptoblob. Furthermore the Institution is not in the know of the Cryptoblob deciphering that has been sent to the AMS (central server). The AMS (central server) can be data compromised and glean only Cryptoblobs all unique to each device for encryption. A Cryptoblob container is an V3x509 OID 1.3.18.0.2.18.6 extension. Essentially an x509 is delivered as the security package.

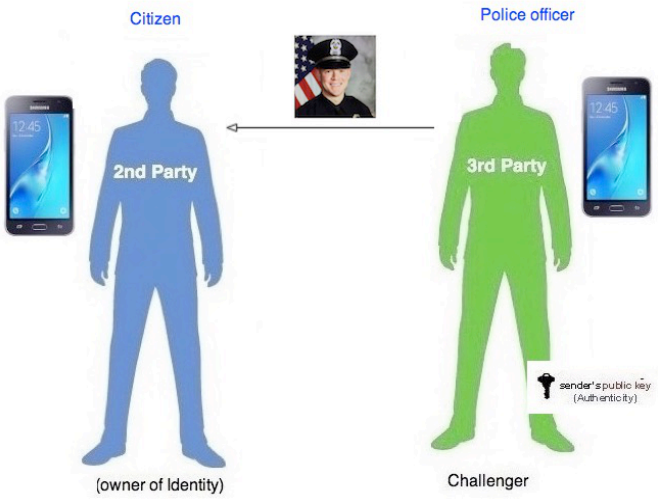
From the Merchant perspective (authenticator) a picture is shown below. The Merchant (authenticator) can register the device with the Central Server, essentially registering your address for delivery of any information from an issuing institution. There is no need to authenticate the Merchant to subscribe other than providing a subscription credential (address) that can be used by issuers (Institution) to know where to deliver a package. The package contains public keys to authenticate signatures of data that the Merchant would receive from an owner providing identity data. This package delivery is once and periodically updated in accordance of the life cycle of certificates by an issuer. The Merchant never contacts the issuing Institution to authenticate an owner of Identity.



Clearly this interaction is now peer to peer for Authentication of Identity.



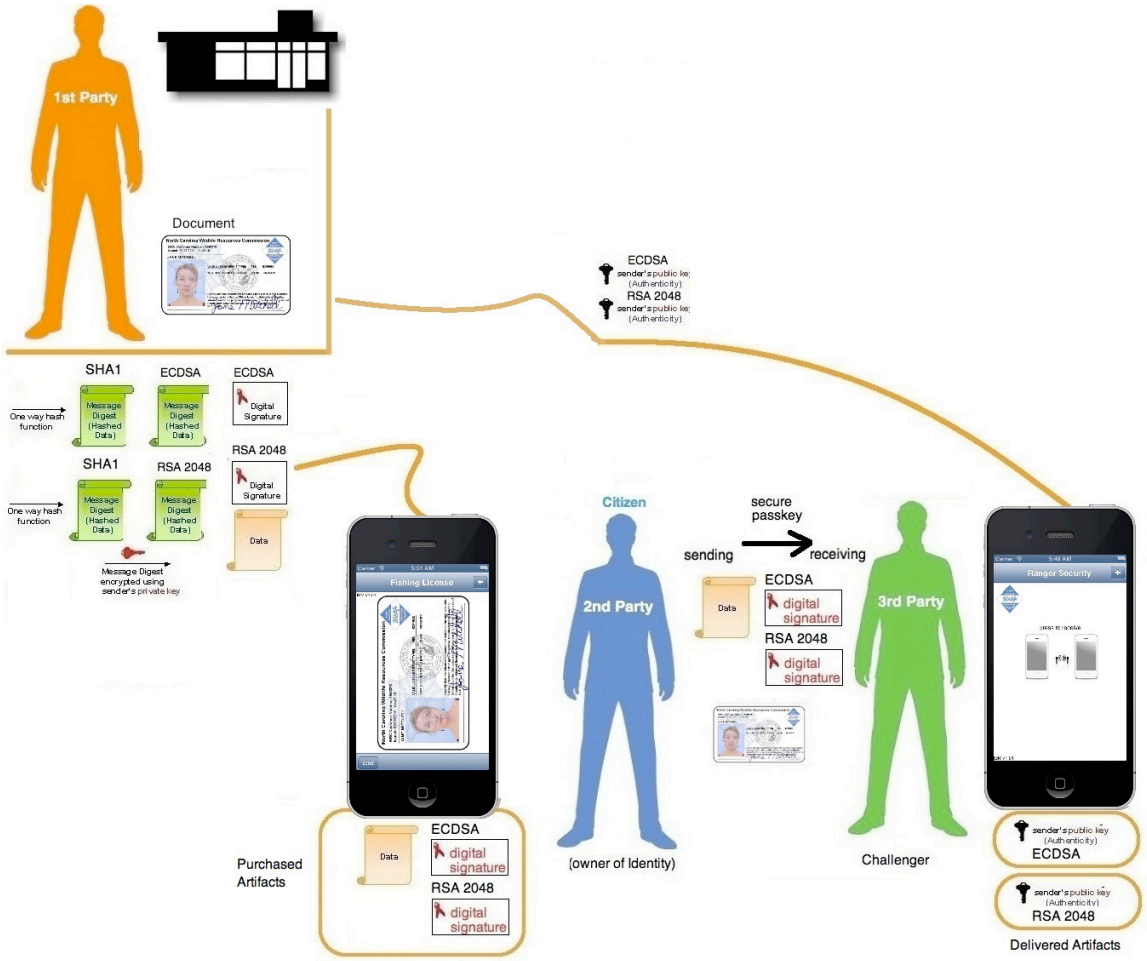
IBM additionally addresses the peer to peer validation for owner security of privacy information as well as safety for the Verifier. The peer to peer validation is shown below in which the Verifier (police officer) has initiated a challenge. The owner will receive a picture of the officer to know where the privacy information will be sent to fulfill the challenge request. Additionally the verifier has an installed configured role which is used by the owner to match selectable identity instruments needed for the context. The owner can choose traits that are sent to the verifier and the verifier can prove the traits belong to each other as well as authentic.



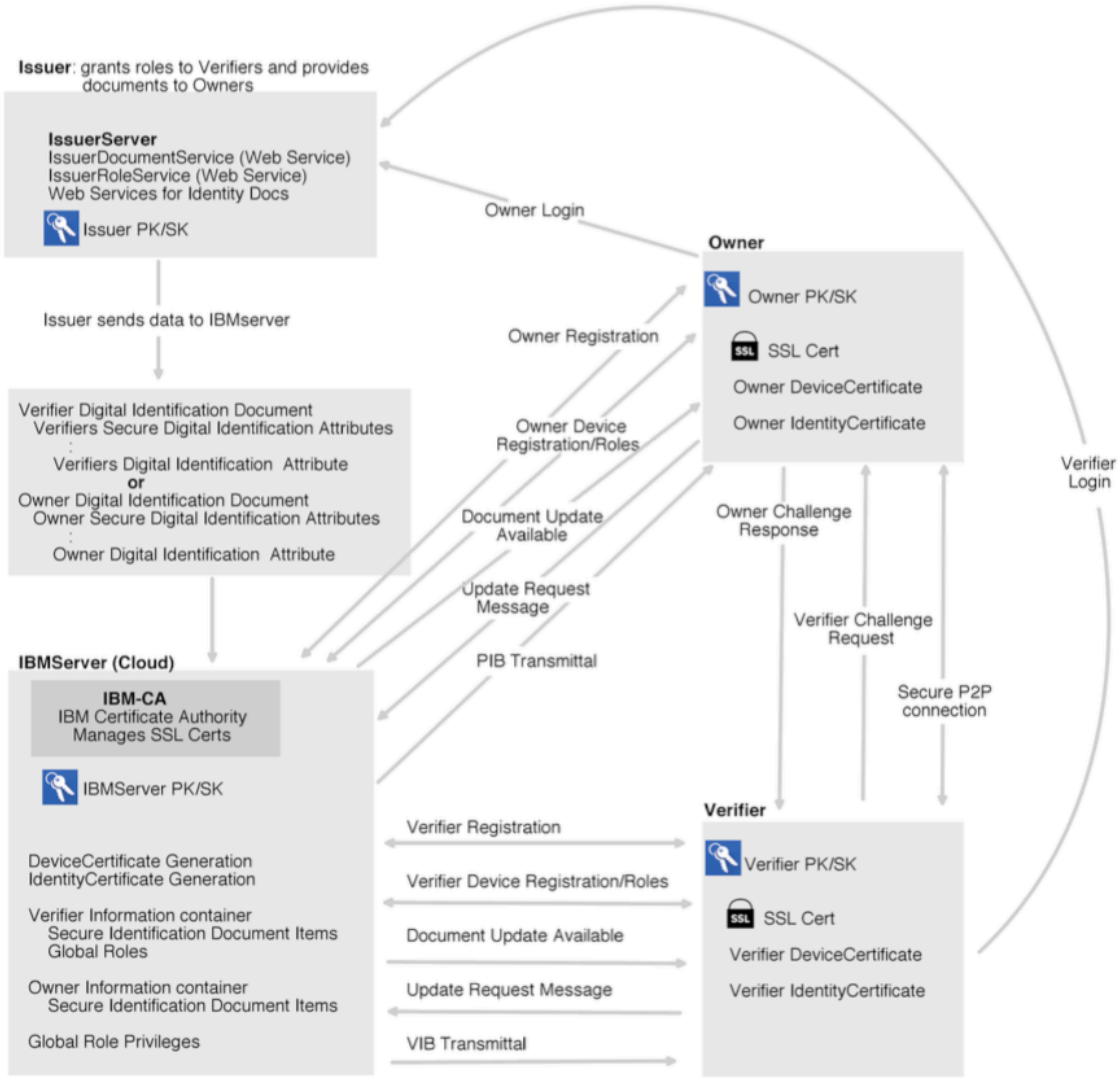
This process also solves the problem of multiple verifiers. For example, If there are three Bartenders at a restaurant vetting customers. The owner will get a picture of a bartender and if it is not the one asking for Identity the owner can swipe and the next Bartender will be shown.

Additionally for safety a Police officer can approach a car with his phone in his pocket and ask for Identity of the owner with both hands free. The owner can state it is digital of which the officer can say send it to me and walk away. The safety of the officer is greater than reaching his hand to obtain a thermal plastic instrument. When the officer receives the identity instrument the phone will vibrate and beep.

A closer simple view of the process for obtaining identity instruments is shown below. The owner obtains a driver's license from the issuing institution which is encrypted by the owner key with DSA traits called the Cryptoblob. The verifier obtains public keys to validate data and signatures for an authentication challenge to an owner from the issuing Institution.



The actual data and encryption model is shown below. There are also other aspects added to the Ecosystem such as Roles for Verifiers to automatically match owner identity instruments for a challenge request by the verifier.



Personal Identification Information

Control of Personal Identification Information (PII) is provided for the owner to deliver identity instruments in context of a request. For example, a 21 year old female is challenged to provide a Bar merchant identity instruments to be served. The female only has to show her picture and that she is over 21. There is no need to present name and stalking address. This process is through a Group Homomorphism for Digital Signature privacy control. It enables a disconnected environment for proofing and is superior to thermal plastic today. The owner has complete control of which traits to hand out for authenticating identity for privacy control. (patent 9,230,133, published Jan 5th 2016)

$$G \rightarrow H$$

$$\varphi_X(u+v) = \varphi_X(v) + \varphi_X(u)$$

Where is equal to means that it represents the same thing which is trust of the elements as a group.

φ is a function for a digital signature of data which includes **X** a unique identifier as part of the data.

If $\varphi_X(u+v)$ is a valid DSA with **X** a unique identifier then $\varphi_X(u)+\varphi_X(v)$ is a valid DSA each having **X** and are equivalent in trust as belong to the same group.

Example

Lets take an example of elements in two different groups Jane and Kris that should not share elements for trust.

Jane has two elements that define a group **A** which is a photo **p** and over21 **o**.

φ is a function for a digital signature of data. Then $\varphi(p+o)$ is a valid DSA from a Certificate Authority indicating this is a trusted group **A** all elements belong to each other.

Kris has two elements that define a group **B** which is a photo **r** and under21 **u**.

$\varphi(r+u)$ is a valid DSA from a Certificate Authority indicating this is a trusted group **B** all elements belong to each other.

If the Certificate Authority creates a DSA for each element in Jane

$\varphi(p) + \varphi(o)$ the information can be trusted but the membership as a group cannot. If the Certificate Authority (CA) creates a DSA for each element in Kris

$\varphi(r) + \varphi(u)$ the information can be trusted it came from the CA but the membership as a group cannot. The elements could be traded between Jane and Kris such as over21 and now Kris has compromised trust as a group though the data is trusted from a CA.

A Group Homomorphism for Digital Signature privacy control can be created such that the elements can stand on their own and knowledge of what group they belong to can be asserted.

$$G \rightarrow H$$

$$\varphi_x(u+v) = \varphi_x(v) + \varphi_x(u)$$

This is an important privacy control function for Identity. Identity contains many fields of information such as Photo, name, over21 and address. If you simply need to prove Photo and over21 there is no need to give your private home address out to strangers. For the case of Jane and Kris

Jane

$$\varphi_j(p+o) = \varphi_j(p) + \varphi_j(o)$$

Kris

$$\varphi_k(r+u) = \varphi_k(r) + \varphi_k(u)$$

Kris cannot trade an element of identity with Jane. This is not a valid DSA for a group

$$\varphi_k(r+u) \neq \varphi_k(r) + \varphi_j(o)$$

Kris cannot compromise his identity for age trading with Jane.

Lets show how this is done.

Jane has two privacy elements that define a group **G** which is a photo **p** and over21 **o**.

φ_j is a function for a digital signature of data that will include j a unique identifier to Jane when creating a valid DSA for data.

Then $\varphi_j(p+o)$ is a valid DSA from a Certificate Authority indicating this is a trusted group **G** all elements belong to each other.

A Group Homomorphism can be created for trust of the group using φ_j a function for a digital signature of data that will include j a unique identifier such as the following.

$$G \rightarrow H$$

$$\varphi_j(p+o) = \varphi_j(p) + \varphi_j(o)$$

The privacy elements $\varphi_j(p)$ can be trusted since it is a DSA and can be validated for its origin. The $\varphi_j(o)$ can be trusted also since it is a DSA and can be validated for its origin. The elements can be proven that they belong to each as a group since the DSA derived from φ_j uses the same unique identifier.

Kris has two elements that define a group **H** which is a photo **r** and under21 **u**.

For Kris φ_k is a function for a digital signature of data that will include k a unique identifier to Kris when creating a valid DSA for data.

Then $\varphi_k(r+u)$ is a valid DSA from a Certificate Authority indicating this is a trusted group **H** all elements belong to each other.

The privacy elements $\varphi_k(r)$ can be trusted since it is a DSA and can be validated for its origin. The $\varphi_j(u)$ can be trusted also since it is a DSA and can be validated for its origin. The elements can be proven that they belong to each as a group H since the DSA derived from φ_k uses the same unique identifier.

Kris cannot trade an element of identity with Jane. This is not a valid DSA for a group since the unique Ids would be different.

$$\varphi_{k(r+u)} \neq \varphi_{k(r)} + \varphi_{j(o)}$$

In group theory, the most important functions between two groups are those that "preserve" the group operations, and they are called homomorphisms. A function f : G → H between two groups is a homomorphism when

$$f(xy) = f(x)f(y) \text{ for all x and y in G}$$

Here the multiplication in xy is in G and the multiplication in f(x)f(y) is in H, so a homomorphism from G to H is a function that transforms the operation in G to the operation in H.

Example homomorphisms are shown below:

$$e^{x+y} = e^x e^y$$

$$\log_a(xy) = \log_a(x) + \log_a(y)$$

The log function Homomorphism shows an excellent example of binary operation of multiplication can translate to a binary operation of addition for a function.

Group Theory

In general a Homomorphism is the function operating on the composition of u and v gives us the same answer as the composition of that function operating on u and composition of that function operating on v. We get the same results which in our case is defined as the trust of a group.

Connected Digital Identity Model

The connected authentication required NIST model is shown below . The applicant (owner) becomes a subscriber to the CSP and is vetted to be a subscriber. This is not required by the new IBM innovation. Validating requires the verifier to connect to the relying party (RP) to validate. This only opens new conduits and opportunities for security threats and requires a connection. Additionally there are some more complicated constraints for adding the authenticator to the CSP. The authentication process requires the owner and verifier to connect which essentially is double the transactions to the relying party (RP). The replying party (RP) should not have to provide such financial infrastructure as well as new security issue conduits into the system. The NIST system is excerpted from the Special Publication 800-63-3 for Figure 4-1 shown below.

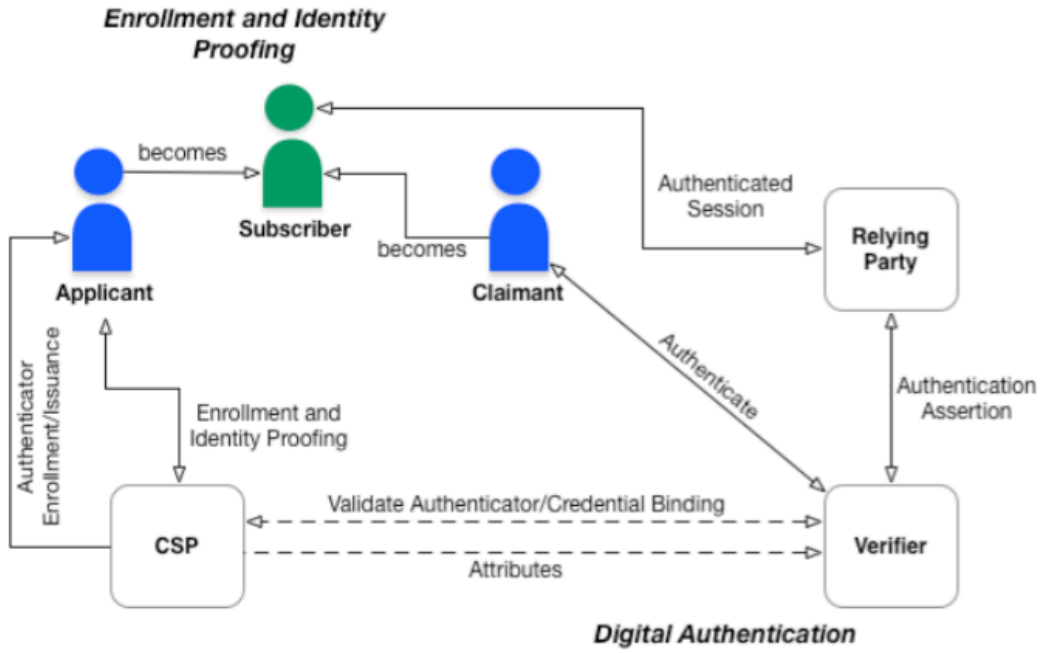


Figure 4-1. Digital Identity Model

Authentication is a double transaction based solution to Server infrastructures and a connected environment. Imagine 10,000 bars and restaurants open every Saturday night in North Carolina and these merchants need to authenticate a license with double the transactions to the Relying Party. Additionally the CSP contains derivative information of the applicant (owner) for identity instruments thereby distributing the information from its origin issuer and weaponizing that service as a target. This figure clearly diagrams the scope as a conversion of a peer to peer model that exists today for real life interaction of individuals to establish that a subject is actually who they claim to be for thermal plastic cards to a connected service model which has twice the transactions to the owner of record thereby increasing security issues to be resolved, scale issues, as well as serious financial infrastructure costs not needed previously for authentication of a driver's license.

This connected model removes the current features of paper/plastic today such as self-sufficency in satisfying one's basic need for authentication by a verifiier. There is no-phone-home requirement with paper/plastic. Going beyond paper/plastic and leaving in place the current no-phone-home requirement for a possible digital solution in a paper/plastic (disconnected) environment is listed below. Note that the NIST model for Guidelines of a Digital License does not enable the collate and presentation of multiple identity instruments required by some scenarios (eg: Pharmacy, Medical Provider). The new IBM innovation provides all these aspects on top of the current paper/plastic today.

- Selective delivery of non-repudiated privacy information
    - Ann can respond to a proof-of-age challenge request with identity traits (photo, age) from her driver's license without revealing additional PII.
- Self-sufficient in satisfying one's basic needs for authenticate and verify an identity challenge response
    - Officer Bob can verify an identity challenge response without needing to depend on secondary communications with the Issuing Authority.
- Provides proof of the integrity and origin of data via cryptographic means thereby yielding a more trust worthy and reliable solution over paper/plastic.
    - Officer Bob can trust the validity and freshness of information received in an identity challenge response.
- Intermixing identity traits from multiple documents to respond to any identity challenge request
    - Ann can respond to a challenge request with a photo from her fishing license and her address from her driver's license
- Immediate update and/or revocation
    - Ann need not wait several years for get her change of address reflected on her DL.
- Immediate reconstitution of your identities from a trusted delivery agent
    - Ann replaces a lost device and without contacting the issuing authorities she can immediate contact the delivery agent to prime her new device
- Avoidance of physical and close proximity interactions for safety purposes
    - Officer Bob need not closely approach a vehicle at a traffic stop just to physically receive identity information thereby avoiding placing himself in a potentially unsafe position. (blog link)
- Availability on multiple devices
    - Ann can reap the benefits of mobile convenience by registering multiple devices with her trusted delivery agent.
- Central access to multiple identity instruments
    - Ann must present two forms of photo ID to procure class 2 drugs
- Ability to present multiple identity instruments simultaneously
    - Ann can respond in a single action to a request for multiple identity documents (traffic accident requires 3 disparate documents: DL, Vehicle Registration, Insurance Card; Medical office requires 2 disparate documents: G3I, Healthcare Insurance Card)
- Protected access to personal identification information
    - Ann need not worry about her lost device containing numerous identity instruments; She can immediately purge the identity instruments from the lost device.
- Empowerment to grant consent to privacy information
    - Ann can provide Carl with a time restricted access to her Boat Registration.