Government Use Case

Laura Barnes has graduated from college and has her first job. She's decided to lease and insure a new car. The car dealer and insurance company both require Laura to present proof of employment and a driver's license.

A few weeks after getting her new car, she gets pulled over for a traffic volition. The officer asks her to present proof of her driver's license, auto registration and insurance. Let's compare how Laura could use a Decentralized Identity Network or a Consortium Identity Network to make the process easier and more secure for her, seamlessly protecting her identity.

In a Decentralized Identity Network, the participants would be...

- Laura
- The Department of Motor Vehicles (DMV)
- Laura's Employer
- Insurance Company
- Car Dealer
- Leasing Company
- Public permissioned network
- Police Officer

Decentralized Identity Network

...and they would take following steps:

Step 1
Laura obtains a driver's license

Step 2
She receives proof of employment from her employer

Step 3
She uses her driver's license and proof of employment to get approved for an auto lease

Step 4
She uses her driver's license and proof of employment to obtain auto insurance

Step 5
She uses her driver's license to register the new car

Step 6
The car dealer uses Laura's digital credentials to complete the sale

Step 7
Laura presents her proof of driver license, auto registration and insurance to the police officer

Decentralized Identity Network actions:

Examine > | Issue > | Hold > | Present > | Verify

Perform required vetting, due diligence, regulatory compliance and other tasks needed to establish confidence in making a claim about an identity trait. The documentation required for this process is typically not in digital form. The entity performing the vetting process takes on all liability about the claims they make.

In order for Laura to have obtained her driver's license, she had to meet the examination/vetting criteria for the issuance of a verifiable credential. Upon completion of the vetting process the government felt confident in making attestations (claims) about her name, date of birth, address, citizenship, and more.

Examine > | Issue > | Hold > | Present > | Verify

Generate and deliver a Credential comprised of a set of Claims in accordance with some predefined schema.

Laura's employer, leasing company, insurance company and the DMV have done their due diligence in examining Laura, issuing a cryptographically signed verifiable credentials attesting, respectively, to her proof of employment, lease agreement, vehicle insurance card, driver's license and vehicle registration. These verifiable credentials are based off a claim schema consisting of attested attributes from each issuer and their digital signatures. Claim schemas for her proof of employment, lease agreement, vehicle insurance card, driver's license and vehicle registration are published on the public, permissioned ledger along with each issuer's decentralized identifier (DID) for any verifier to resolve. Exchanges of these verifiable credentials are done point to point, directly with Laura, specific to each relationship she has. In this case, point to point with her employer, leasing company, insurance company and the DMV.

The car sale is completed, and Laura gets the keys to her new car and a digital bill of sale. The car dealer has performed its sales workflow business process, issuing a cryptographically signed verifiable credential attesting to the bill of sale for Laura's new car. This verifiable credential is based off a claim schema, which consists of the digitally signed attested attributes from the car dealer. The claim schema for the bill of sale is published on the ledger associated with the car dealer's decentralized identifier (DID) for any verifier to resolve.

Examine > | Issue > | Hold > | Present > | Verify

Individual or organization holds a credential.

- Upon completion of her vetting experience with the Government, Laura uses her digital wallet to connect with the Government's issuer service. Through this interaction she obtains her existing identity traits, in the form of a verifiable credential, and stores it in her digital wallet.
- Laura uses her digital wallet to establish personal (peer to peer) relationships with entities. Through this interaction she is issued a new credential in her digital wallet along with a private decentralized identifier (DID) that is unique to her relationship with the entity.
  - Employer: She requests a verifiable credential version of a proof of employment certificate from her employer's issuing service.
  - Leasing company: the car dealer provides Laura with a point-of-sale device that initiates a proof request from the leasing company's issuing service requiring her to present her driver's license and proof of employment.
  - Insurance company: the car dealer provides Laura with a point-of-sale device that initiates a proof request from the insurance company's issuing service requiring her to present her driver's license and proof of employment.
  - DMV: the car dealer provides Laura with a point-of-sale device that initiates a proof request from the government's vehicle registration issuing service requiring her to present her driver's license.

Examine > | Issue > | Hold > | Present > | Verify

User presents one or more credentials to an entity as proof of identity.

Laura (Person to Organization)
Laura needs to establish peer-to-peer identity relationships with organizations (her employer, leasing company, insurance company, DMV and car dealer) that issue her verifiable credentials. When she interacts with her identity relationships, she uses her digital wallet. She establishes a connection with each identity relationship, accepts a proof request that coincides with the organizations verification process and uses the corpus of her verifiable credentials in her digital wallet to selectively disclose the required identity traits necessary to send a proof response.

Laura (Person to Person)
Laura needs to establish peer to peer identity relationships with the police officer. She responds to an identity challenge (proof request) from the officer's smartphone. Her interaction with the officer can be online (connected to the web) or offline (not connected to the web) in cases where web access is unavailable to share her verifiable credentials. She accepts the proof request using the corpus of her verifiable credentials in her digital wallet to selectively disclose the required identity traits necessary to send a proof response

Examine > | Issue > | Hold > | Present > | Verify

Participants validate authenticity of issuer and holder, then consume data as defined through their verification process which can be verified through a web of trust rooted in the public ledger.

Laura (Person to Organization)
Before an organization can issue a verifiable credential to Laura, the organizations (employer, leasing company, insurance company, DMV and car dealer) must verify content received in a proof response and then process that information in accordance with organizational policies associated with the issuance of credentials. The organization uses the public, permissioned ledger to establish trust in the issuing organization that digitally signed each of the identity traits provided in the proof response. The ledger is used because each issuer's decentralized identifier (DID) is publicly visible and cryptographically verifiable.

Laura (Person to Person)
The officer must be able to quickly establish trust in authenticity of the information Laura has provided as well as the fact that the information represents claims about her. The officer must verify content received in a proof response and then process that information in accordance with government policies associated with traffic stops. The officer uses the public, permissioned ledger to establish trust in the issuing organizations that digitally signed each of the identity traits provided in the proof response. The ledger is used because each issuer's decentralized identifier (DID) is publicly visible and cryptographically verifiable.

Continue to Consortium Verification Network on next page

IBM **Blockchain** Trusted Identity™

Now let's see how Laura would use a Consortium Verification Network, which would consist of the following participants...

Laura

The Department of Motor Vehicles (DMV)

Laura's Employer

Insurance Company

Car Dealer

Leasing Company

Digital Lockbox Provider

Verification Network

Police Officer

Consortium Verification Network

...and they would take following steps:

Step 1

Laura choses her Digital Lockbox Provider, a founding member of the Verification Network

Step 2

Laura uses her Verification Network application to confirm identity traits known by identity providers in the Verification Network

Step 3

The leasing company uses the Verification Network to verify the claims made about Laura by the government and her employer before approving a lease agreement

Step 4

The insurance company uses the Verification Network to verify the claims made about Laura by the government and her employer before approving an insurance policy

Step 5

The DMV uses the Verification Network to verify the claims made about Laura by the government before registering her car

Step 6

The car dealer completes the sale of the new car to Laura

Step 7

The police officer uses the Verification Network to verify the information presented in paper form by Laura

Consortium Verification Network actions:

Note: The "Issue" action is not used in this network. See below for further details.

Examine > | Hold > | Present > | Verify

Perform required vetting, due diligence, regulatory compliance and other tasks needed to establish confidence in making a claim about an identity trait. The documentation required for this process is typically not in digital form. The entity performing the vetting process takes on all liability about the claims they make.

Registers Laura based on the vetting policies of the digital lockbox provider and the Verification Network. Laura is required to download a mobile app, Verified.Me, and is given an identity token to interact with the network via the digital lockbox provider. Laura is required to use the provided identity token in every transaction.

Issue

Generate and deliver a credential comprised of a set of claims in accordance with some predefined schema.

There is no concept of the issuing of credentials in a Consortium Verification Network. Laura's identity traits are known by the Verification Network and are confirmed by her and used by the Digital Asset Providers to respond to verification transaction requests by Digital Asset Consumers.

Digital Asset Providers in this scenario include the DMV, Laura's employer, insurance company and the leasing company.
Digital Asset Consumers in this scenario include the car dealer and police officer.

Examine > | **Hold >** | Present > | Verify

Individual or organization holds a credential.

Comprised of Digital Asset Providers who maintain systems of record about relationship they have with individuals like Laura.

Examine > | Hold > | **Present >** | Verify

User presents one or more credentials to an entity as proof of identity.

Prior to her employer and bank performing verification transaction requests as Digital Asset Consumers, Laura used her mobile app to provide consent to the Digital Asset Providers in the Verification Network.

Examine > | Hold > | Present > | **Verify**

Validate authenticity of issuer and holder then consume data.

- In accordance with the business workflow processes of the car dealer, several verification checks need to be performed by the salesman to complete the sale. Based on verbal information presented by Laura, the salesman executes several proof requests to the Verification Network to verify the data known by Digital Asset Provider:
  - The DMV verifies her Driver's License data
  - Her employer verifies her income and employment status
  - Her insurance company verifies her policy data
  - The leasing company approves a lease agreement based on successful verification of her income and employment status

Laura presents the officer with physical documents representing her driver license, auto registration and insurance cards. The officer uses a device in his patrol car to scan the barcodes on the documents to obtain Laura's identity traits. He then uses the same device to submit a proof request to the Verification Network to verify the data known by Digital Asset Providers (DMV, insurance company) and validated by Laura.