Healthcare Use Case

A physical exam advises a patient to get her bloodwork done from a local clinic by her. The patient could use a Decentralized Identity Network or a Consortium Identity Network to simplify the process while making protecting her identity. Below, we will see how the two processes are different from one another.

Decentralized Identity Network

On reaching the clinic, the patient is required to provide the prescription with the order of the bloodwork, the patient's proof of insurance, and driver's license. Therefore, the participants of the process would be – the patient, doctor's office, the clinic, her healthcare insurance company, and the Department of Motor Vehicles (DMV).

Digital Identity Network

The process would involve the following steps:

Step 1

The patient carries her insurance and driver's license credentials in her Insurance company and DMV-digital wallet.

Step 2

The doctor's office provides a bloodwork order digital credential after the patient's physical.

Step 3

The patient provides her insurance, driver's license and bloodwork order credentials at the clinic for her bloodwork.

Step 4

The clinic verifies the patient's credentials and does the blood work.

Decentralized Identity Network actions:

Examine > Issue > Hold > Present > Verify

The participants are vetted: Participants undergo thorough vetting to ensure adherence to regulatory compliance and instill confidence in their claim of an identity trait. The relating documentation are generally in hard copy, and all liability about the claims made lie on the entity performing the vetting process.

Examine > Issue > Hold > Present > Verify

Credentials are issued: Credentials consisting of a set of claims adhering with some predefined schema are generated and delivered by the participants. The DMV, the patient's health insurance company and her doctor's office issue a cryptographically-signed verifiable credentials validating her driver's license, insurance coverage and bloodwork order – all of which are based off a claim schema and digital signatures of the issuers. Claim schemas for her driver's license, insurance coverage and bloodwork released on the public, permissioned ledger in conjunction with decentralized identifier (DID) of each issuer for cross-checking.

Examine > Issue > Hold > Present > Verify

A credential is held by an individual or organization: After the patient has undergone vetting with the doctor's office, , insurance company, and the DMV, the patient is issued verifiable credentials by these trusted entities to store in her digital wallet.

A private, pair-wise decentralized identifier (DID) for the relationship she has with the doctor's office, the insurance company, and the DMW, are contained in each credential.

Examine > Issue > Hold > Present > Verify

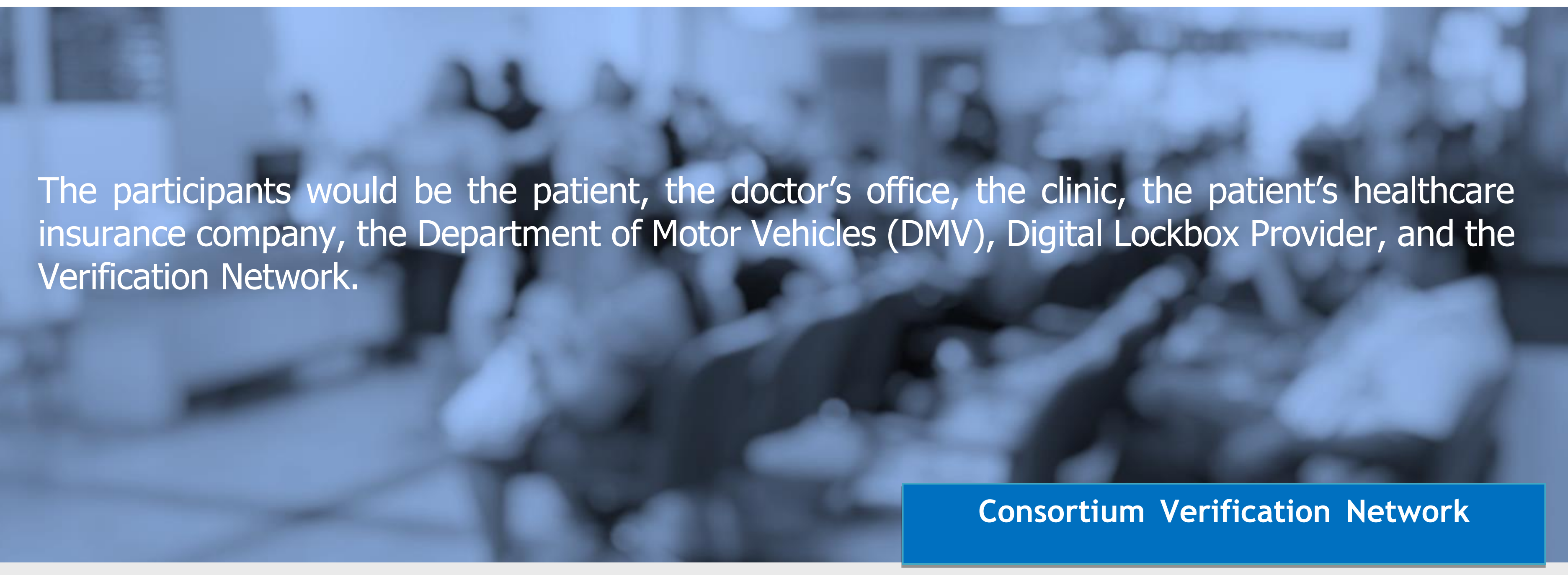
Individuals can present one or more credentials as proof of identity: The patient uses her digital wallet to share her verifiable credentials at the clinic, and accepts a proof request. This proof request uses the corpus of her driver's license, insurance and bloodwork order verifiable credentials in her digital wallet to selectively disclose the required identity traits needed to send a proof response.

Examine > Issue > Hold > Prese Verify

Participants validate authenticity of issuer, holder, and data – all through a public ledger: The patient has established relationships with her doctor and insurance provider. The patient uses her digital wallet to provide verifiable credentials to her insurance company and her doctor and collects proof requests for identity traits validated by trusted issuers. This proof request complies with the policies of the doctor's office and the insurance company who use the public, permissioned ledger to instill trust with other trusted issuers. This is possible because their individual decentralized identifier (DID) is publicly visible and cryptographically verifiable.

On reaching the clinic, the patient identifies herself using a point-to-point exchange with a device which, abiding by the policies of the clinic, requires a proof request. These would be her driver's license, insurance and bloodwork credentials issued by the DMV, insurance company and doctor's office, respectively. The public, permissioned ledger is used by the clinic to establish trust with the DMV, insurance company and doctor's office since their individual decentralized identifier (DID).

Continue to Consortium Verification Network on next page



The participants would be the patient, the doctor's office, the clinic, the patient's healthcare insurance company, the Department of Motor Vehicles (DMV), Digital Lockbox Provider, and the Verification Network.

Consortium Verification Network

...and they would take following steps:

Step 1

The patient picks a Digital Lockbox Provider — a founding member of the Verification Network

Step 2

The patient confirms her identity traits using her Verification Network application

Step 3

The doctor's office and the insurance company use the Verification Network to verify claims about the patient.

Step 4

The patient uses the Verification Network to verify claims about her from the DMV, her insurance company and her doctor's office at the clinic.

Consortium Verification Network actions:

Examine > Hold > Present > Verify

Thorough examination - Participants undergo thorough vetting to ensure adherence to regulatory compliance and instill confidence in their claim of an identity trait. The relating documentation are generally in hard copy, and all liability about the claims made lie on the entity performing the vetting process.

The patient is registered based on the vetting policies of the Digital Lockbox Provider and the Verification Network. She receives an identity token that she will have to use in every transaction and interaction with the network.

Issue

Credentials are issued: Credentials consisting of a set of claims adhering with some predefined schema are generated and delivered by the participants. However, credentials are not issued in a Consortium Verification Network. The patient's identity traits are confirmed by the Verification Network and used by Digital Asset Providers to respond to verification transaction requests by Digital Asset Consumers. In this case, the DMV, the patient's insurance company and the doctor's office make up the Digital Asset Providers, while the patient's health insurance company, doctor's office and the clinic would make up the Digital Asset Consumers.

Examine > **Hold >** Present > Verify

.

A credential is held by an individual or organization: Digital Asset Providers maintain records of relationships they have with individuals like the patient.

Examine > Hold > **Present >** Verify

Individuals can present one or more credentials as proof of identity: The patient can now use her digital wallet to provide consent to Digital Asset Providers in the Verification Network. However, the patient has to be online to provide consent of sharing her identity.

Examine > Hold > Present > **Verify**

Verification of authenticity of issuer and holder, followed by consumption of data: When the patient provides identity traits attested to by known and trusted issuers to the insurance provider and doctor she picks. These two in their turn use the Verification Network to verify data known by Digital Asset Providers and validated by the patient. The patient's request to get her bloodwork done reaches the clinic which asks her to prove identity traits that are validated by trusted issuers on the network. In this case, the trusted issuers are the DMV, the patient's insurance company and her doctor's office.