OPEN IDENTITY EXCHANGE

Making Digital ID a Success

OIX Trust Framework Overview for ToIP V2

OIX New Trust Framework

- The OIX Trust Framework has been re-written to be embracing of self sovereign identities whilst remaining technology agnostic.

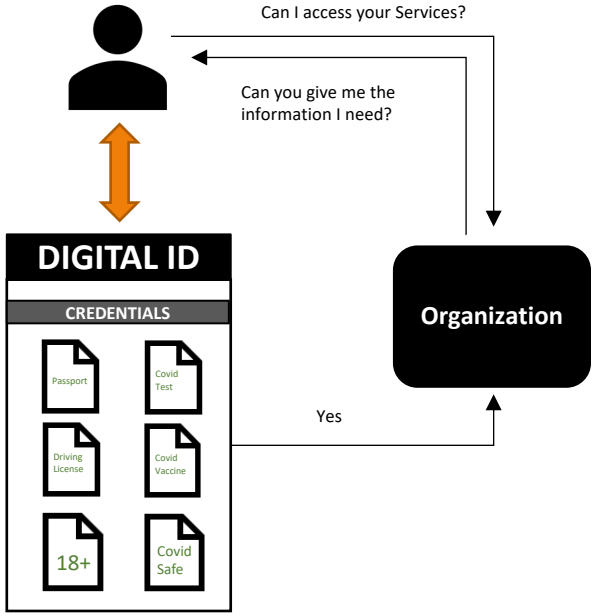
- It remains user centric and calls for Digital IDs to be 'smart' and help the user answer the complex questions organisations ask of them, such as: "Are you over 18?", "Are you COVID safe?" or "Are you able to meet my level of assurance requirements?".

- It focusses on the rules and governance need to make Digital Identity ecosystems successful and acceptable to all parties.

OIX New Trust Framework

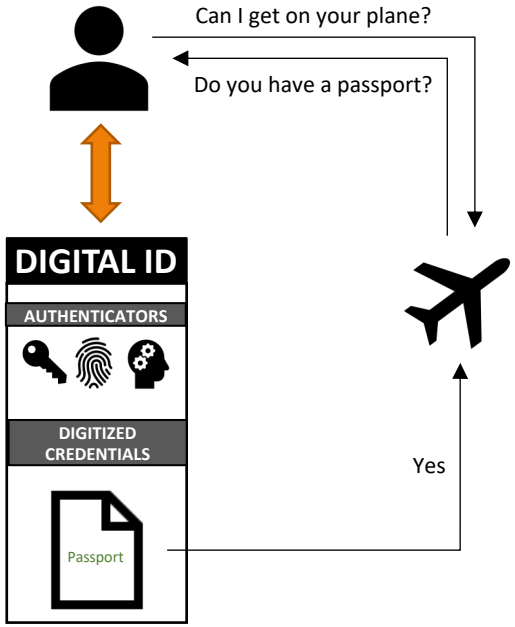
- Key features of a Digital Identity that the framework supports are:
  - The Digital ID works out what a user needs to meet an organizations business rules using a **rules engine** or **rules agent**, and helps the user gather, derive and present credentials to meet the organizations needs.
  - The Digital ID can carry **digitized versions** of existing credentials, such a passport, driving license, vaccine certificate or relevant qualifications.
  - The Digital ID can also **derive credentials** that show users meet the business rules of an organization, such as being over 18, COVID safe or meeting a specific “level of assurance”.
  - Organizations can also choose to allow users to use their **Digital ID to access an account** they hold with them. Thus, removing the need for them to issue their own logon authenticators (e.g., user IDs and passwords).

What is a Digital ID?



- A Digital ID is a set of (verified) digital Credentials.
- Examples of Credentials include:
  - Digtized real world credentials,
    - Driving licence
    - Passport
    - Vaccine Certificate
  - Derived Credentials:
    - Over 18
    - Covid Safe

What is a Digital ID?

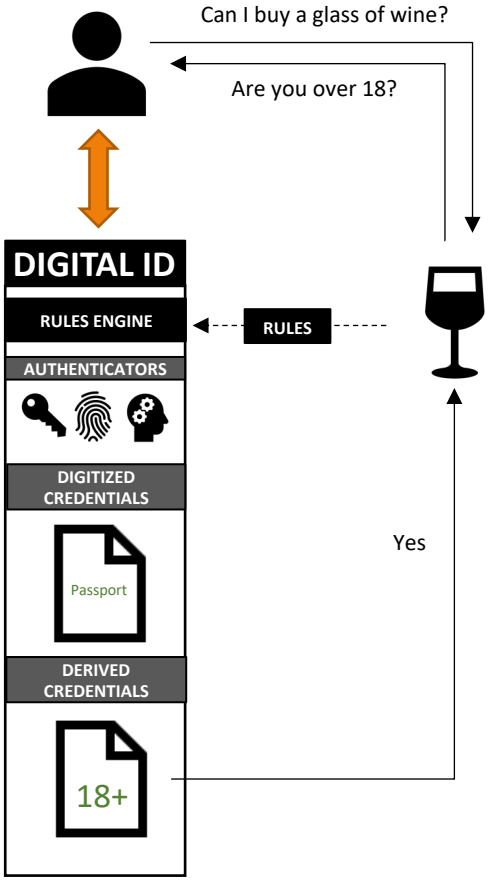


- Organizations ask the user for information. The user's Digital ID enables them to gather and provide that information.
- The simplest implementation of this is providing a Digitized version of a real-world Credential, such as a passport, driving license, covid vaccine or qualifications.
- The Digitized Credential must have been verified as belonging to the user.
- Authenticators are used to identify the user is the owner of the Digital ID.

Digtized Credential

Claims	Name, Address, DoB, DL#
Evidence - Type	Driving License
Evidence - How Verified	Scan and Selfie Cross Check
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Signature	############
Authenticators	Auth 1, Auth 2

What is a Digital ID?



- Organizations might not ask the user for a specific Digitized Credential but might ask for information that can be derived from one or more credentials.
- For example, the user can provide a Derived Credential that says they are Over 18.
- This could be derived programmatically from a digitized credential that has been verified as belonging to the user. The digitized credential itself does not need to be shared with the wine seller.
- The Rules for deriving Over 18 are determined by a Rules Engine. For instance, a rule might be that a) the Over 18 proof must be derived from a government issued credential and b) the government credential must have been verified as belonging to the user to an agreed standard and c) the user has used authenticators to access the digital ID that prove this is the genuine user.
- Organizations must be able to set their own rules.

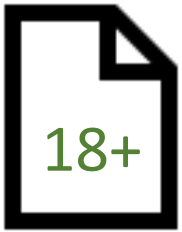
Selective Disclosure

Digtized Credential

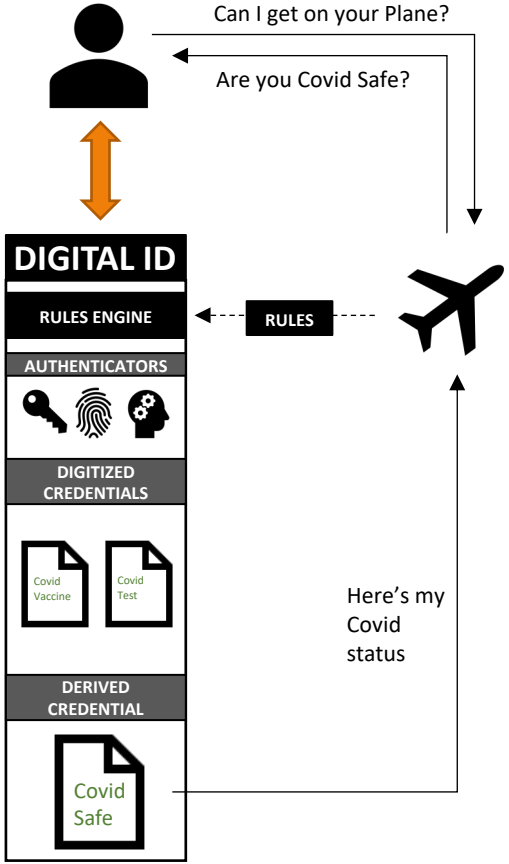
Claims	Name, Address, DoB, DL#
Evidence - Type	Driving License
Evidence - How Verified	Scan and Selfie Cross Check
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Signature	############
Authenticators	Auth 1, Auth 2

Selectively Disclosed Credential

Claims	Over 18
Evidence - Type	Driving License (Selective)
Evidence – Derived From	Driving License
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Signature	############
Authenticators	Auth 1, Auth 2

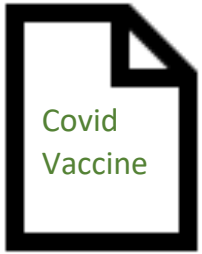


What is a Digital ID?



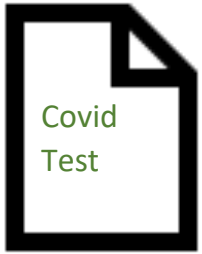
- To answer an organizations question, a complex set of rules might be required that may require several digitized credentials to be gathered.
- Here we use a Covid Safe example.
- The rules for a COVID Safe status might be: a vaccine course from a list of approved types completed within the last 12 months PLUS a negative test from a list of approve types within the last 72 hours.
- Rules may vary by use case, trust framework or individual organization
- Many Derived Credentials are point-in-time and need to re-assessed at point of next request.
- Also, Digitized Credentials may expire or be revoked. In which case and other credentials derived from them may no longer be valid.

Derived Credentials



Digtized Credential

Claims	Vaccine Date, Vaccine Type
Evidence - Type	COVID Vaccination
Evidence - How Verified	By Issuer
Evidence - Rules Applied	National Health Policy
Issuer	National Heath Authority
Signature	############
Authenticators	Auth 1, Auth 2



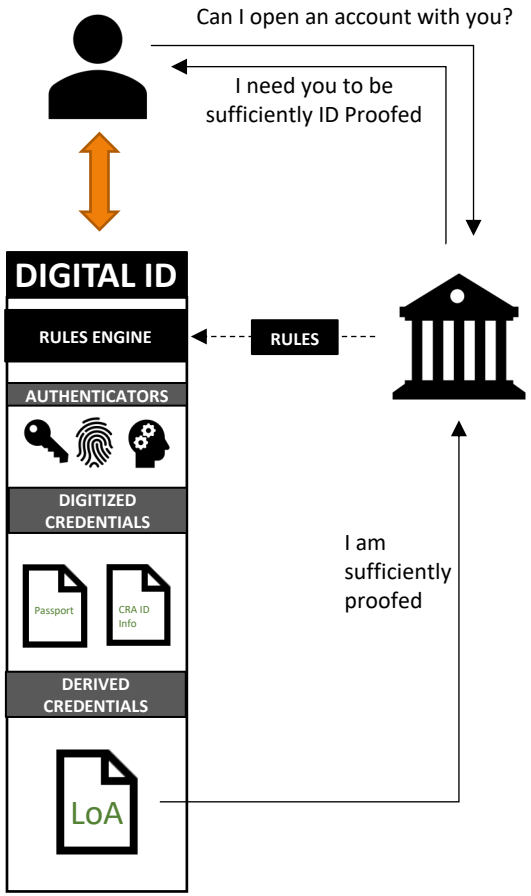
Digtized Credential

Claims	Test Date, Type and Result
Evidence - Type	COVID PCR Test
Evidence - How Verified	By Issuer
Evidence - Rules Applied	Airline Health Policy
Issuer	Pharmacist
Signature	############
Authenticators	Auth 1, Auth 2

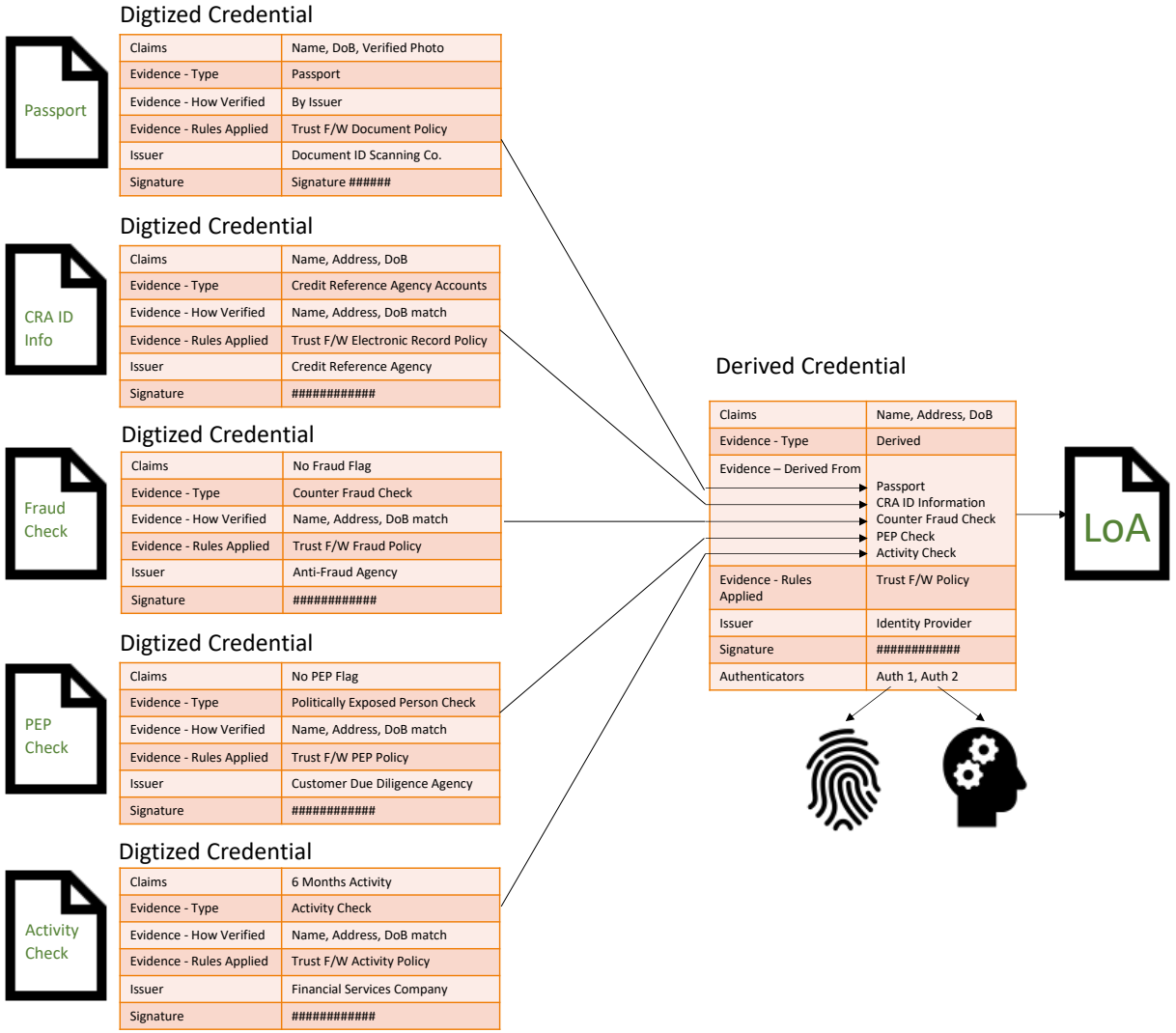
Derived Credential

Claims	COVID Safe
Evidence - Type	Derived
Evidence – Derived From	COVID Vaccination COVID PCR Test
Evidence - Rules Applied	Airline Heath Policy
Issuer	Identity Provider
Signature	############
Authenticators	Auth 1, Auth 2

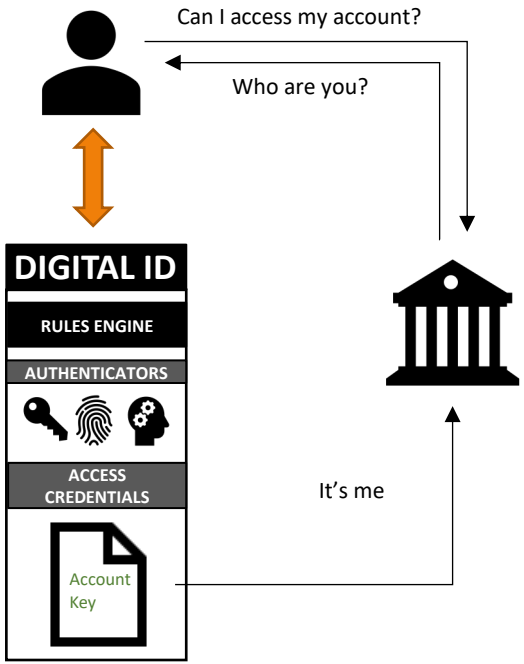
How does the Service Provider know the user is who they are claiming to be?



- Trust that the user is the genuine individual is derived from the credentials gathered by the user.
- For example, a photo from a passport or driving license cross checked with a selfie of the user, can be used to verify that this is the genuine user. Or a logon to online banking.
- Many Digital ID ecosystems assign “levels of assurance” or “levels of confidence” to the user’s ID based on assessing credentials that have been gathered.
- Higher levels of assurance usually also need multiple robust Authenticators to be “bound” to the users as part of the proofing process, to provide multi-factor authentication.
- A Levels of Assurance is a form of Derived Credential. They are dynamic and need to be continually re-assessed as the users' credentials expire and fraud risks are re-assessed.
- The process is handled by the Rules Engine. The user sees that they are asked to gather certain credentials and set up specific authenticators. They will not usually be aware they have achieved a specific Level of Assurance.
- A user may have many different Levels of Assurance for different use cases and organizations.
- Some trust framework may also require that the credentials used to derived a level of assurance are shared with the organization.

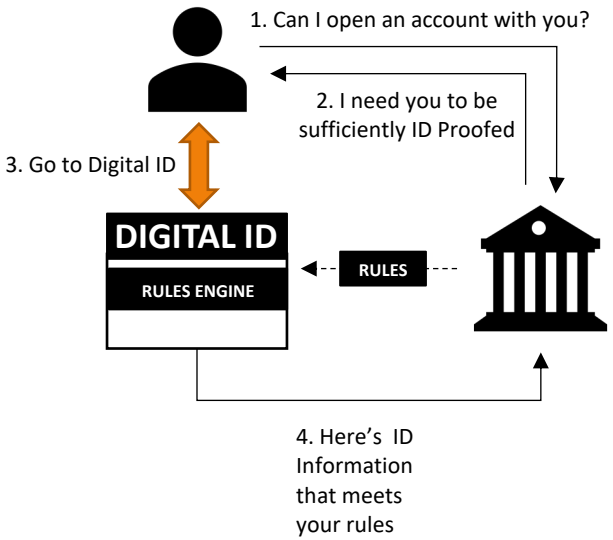

Digtized Credential
Passport
Claims
Name, DoB, Verified Photo
Evidence - Type
Passport
Evidence - How Verified
By Issuer
Evidence - Rules Applied
Trust F/W Document Policy
Issuer
Document ID Scanning Co.
Signature
Signature ######
Digtized Credential
CRA ID Info
Claims
Name, Address, DoB
Evidence - Type
Credit Reference Agency Accounts
Evidence - How Verified
Name, Address, DoB match
Evidence - Rules Applied
Trust F/W Electronic Record Policy
Issuer
Credit Reference Agency
Signature
############
Digtized Credential
Fraud Check
Claims
No Fraud Flag
Evidence - Type
Counter Fraud Check
Evidence - How Verified
Name, Address, DoB match
Evidence - Rules Applied
Trust F/W Fraud Policy
Issuer
Anti-Fraud Agency
Signature
############
Digtized Credential
PEP Check
Claims
No PEP Flag
Evidence - Type
Politically Exposed Person Check
Evidence - How Verified
Name, Address, DoB match
Evidence - Rules Applied
Trust F/W PEP Policy
Issuer
Customer Due Diligence Agency
Signature
############
Digtized Credential
Activity Check
Claims
6 Months Activity
Evidence - Type
Activity Check
Evidence - How Verified
Name, Address, DoB match
Evidence - Rules Applied
Trust F/W Activity Policy
Issuer
Financial Services Company
Signature
############
Derived Credential
Claims
Name, Address, DoB
Evidence - Type
Derived
Evidence – Derived From
Passport
CRA ID Information
Counter Fraud Check
PEP Check
Activity Check
Evidence - Rules Applied
Trust F/W Policy
Issuer
Identity Provider
Signature
############
Authenticators
Auth 1, Auth 2
LoA

Using a Digital ID to logon to an Organization



- Another feature of Digital IDs is that the user can use a Digital ID to logon to the organization again and again.
- Users use Facebook, Apple and Google IDs to do this all the time – they are acting as a form a Digital ID, but with no level of assurance expressed.
- The organization would issue the User with an Access Credential that is their Account Key for that organization.
- Or many organizations could rely on a generic Account Key created by the Digital ID.
- Next time the user interacts with the organization they present them with their Account Key to show them who they are.
- The organization may require authenticators of a particular type or level of quality in order to trust the Digital ID.

Rules Engines



A Digital ID needs to be able to interpret the rules required to meet the needs of a particular use case.

The rules might be:

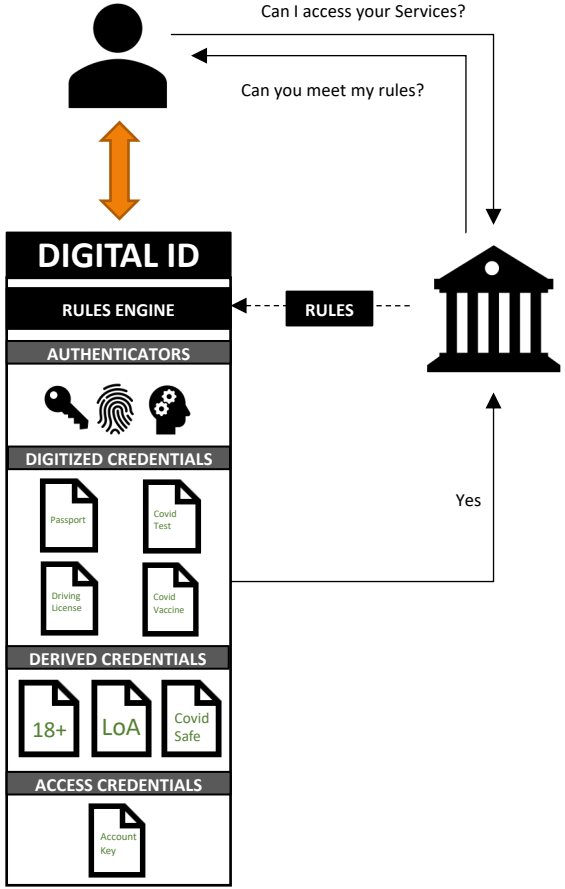
- Relying specific rules
- Rules defined by the framework, scheme or IdP as part of their services.

Rules might:

- Require specific type of Digitized Credential is required, e.g. a passport from a ICAO recognized passport authority.
- Define how a Derived Credential is determined e.g. Over 18 must come from a passport or driving license issued to the user by a Direct Issuer.
- Define specific Authenticators are required: e.g. 2 factor from one of possession, inherence or knowledge.
- Define a level of assurance determined using an Identity Assurance model.

A Digital ID will typically have a Rules Engine to allow it to interpret rules.

Putting it all together



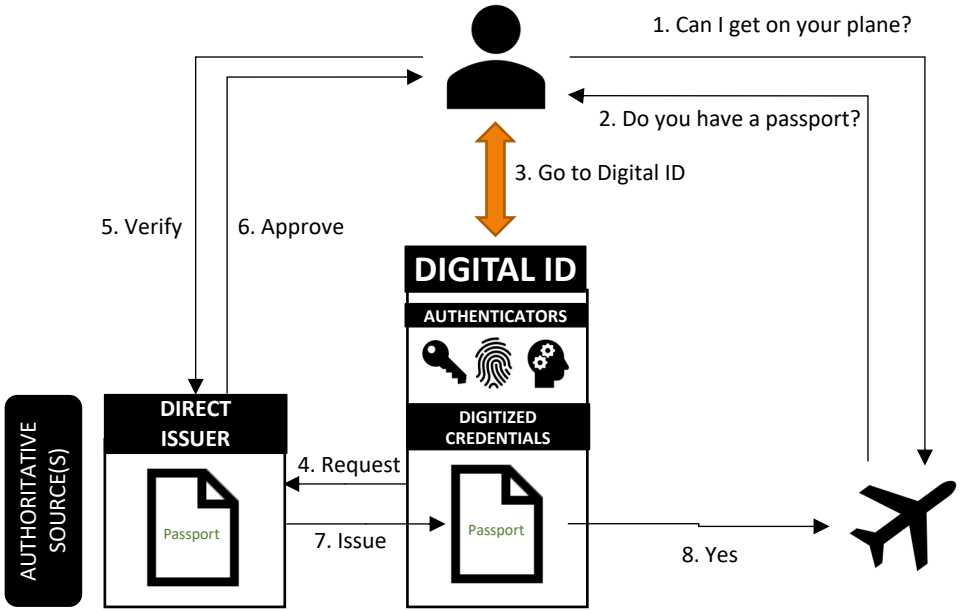
- Users can use a Digital ID to **confirm who they are**, and **share other important information about themselves**, to many different organizations who they want services from.
- The Digital ID **works out what a user needs** to meet an organizations business rules **using a rules engine** or rules agent, and helps the user gather, derive and present credentials to meet the organizations needs.
- It can carry **digitized versions of existing credentials**, such a passport, driving license, vaccine certificate or relevant qualifications.
- It can also **derive credentials** that show users meet the business rules of an organization, **such as being over 18, COVID safe** or meeting a specific **"level of assurance".**
- Organizations can also choose to allow users to use their **Digital ID to access an account** they hold with you. Thus, removing the need for you to issue your own logon authenticators (e.g., user IDs and passwords).

OPEN IDENTITY EXCHANGE

Making Digital ID a Success

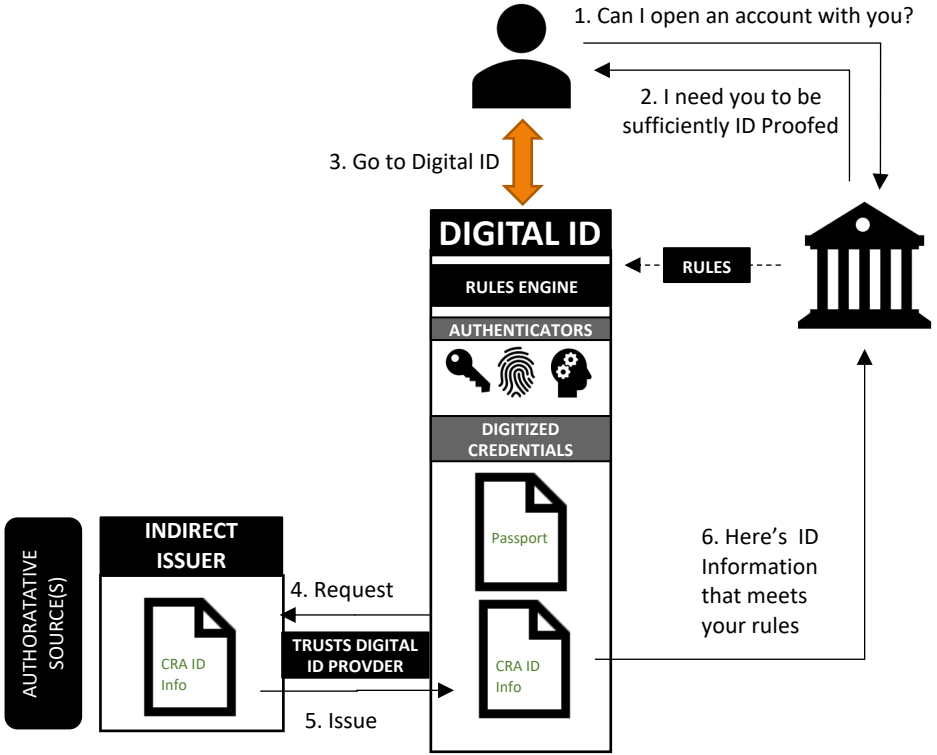
How does a Digital ID Gather Credentials and Establish a Chain of Trust?

What if the user does not have a Credential that's required?



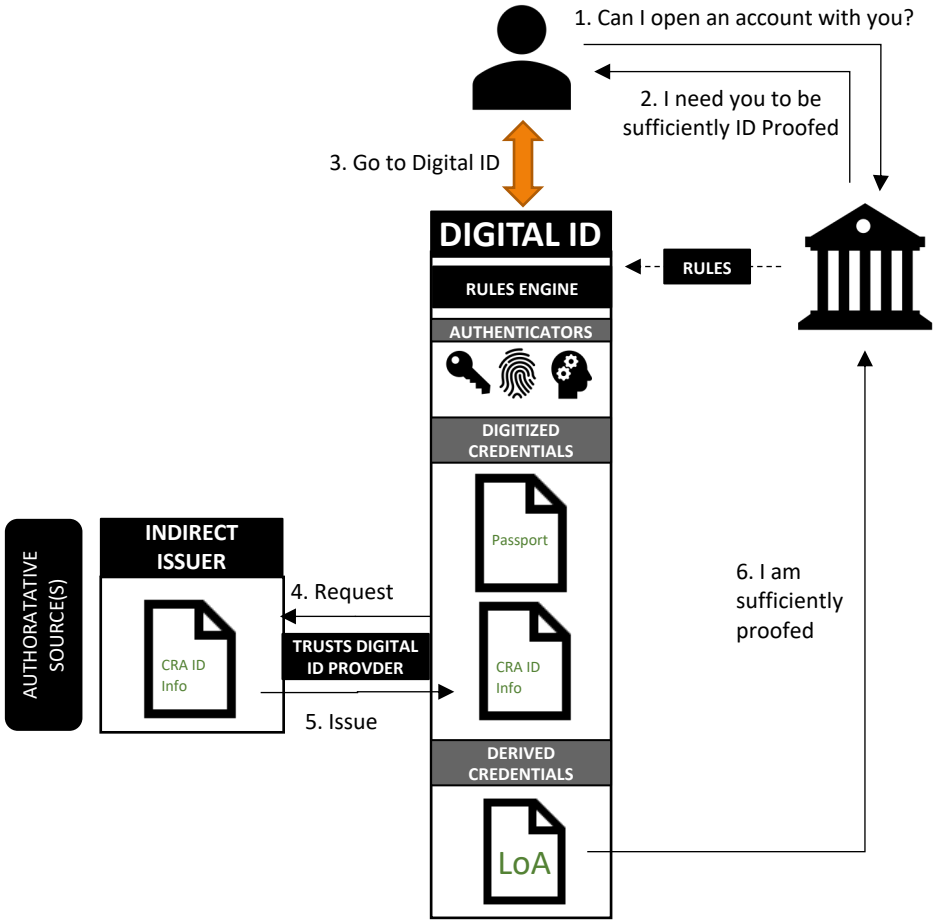
- The User can get a Digitized Credential from an Issuer.
- This could be the Authoritative Source of the credential, such as a government passport office, or a third party that creates a trusted credential using the source issued document and / or data.
- Third party credential issuers may act as an aggregator for several authoritative sources of the same information, such as passport agencies, licensing agencies or educational institutions.
- In this case the Credential Issuer interacts DIRECTLY with the user to verify who they are before issuing the credential to them – thus we call them a Direct Issuer
- The trust in the credential can be traced back to the Direct Issuer.

What if the user does not have a Credential that's required?



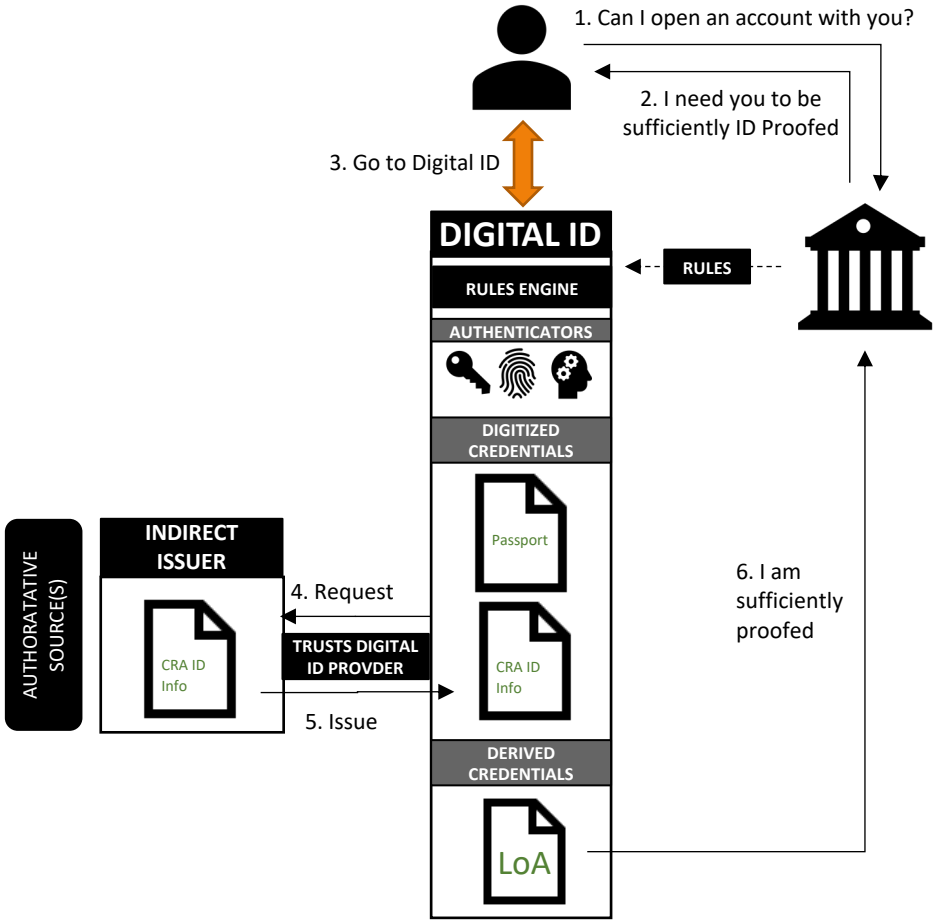
- The Digital ID might get a credential for the user, with the users consent, from a credential Issuer that trusts that the Digital ID Provider trusts the user.
- Third party credential issuers may act as an aggregator for several authoritative sources of the same information.
- In this case the credential Issuer does not interact directly with the user to verify who they are, they trust the Digital Identity Provider has verified the user - thus we call them an Indirect Issuer.
- The Indirect Issuer does not verify who the user is themselves.

What if the user does not have a Credential that's required?



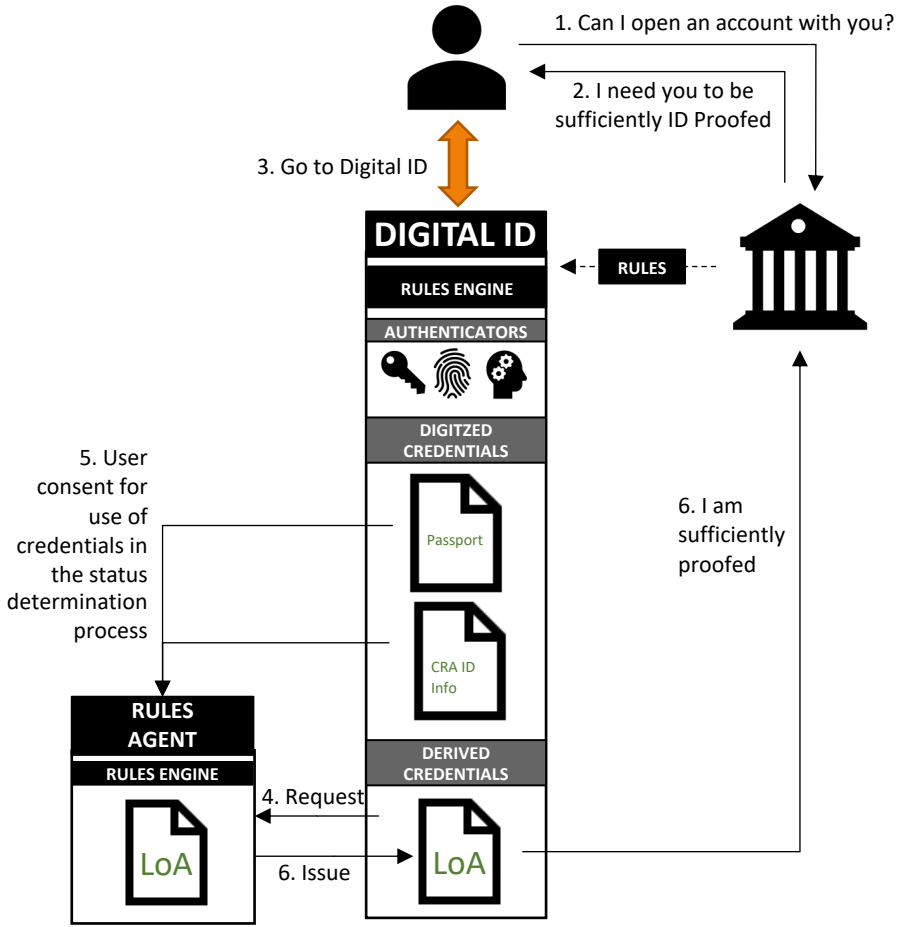
- A Digital ID must help derive credentials to meet the rules of the organizations the user is interacting with. A good digital ID will help the user through the process, guiding them to gather credentials to meet the often-complex rules of organizations.
- The Digital ID rules engine can combine the credentials, direct and indirect, to create a derived credential that is the level of assurance the organization requires.

What if the user does not have a Credential that's required?



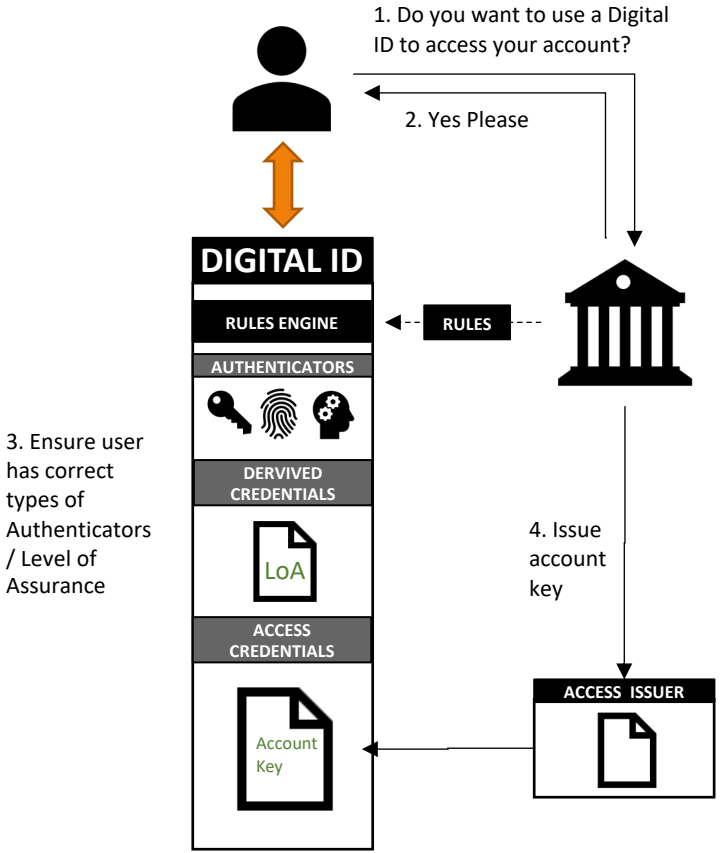
- A Digital ID must help derive credentials to meet the rules of the organizations the user is interacting with. A good digital ID will help the user through the process, guiding them to gather credentials to meet the often-complex rules of organizations.
- The Digital ID rules engine can combine the credentials, direct and indirect, to create a derived credential that is the level of assurance the organization requires.

Using a Rules Agent



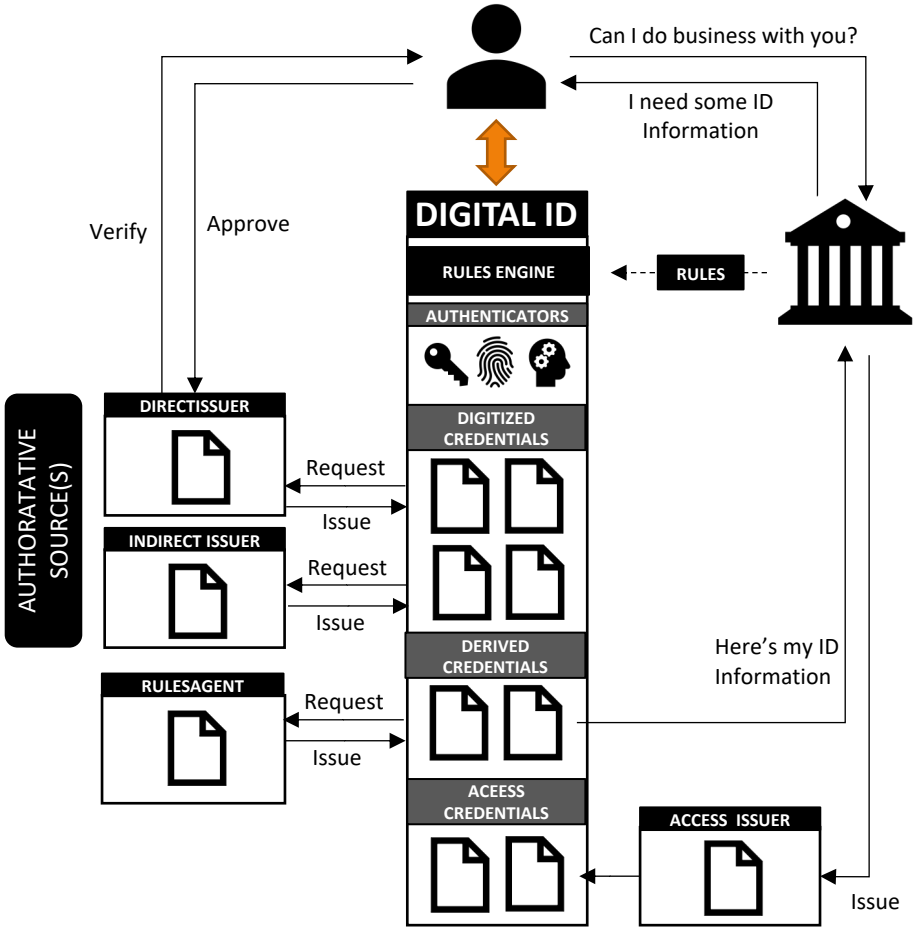
- A Derived Credential may not be created directly by the Digital ID, but may be created by a Rules Agent. The Rules Agent reads Digitized credentials to derived the new Credential
- Like with the background issuer, the user may not interact directly with the Rules Agent. The Digital Identity Provider may call the Rules Agent directly with the user's consent, passing them the required credentials to make the determination.
- Who the Rules Agent is could be a preference of the organization asking for the ID information.

Setting up a User's Digital ID to allow Access to an Account



- The organization needs to securely connect the users Digital ID to their account as the access mechanism.
- The user may need to have the right strength of Authenticators to meet the organizations needs.
- Our example here shows the organization issuing the trusted user with an account key that would be unique to the user and only presentable via that users digital ID.
- The Account Key may contain the access Authenticator requirements for the Organization.
- The Organization is effectively the credential issuer for the Account Key. We call this an Access Issuer

Adding the other roles to the overall picture



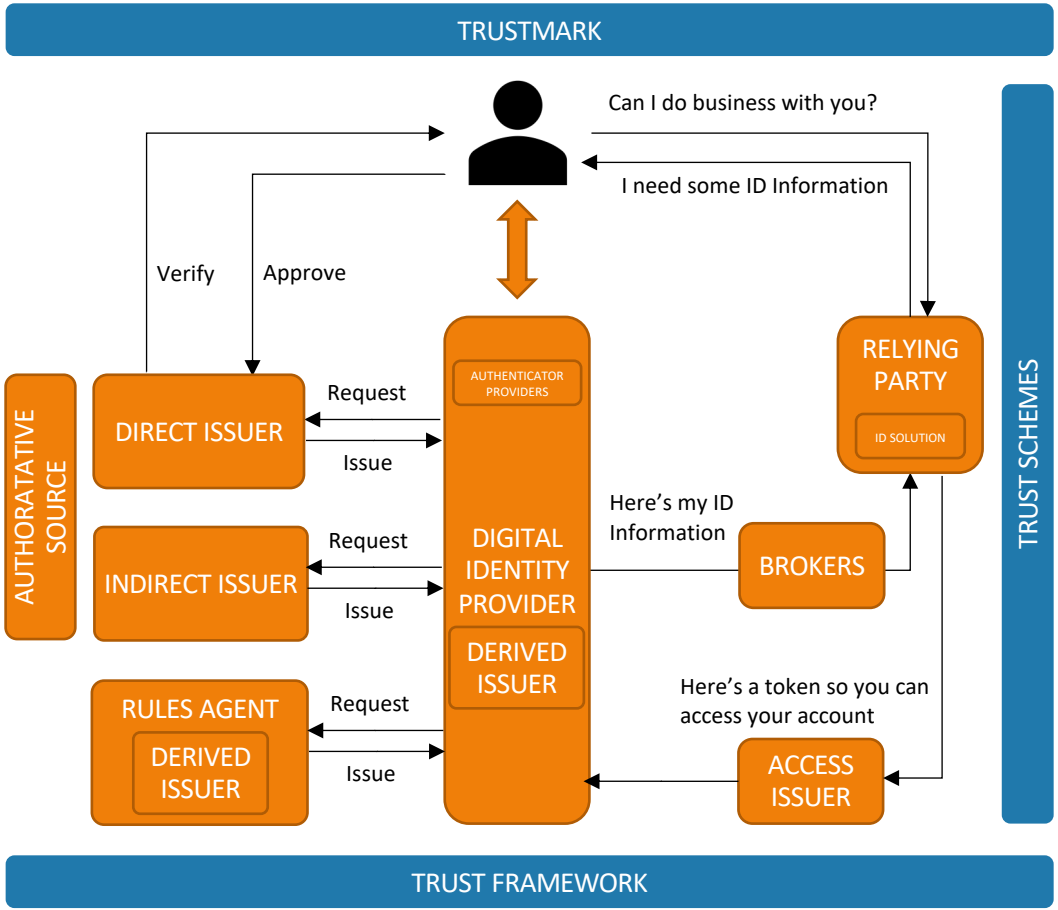
- Key features of a Digital Identity that the framework supports are:
  - The Digital ID works out what a user needs to meet an organizations business rules using a **rules engine** or **rules agent**, and helps the user gather, derive and present credentials to meet the organizations needs.
  - The Digital ID can carry **digitized versions** of existing credentials, such a passport, driving license, vaccine certificate or relevant qualifications.
  - The Digital ID can also **derive credentials** that show users meet the business rules of an organization, such as being over 18, COVID safe or meeting a specific "level of assurance".
  - Organizations can also choose to allow users to use their **Digital ID to access an account** they hold with them. Thus, removing the need for them to issue their own logon authenticators (e.g., user IDs and passwords).

OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Roles in the Ecosystem

Roles in the ID ECOSYSTEM



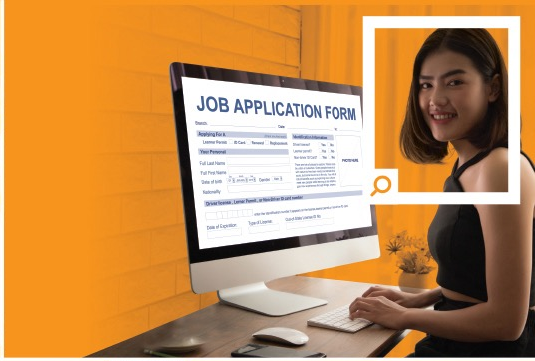
- The Digital Ecosystem comprises the following roles:
  - Users
  - Relying Party
  - Brokers
  - Digital Identity Provider
  - Authenticator Provider
  - Direct Issuers
  - Indirect Issuers
  - Derived Issuer
  - Rules Agent
  - Authoritative Sources

- The Digital Ecosystem governance comprises
  - Trust Framework
  - Trust Mark
  - Possibly, Trust Schemes

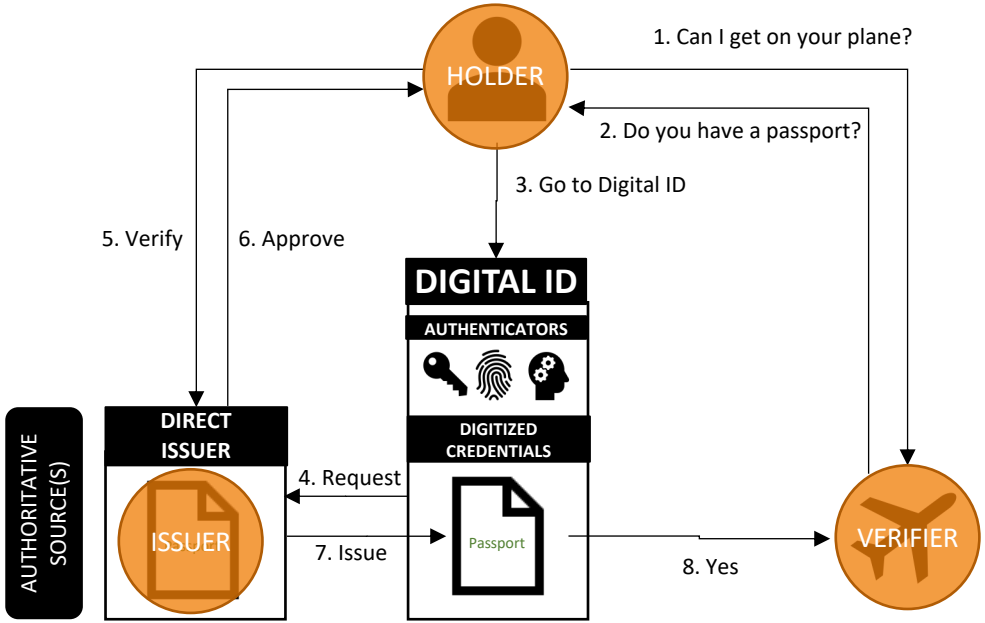
OPEN IDENTITY EXCHANGE

Making Digital ID a Success

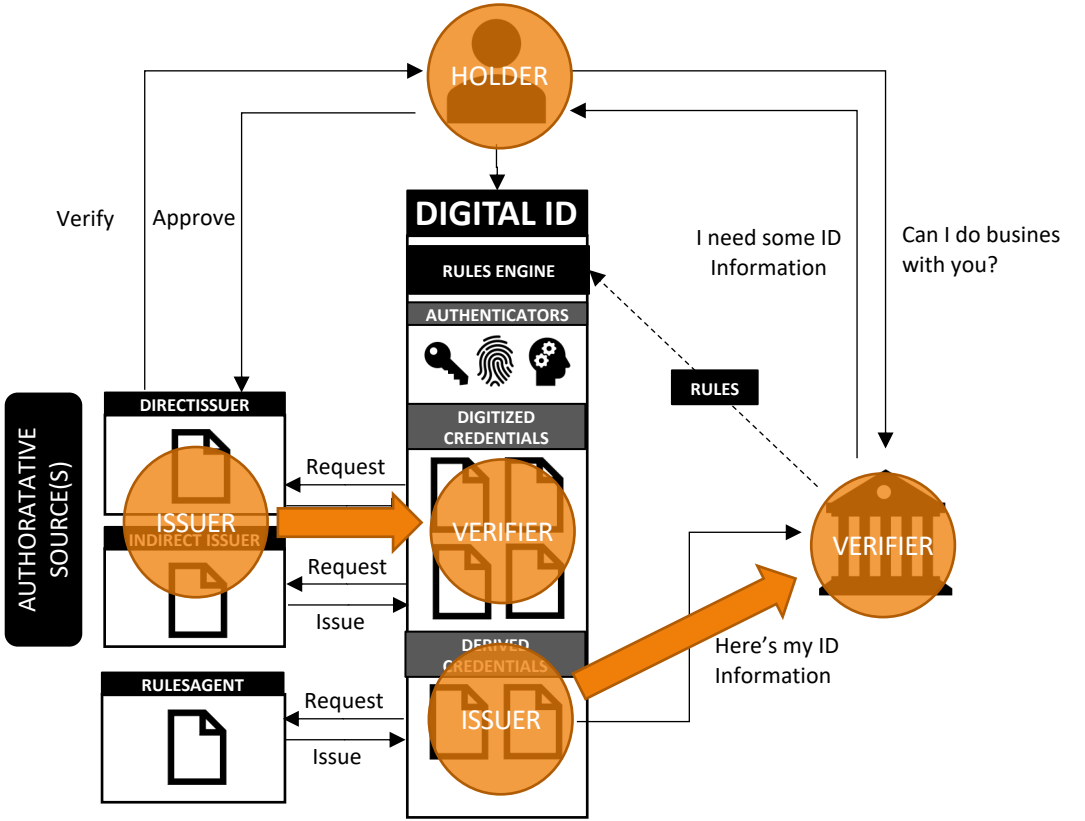
SSI Alignment



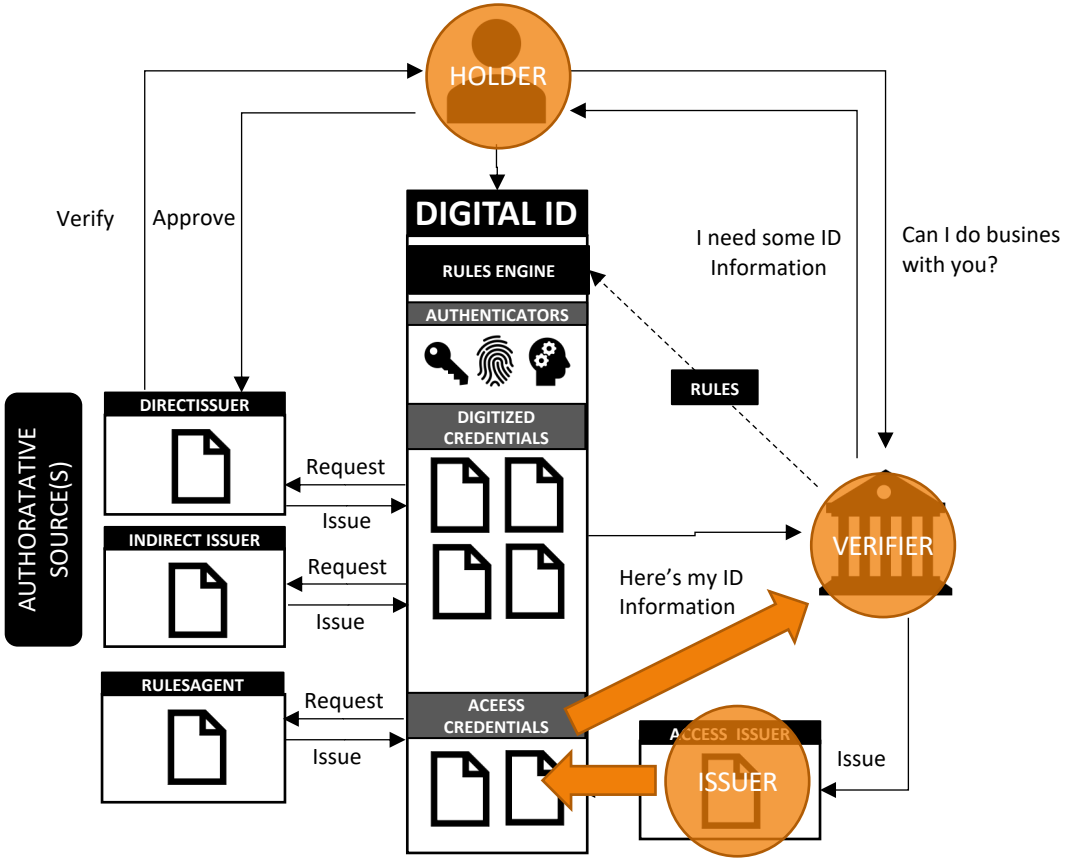
SSI Roles Overlaid



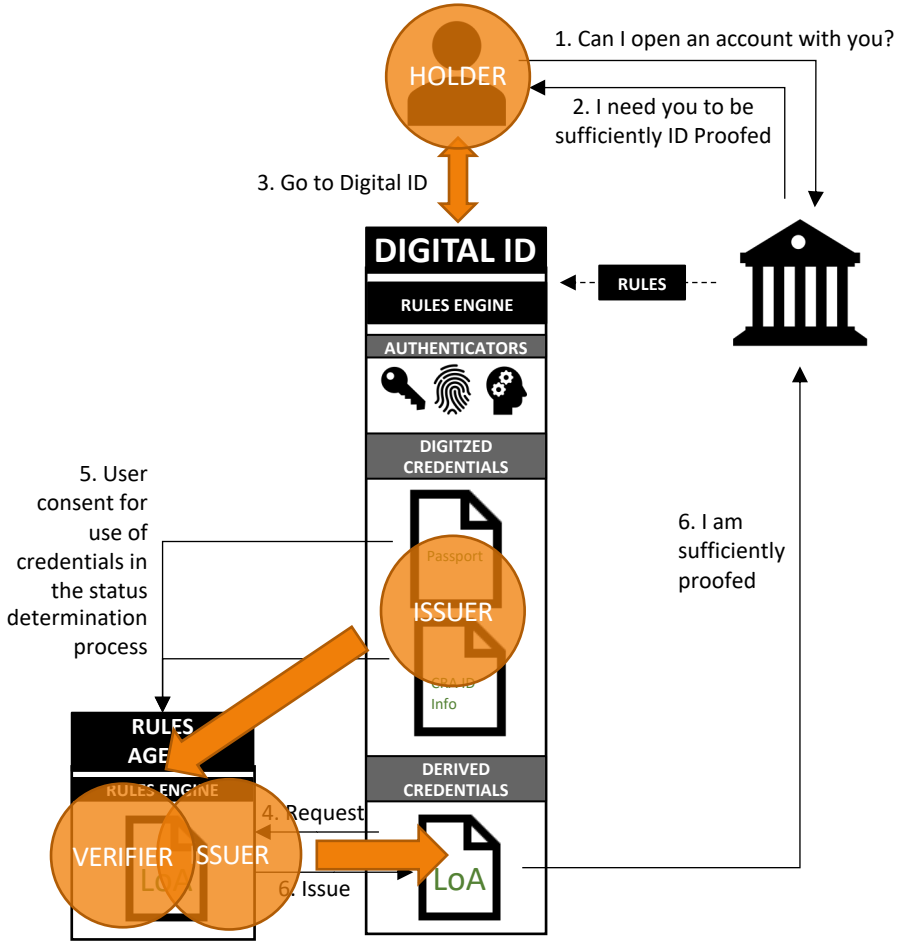
Adding other roles to the overall picture – SSI Style



Adding other roles to the overall picture – SSI Style



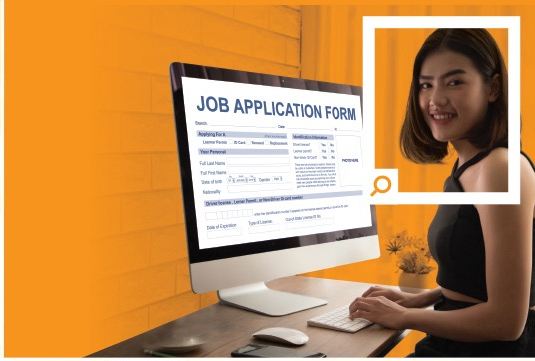
Adding other roles to the overall picture – SSI Style



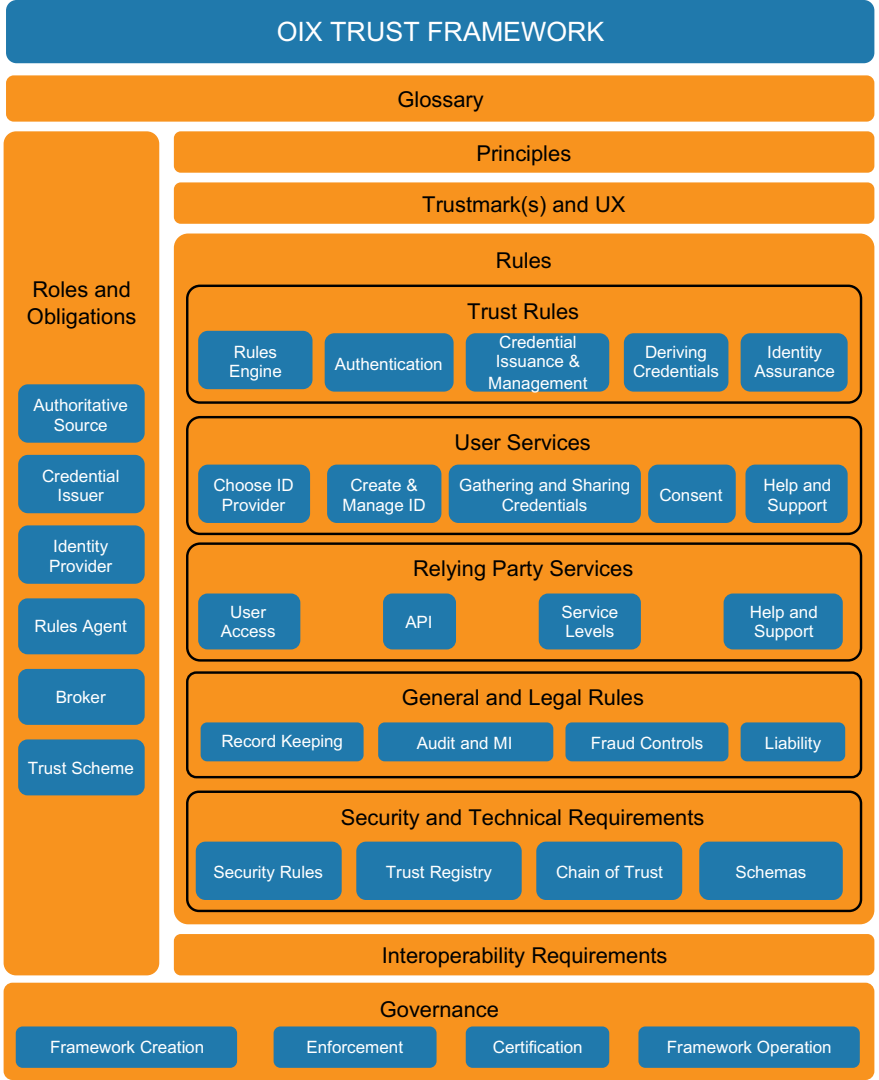
OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Trust Framework
Contents / Layers



Trust Framework Contents



Wrap Up

- Final Version to be signed off in November
- Launch December / January
- New version of online guide that is easier to use will also be released
- Drill down guides already in place:
  - Principles
  - Trustmark's
  - ID Proofing and Authentication
  - Fraud Controls
  - User and Organizational Support Services
  - Liability Options

- Data Standards approach being worked upon