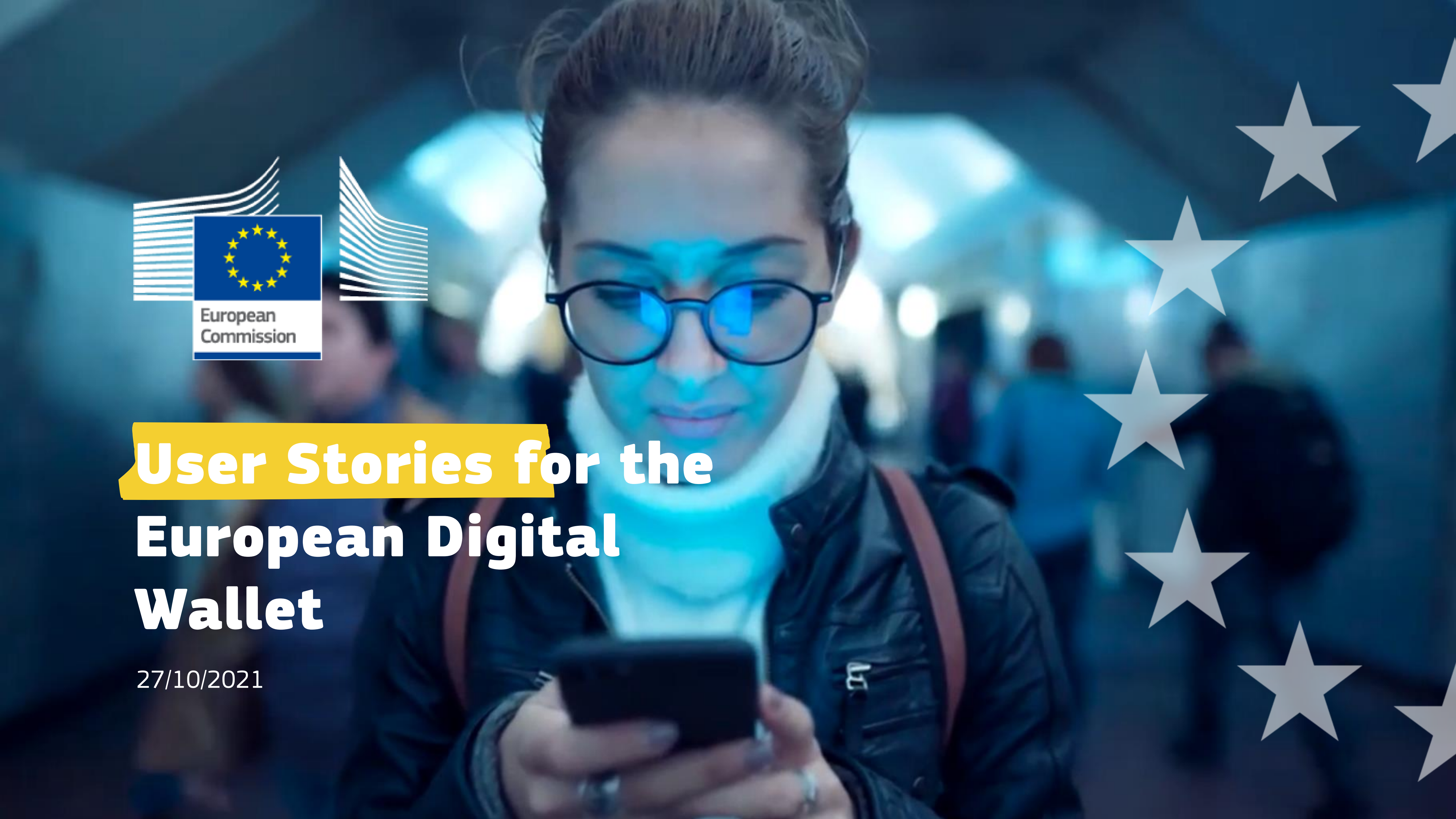
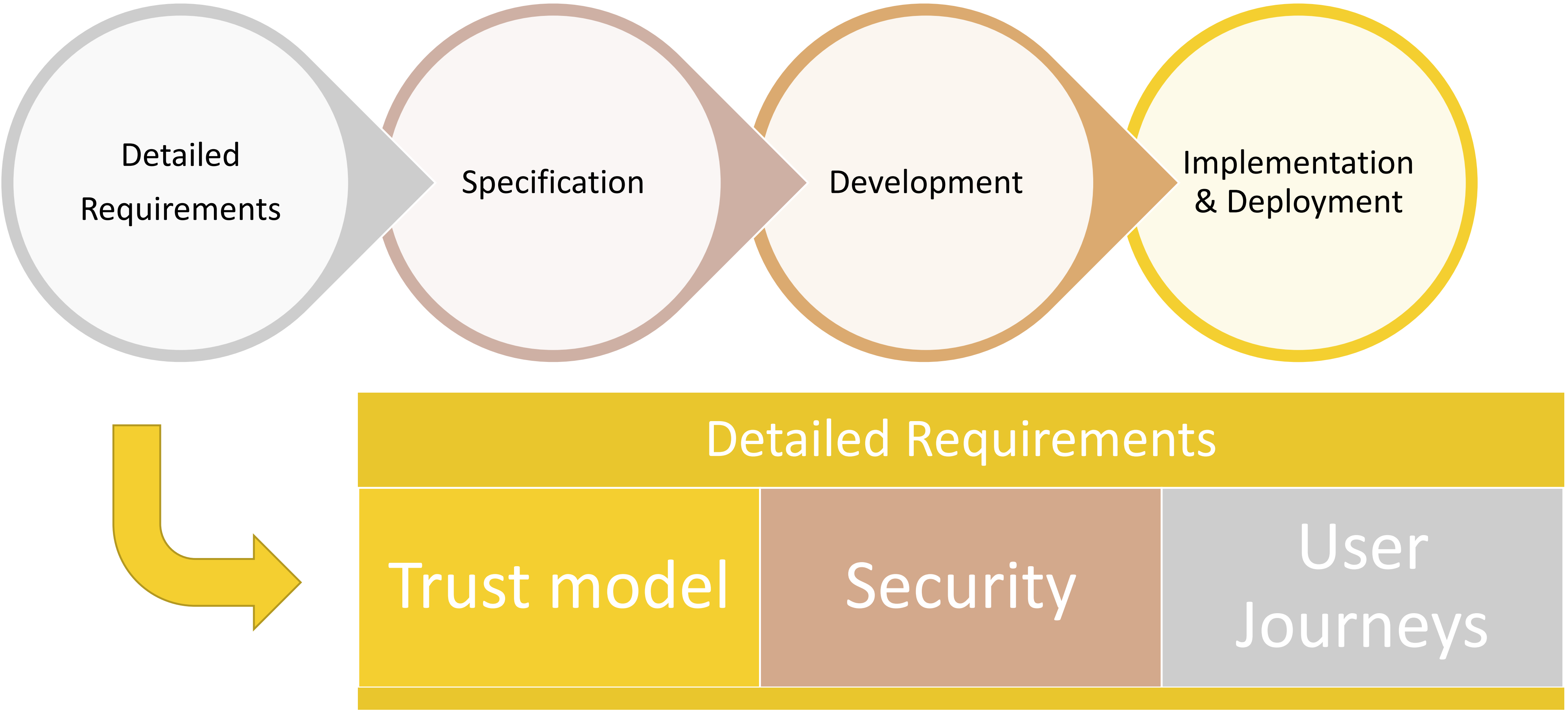


European Commission

User Stories for the European Digital Wallet

27/10/2021

Next Steps towards implementation



Detailed Requirements

Specification

Development

Implementation & Deployment

Detailed Requirements

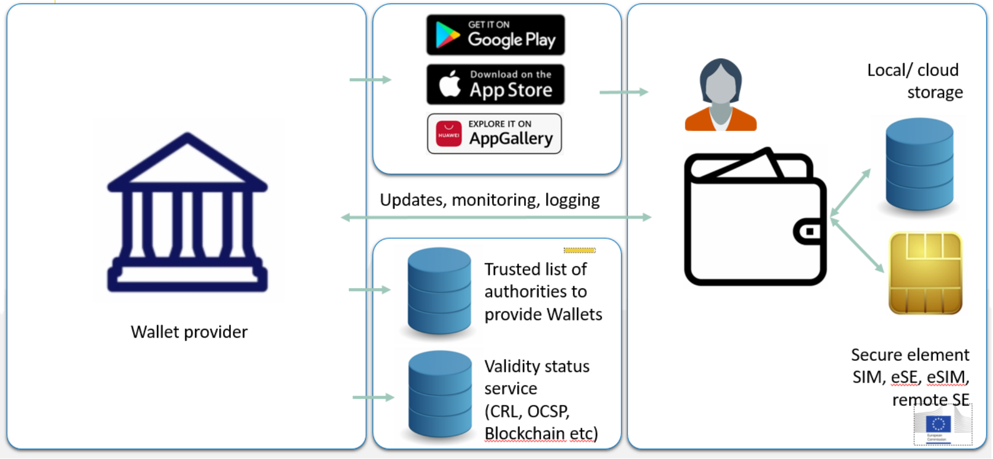
Trust model

Security

User Journeys

User Stories

User story 1: issuing Wallets



Wallet provider

GET IT ON Google Play

Download on the App Store

EXPLORE IT ON AppGallery

Updates, monitoring, logging

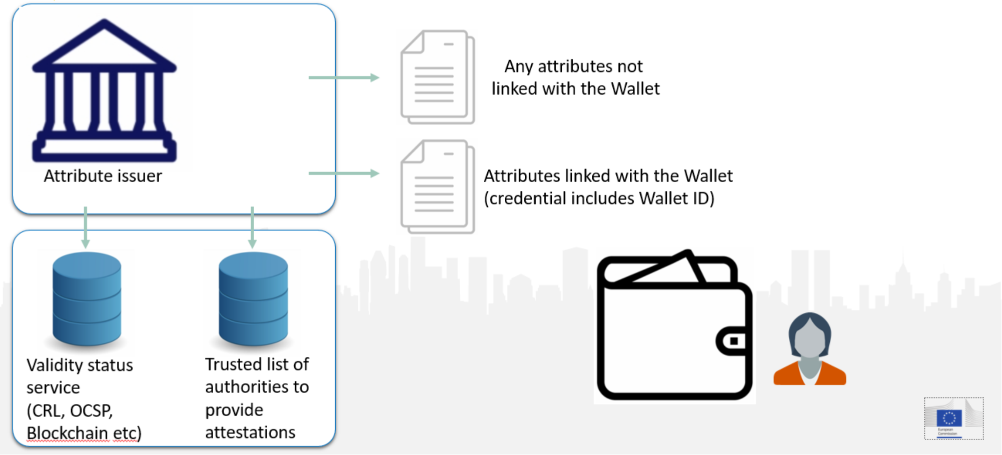
Trusted list of authorities to provide Wallets

Validity status service (CRL, OCSP, Blockchain etc)

Local/ cloud storage

Secure element SIM, eSE, eSIM, remote SE

User story 2: issuing attributes



Attribute issuer

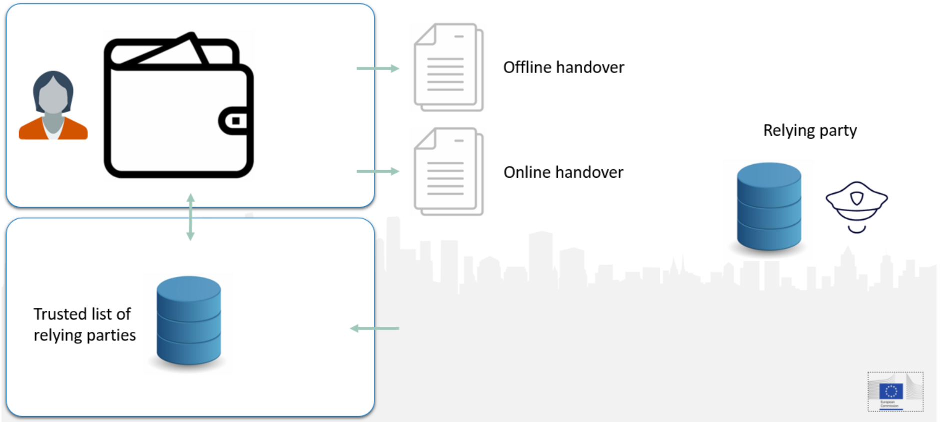
Any attributes not linked with the Wallet

Attributes linked with the Wallet (credential includes Wallet ID)

Validity status service (CRL, OCSP, Blockchain etc)

Trusted list of authorities to provide attestations

User story 3: providing/ presenting credentials



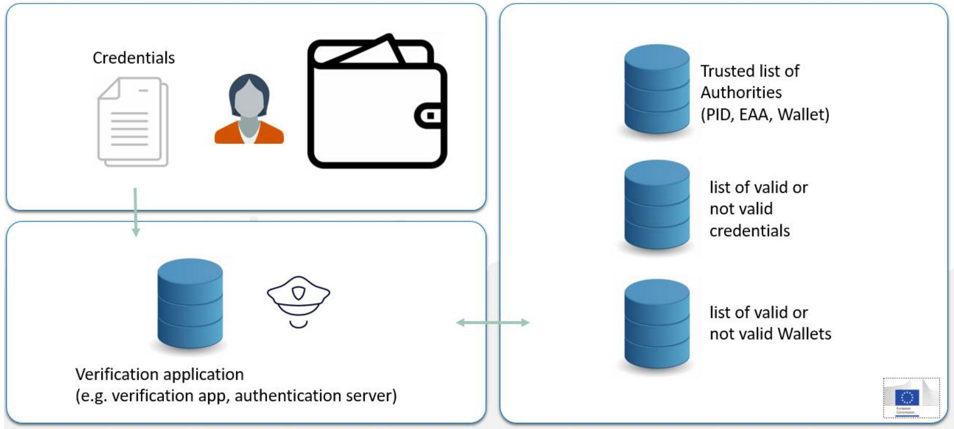
Offline handover

Online handover

Relying party

Trusted list of relying parties

User story 4: authentication of credentials



Credentials

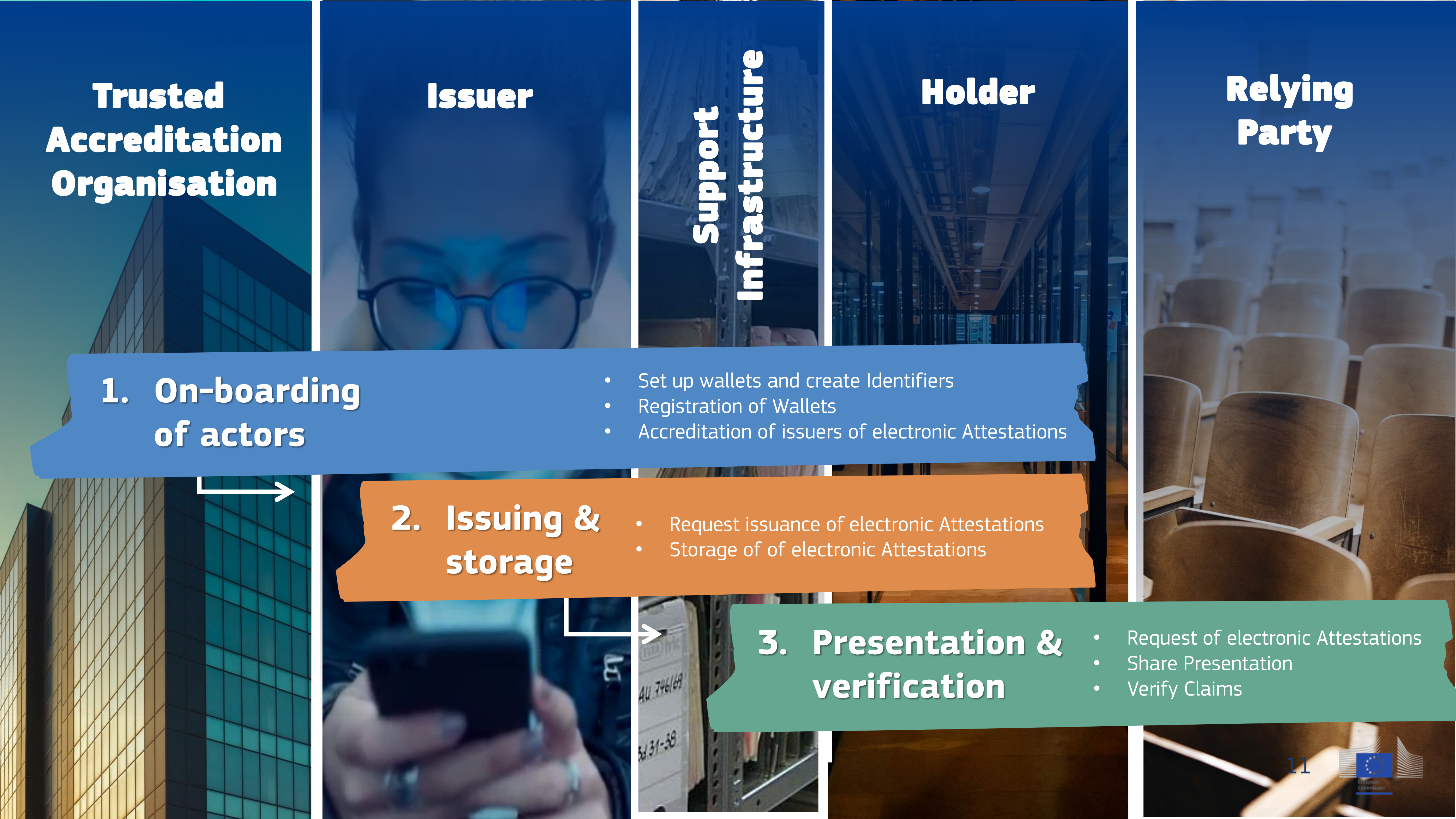
Verification application (e.g. verification app, authentication server)

Trusted list of Authorities (PID, EAA, Wallet)

list of valid or not valid credentials

list of valid or not valid Wallets

Detailing the Lifecycle into User journeys



Trusted Accreditation Organisation

Issuer

Support Infrastructure

Holder

Relying Party

1. On-boarding of actors

- Set up wallets and create Identifiers
- Registration of Wallets
- Accreditation of issuers of electronic Attestations

2. Issuing & storage

- Request issuance of electronic Attestations
- Storage of of electronic Attestations

3. Presentation & verification

- Request of electronic Attestations
- Share Presentation
- Verify Claims

Understanding the roles

Distribution of roles per Member State

MS A

Domain List(s) of trusted Issuers

Gov. Entity

Registers issuers of educational credentials in the Trusted Register of Universities

Issuer

University A

Issues educational credential upon the request of the student

Mobile

Holder

Student

Configures the wallet, requests the issuance of educational credentials and share it with university / employer

MS B

Relying Party

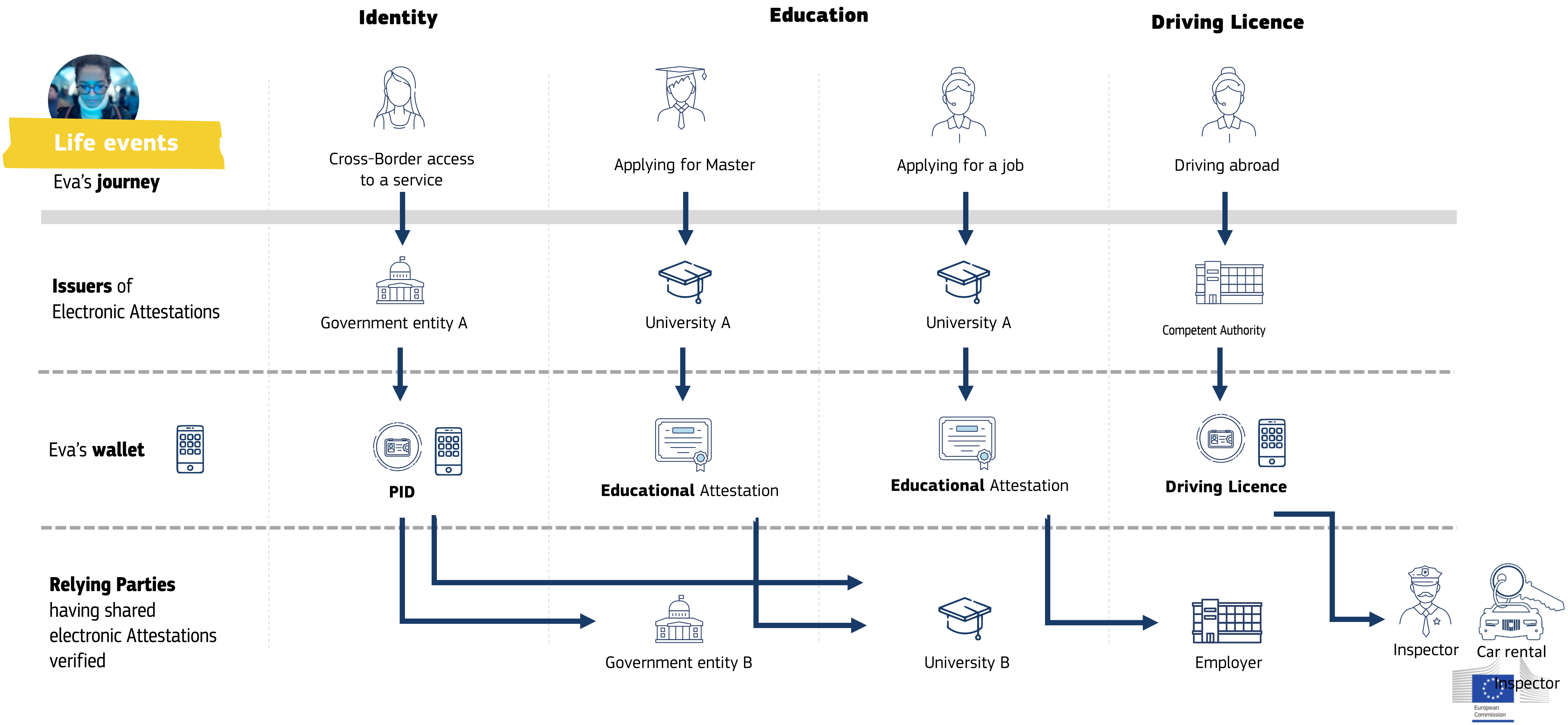
University B

Company

Verifies the educational shared by the student

Electronic Attestation of Attributes applied to use cases

A look at the exchange of electronic Attestations into concrete cases provides further insights



Identity

Education

Driving Licence

Life events

Eva's **journey**

Cross-Border access to a service

Applying for Master

Applying for a job

Driving abroad

Issuers of Electronic Attestations

Government entity A

University A

University A

Competent Authority

Eva's **wallet**

PID

Educational Attestation

Educational Attestation

Driving Licence

Relying Parties having shared electronic Attestations verified

Government entity B

University B

Employer

Inspector

Car rental

Inspector

Use cases as journeys

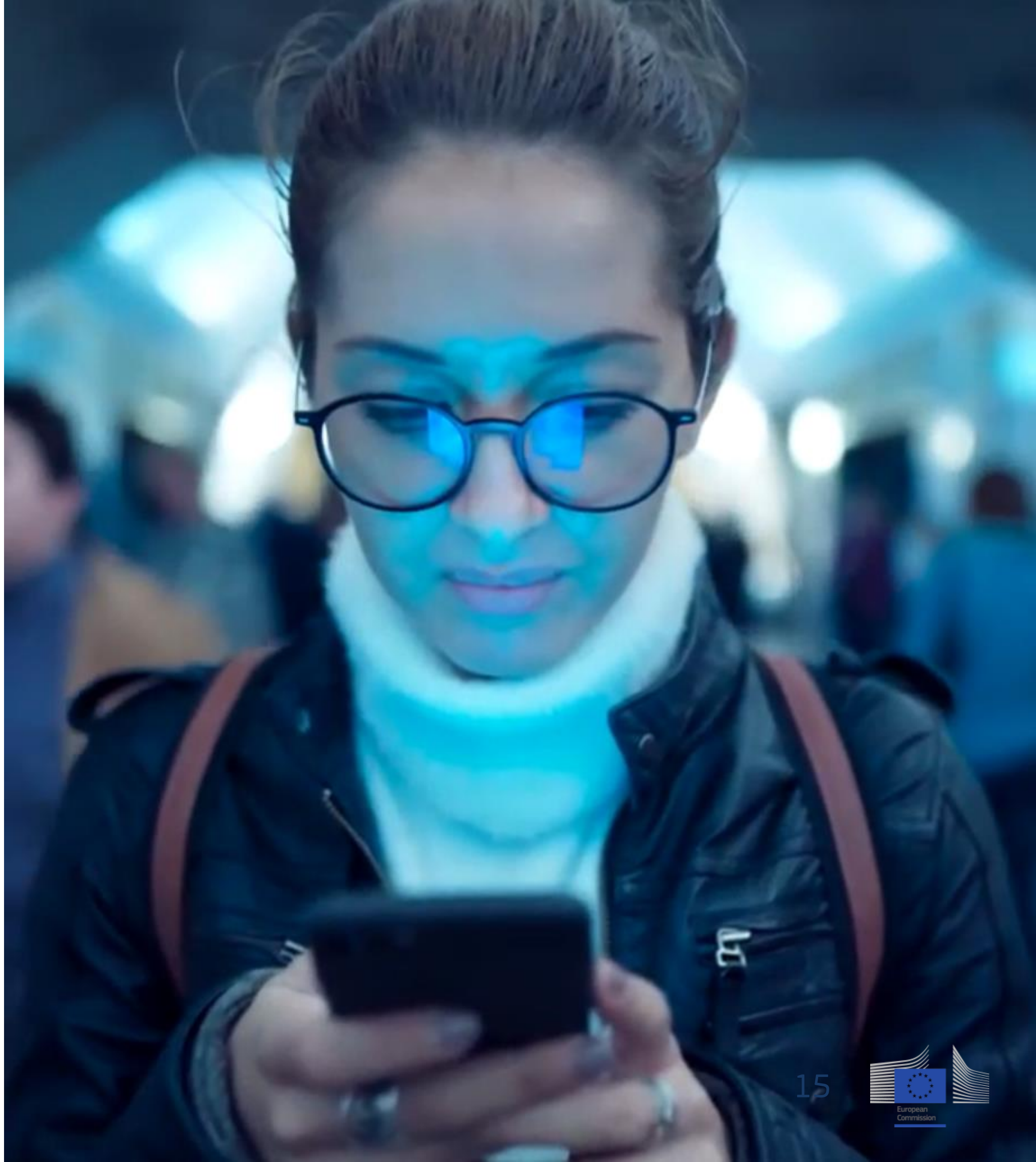
Studying abroad Use Case

What do we want to achieve?

The Diploma Use Case concerns the cross-border verification of educational credentials.

This means that a verifiable attestation (such as a diploma) issued by Member State A can be verified by a university or third party, e.g. an "employer", from Member State B.

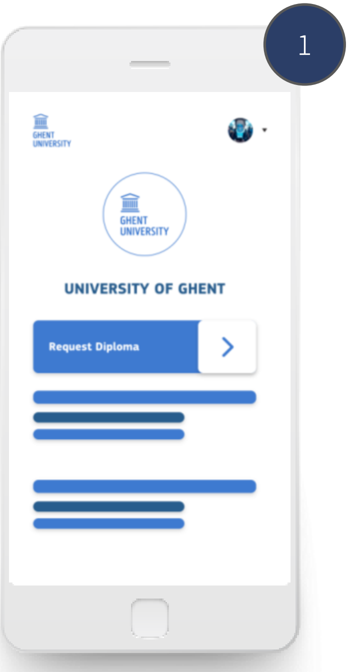
.



Identifying the user journey

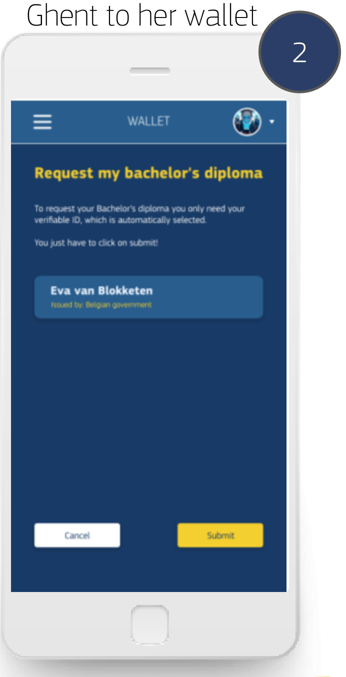
Example (1): Eva requests the issuance of her Bachelor's diploma to the University of Ghent (BE)

Eva initiates the request for the issuance of her Bachelor's Diploma



- Connect to University platform
- Initiate the action

Eva directs the issuance of her Bachelor's Diploma from the University of Ghent to her wallet



Request my bachelor's diploma

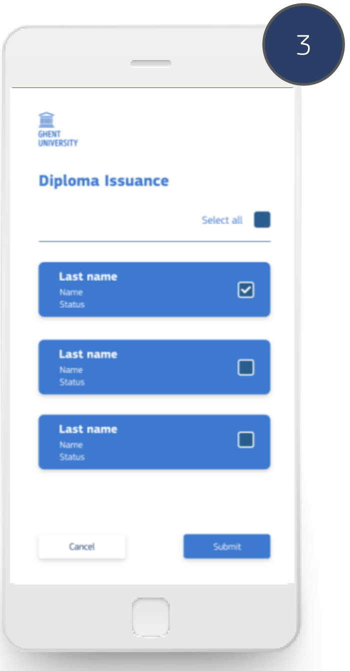
To request your Bachelor's diploma you only need your verifiable ID, which is automatically selected.

You just have to click on submit!

Eva van Blokketen
Issued by: Belgian government

- Select Verifiable ID
- Submit the request

The University of Ghent issues the Bachelor's Diploma



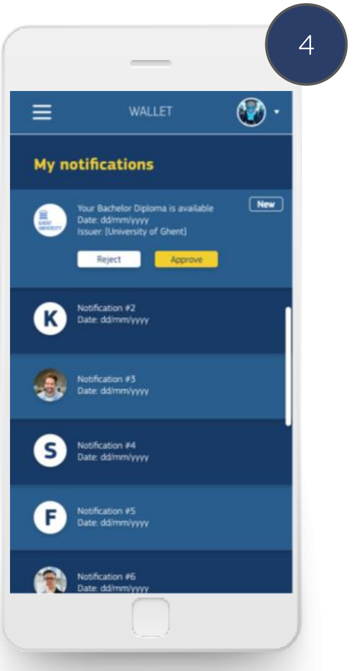
☑ Last name
Name
Status

□ Last name
Name
Status

□ Last name
Name
Status

- Check list of students
- Select the students
- Submit the credential

Eva receives and accepts the Bachelor's Diploma.



Your Bachelor Diploma is available
Date: dd/mm/yyyy
Issuer: [University of Ghent]

Notification #2
Date: dd/mm/yyyy

Notification #3
Date: dd/mm/yyyy

Notification #4
Date: dd/mm/yyyy

Notification #5
Date: dd/mm/yyyy

Notification #6
Date: dd/mm/yyyy

- Get notification
- Accept the credential
- Store in the wallet.

An Inventory of User Stories

Structuring the user journey in distinct steps

(Based on ESSIF work)

Discrete user Stories

A Natural Person requests an electronic Attestation of an attribute from Legal Entity

- A Natural Person seeks access towards a Trusted Issuer and ensure he is interacting with the right (and not rogue) issuer.
- A Natural Person requests a (set of) electronic Attestations
- The Natural Person proof possession over a an identity (e.g. through authentication means (aligned with existing regulations).
- Natural Person verifies that the Issuer is listed in the Trusted Issuers Registry for the type of Verifiable Attestation the Natural Person is requesting.
- A Natural person opts to use an existing identifier to which the electronic attestation is to be issued.
- A Natural Person proves control over the existing identifier.

A Natural Person presents its electronic Attestation to a Legal Entity as Relying Party

- The Legal Entity requests from the Natural Person an electronic attestation of a certain type for a given purpose.
- The Natural Person receives the request for the electronic Attestation and transfers it to its User Wallet.
- If the Natural Person accepts, he/she can choose which information (contained in one or more electronic Attestations) will be shared (via the user wallet) with the Legal Entity.
- The Legal Entity receives and verifies electronic attestation shared by the Natural Person.
- A proof that the Verifiable Presentation has been Received by the Legal Entity is logged.

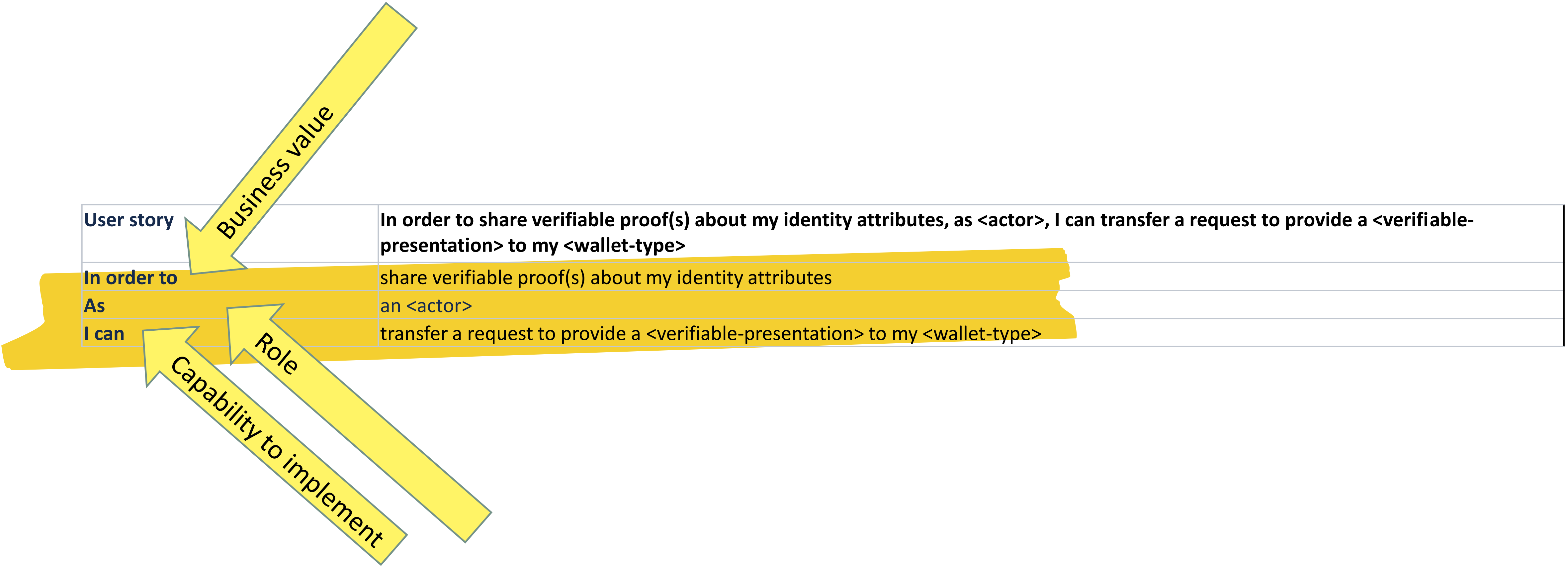
Example Liaison Texts and User Stories as prepared for EBSI

Liaison Text	A Natural Person seeks access towards a Trusted Issuer and ensure he is interacting with the right (and not rogue) issuer.
User Story	In order to request an attestation from a Legal Entity, as a Natural Person, I can visit the official website of the Legal Entity and make sure I'm visiting the right website. (Does not require an EBSI service.)
Liaison Text	A Natural Person requests a (set of) Verifiable Attestations
User Story	In order to get a Verifiable Attestation from a Legal Entity that proves my identity-related attributes, as a Natural Person, I can request a Verifiable Credential within a mutual authenticated session (ESSIF-BC-11)
Liaison Text	The Natural Person performs mutual authentication with a Trusted Issuer to proof possession over a DID and possibly identification using Verifiable ID, or other authentication means (aligned with existing regulations).
Business Scenario	A Natural Person performs mutual authentication using Verifiable ID with a Legal Entity
Liaison Text	(Optional) Natural Person verifies that the Issuer is listed in the Trusted Issuers Registry and is authoritative to issue the Verifiable Attestation the Natural Person is requesting.
User Story	In order to check whether the Issuer is authoritative for a given Verifiable Credential type, as a Natural Person, I can consult the TIR (ESSIF-BC-20)
Liaison Text	A Natural person opts to use an existing DID to which the Verifiable ID is to be issued.
User Story	In order to be able to receive a Verifiable ID, as a Natural person, I can decide whether to issue this Verifiable ID to an existing one or to one that is to be newly registered.
Liaison Text	A Natural Person proves control over its DID. (Remark: DID (keys) must be of sufficient strength. The authentication is mutual. This proof of control must be linked to the authentication of the previous User Story ensuring that they are performed by the same entity; e.g. DID control proof during a session established with classical authentication.
User Story	In order to prove ownership of a DID, as an user, I can prove control over this DID (via associated public/private keys) (ESSIF-BC-06)
Liaison Text	(Optional: if the Legal Entity requires additional information to issue the requested Verifiable Attestation, it can request that information from the Natural Person. In such a case, the Legal Entity initiatives the User Journey "Natural Person presents its Verifiable Attestation to a Legal Entity". For the sake of completeness, the relevant steps are also included below within this User Journey)
User Story	In order to get proof from a Natural Person, as a Legal Entity, I can request Verifiable Presentation (ESSIF-BC-07)

Liaison text	(Optional. Only if Verifiable Presentation Request (that contains relevant information from Verifiable Attestation(s) [VC-Type]) has been triggered.) The Natural Person receives a request to its User Wallet.
User Story	In order to authenticate using SSI Wallet, as <subject>, I can receive an Authentication Request to my SSI Wallet (ESSIF-BC-08)
Liaison text	(Optional. Only if Verifiable Presentation Request has been triggered.) The Natural Person accepts/confirms the request and presents the Verifiable Presentation to the Legal Entity.
User Story	In order to share <credential> upon a request, as a Natural Person, I can issue Verifiable Presentation (ESSIF-BC-09)
Liaison text	(Optional. Only if Verifiable Presentation Request has been triggered.) The Legal Entity receives and verifies the Verifiable Presentation.
User Story	In order to verify <credential>, as a Legal Entity, I can verify Verifiable Presentation (ESSIF-BC-10)
Liaison Text	If a Natural Person's request is accepted, the Legal Entity issues Verifiable Attestation(s).
User Story	In order to issue a digital proof of credentials to a Natural Person, as an Issuer, I can issue a Verifiable Attestation (ESSIF-BC-12)
Liaison text	The Legal Entity notifies the Natural Person about the Verifiable Attestation(s) issuance.
User Story	In order to inform a Natural Person about its Verifiable Credential issuance or revocation, as a Legal Entity, I can notify the Natural Person (ESSIF-BC-13)
Liaison Text	The Natural Person receives a notification and collects/stores Verifiable Attestation(s).
User Story	In order to receive a digital proof of my credentials from a Legal Entity, as a Natural Person, I collect my Verifiable Credential (ESSIF-BC-15)
Liaison Text	(Optional) The Legal Entity anchors an issuance proof of the issuance of the Verifiable Attestation(s) on EBSI Ledger.)
User Story (Optional)	In order to create verifiable evidence on EBSI Ledger that I issued/revoked a Verifiable Attestation, as an <Actor> y, I can notarize Verifiable Attestation issuance/revocation (ESSIF-BC-14)
Liaison Text	(Optional). The Natural Person and/or the Legal Entity anchors a reception proof of the Verifiable Attestation on EBSI Ledger.
User Story (Optional)	In order to create verifiable evidence on EBSI Ledger that I received/revoked a Verifiable Attestation, as a Natural Person , I can notarize Verifiable Attestation reception/revocation (ESSIF-BC-14)

User story - Form

Connextra template – modified by Chris Matts



User story	**In order to share verifiable proof(s) about my identity attributes, as <actor>, I can transfer a request to provide a <verifiable-presentation> to my <wallet-type>**
In order to	share verifiable proof(s) about my identity attributes
As	an <actor>
I can	transfer a request to provide a <verifiable-presentation> to my <wallet-type>

<table>
<tr><td><b>User story</b></td><td colspan="4"><b>In order to share verifiable proof(s) about my identity attributes, as <actor>, I can transfer a request to provide a <verifiable-presentation> to my <wallet-type&gt;</b></td></tr>
<tr><td><b>In order to</b></td><td colspan="4">share verifiable proof(s) about my identity attributes</td></tr>
<tr><td><b>As</b></td><td colspan="4">an &lt;actor&gt;</td></tr>
<tr><td><b>I can</b></td><td colspan="4">transfer a request to provide a <verifiable-presentation> to my <wallet-type&gt;</td></tr>
<tr><td><b>Functional scenario</b></td><td colspan="4">Feature: Receive request to share a <verifiable-presentation> request (on <wallet-type>)
Background:
Given "<relying-party>" requested a "<verifiable-presentation>" from an "<actor>"

Scenario: QR Code
Given "<actor>" is presented a QR Code (that “contains” (a link to) a "<presentation-request>")
When "<actor>" opens/accesses the "<wallet-type>"
And "<actor>" scans the QR Code with "<wallet-type>"
And "<actor>" verifies signatures on the "<presentation-request>"
Then "<actor>" is asked to share a "<verifiable-presentation>" (to prove certain identity attributes) with "<relying-party>”
And "<actor>" can accept or decline the request
Scenario: (Deep) Link
Given "<actor>" is presented a deep link (that “contains” (a link to) a "<presentation-request>")
When "<actor>" clicks on the (deep) link
And "<actor>" is redirected to her "<wallet-type>"
Then "<actor>" is asked to share a "<verifiable-presentation>" (to prove certain identity attributes) with "<relying-party>”
And "<actor>" can accept or decline the "<presentation-request>"

Examples:</td></tr>
<tr><td></td><td>Actor</td><td>Relying Party</td><td>Wallet-type</td><td>Attestation</td></tr>
<tr><td></td><td>Natural Person (main use case)</td><td>e.g. a Legal Entity that intends to issue a Verifiable Attestation but requires more information</td><td>User Wallet (web, mobile client)</td><td>Proof of higher education certificates (Verifiable Attestations)</td></tr>
<tr><td></td><td>Legal Entity</td><td>e.g. a Legal Entity that is asked to provide a service but requires more information</td><td>Enterprise Wallet (web, mobile client)</td><td>Proof of legal incorporation (Verifiable Attestation)</td></tr>
<tr><td><b>Outcomes</b></td><td colspan="4">&lt;actor> accepts or rejects a Verifiable Presentation request.</td></tr>
<tr><td><b>Important remarks</b></td><td colspan="4">QR codes are very small, probably for most Presentation Request a single use link (tiny-url) to the Presentation Request must be included in the QR instead of the full Presentation Request</td></tr>
</table>

Thank you !