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**
  - Updates, monitoring, logging
  - Trusted list of authorities to provide Wallets
  - Validity status service (CRL, OCSP, Blockchain etc.)
- **Local/cloud storage**
- **Secure element** SIM, eSE, cSIM, remote SE

### User story 2: issuing attributes
- **Attribute issuer**
- **Validity status service** (CRL, OCSP, Blockchain etc.)
- **Trusted list of authorities to provide attestations**
- Any attributes not linked with the Wallet
- Attributes linked with the iWallet (credential includes Wallet ID)

### User story 3: providing/presenting credentials
- **Offline handover**
- **Relying party**
- Trusted list of relying parties
- **Online handover**

### 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
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 electronic Attestations

3. Presentation & verification
   - Request of electronic Attestations
   - Share presentation
   - Verify claims
Understanding the roles
Distribution of roles per Member State

**Domain List(s) of trusted Issuers**
- **Gov. Entity** (MS A)
- **University A** (MS B)

**Issuer**
- Issues educational credential upon the request of the student

**Holder**
- Student

**Relying Party**
- University B
- Company

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

- 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.

Life events

Eva's journey

Identity

Cross-Border access to a service

Government entity A

PID

University A

Educational Attestation

University B

Government entity B

Education

Applying for Master

University A

Educational Attestation

University B

Educational Attestation

Driving Licence

Applying for a job

University A

Driving abroad

Competent Authority

Relying Parties

having shared electronic Attestations verified

Inspector

Employer

Car rental

Eva's wallet

PID

University A

Educational Attestation

University B

Driving Licence

Eva's wallet

University B

Driving Licence
Use cases as journeys
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)

1. Eva initiates the request for the issuance of her Bachelor’s Diploma
   - Connect to University platform
   - Initiate the action

2. Eva directs the issuance of her Bachelor’s Diploma from the University of Ghent to her wallet
   - Select Verifiable ID
   - Submit the request

3. The University of Ghent issues the Bachelor’s Diploma
   - Check list of students
   - Select the students
   - Submit the credential

4. Eva receives and accepts the Bachelor’s Diploma
   - Get notification
   - Accept the credential
   - Store in the wallet.

Eva initiates the request for the issuance of her Bachelor’s Diploma
Eva directs the issuance of her Bachelor’s Diploma from the University of Ghent to her wallet
Eva requests the issuance of her Bachelor’s diploma to the University of Ghent (BE)
Eva receives and accepts the Bachelor’s Diploma.
An Inventory of User Stories
**Structuring the user journey in distinct steps**
(Based on ESSIF work)

**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 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A Natural Person seeks access towards a Trusted Issuer and ensure he is interacting with the right (and not rogue) issuer.</td>
<td>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.)</td>
<td>A 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.</td>
<td>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)</td>
<td>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.</td>
<td>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)</td>
<td>(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 initiates 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)</td>
<td>In order to get proof from a Natural Person, as a Legal Entity, I can request Verifiable Presentation (ESSIF-BC-07)</td>
<td>(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.</td>
<td>In order to authenticate using SSI Wallet, as &lt;subject&gt;, I can receive an Authentication Request to my SSI Wallet [ESSIF-BC-08]</td>
<td>(Optional. Only if Verifiable Presentation Request has been triggered.) The Natural Person accepts/verifies the request and presents the Verifiable Presentation to the Legal Entity.</td>
<td>In order to share &lt;credential&gt; upon a request, as a Natural Person, I can issue Verifiable Presentation (ESSIF-BC-09)</td>
<td>(Optional. Only if Verifiable Presentation Request has been triggered.) The Legal Entity receives and verifies the Verifiable Presentation.</td>
<td>In order to verify &lt;credential&gt;, as a Legal Entity, I can verify Verifiable Presentation (ESSIF-BC-10)</td>
<td>If a Natural Person’s request is accepted, the Legal Entity issues Verifiable Attestation(s).</td>
<td>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)</td>
<td>The Legal Entity notifies the Natural Person about the Verifiable Attestation(s) issuance.</td>
<td>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)</td>
<td>The Natural Person receives a notification and collects/stores Verifiable Attestation(s).</td>
<td>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-06)</td>
<td>(Optional) The Legal Entity anchors an issuance proof of the issuance of the Verifiable Attestation(s) on EBSI Ledger.</td>
<td>In order to create verifiable evidence on EBSI Ledger that I issued/revoked a Verifiable Attestation, as an &lt;Actor&gt; y, I can notarize Verifiable Attestation issuance/revocation (ESSIF-BC-14)</td>
<td>(Optional). The Natural Person and/or the Legal Entity anchors a reception proof of the Verifiable Attestation on EBSI Ledger.</td>
<td>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)</td>
</tr>
</tbody>
</table>
User Story - Form
Connextra template – modified by Chris Matts

<table>
<thead>
<tr>
<th>Business Value</th>
<th>Capability to Implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to share verifiable proof(s) about my identity attributes, as &lt;actor&gt;, I can transfer a request to provide a &lt;verifiable-presentation&gt; to my &lt;wallet-type&gt;</td>
<td></td>
</tr>
</tbody>
</table>

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>
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>

Functional scenario
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-presentations>" (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:

<table>
<thead>
<tr>
<th>Actor</th>
<th>Relying Party</th>
<th>Wallet-type</th>
<th>Attestation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Person (main use case)</td>
<td>e.g. a Legal Entity that intends to issue a</td>
<td>User Wallet (web, mobile client)</td>
<td>Proof of higher education certificates (Verifiable Attestations)</td>
</tr>
<tr>
<td></td>
<td>Verifiable Attestation but requires more information</td>
<td></td>
<td></td>
</tr>
<tr>
<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>
</tbody>
</table>

Outcomes
<actor> accepts or rejects a Verifiable Presentation request.

Important remarks
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
Thank you !