Infrastructure supporting the access to the LEAR Credential

This section describes the components and infrastructure required by an organisation to create the LEAR Credential for one of its employees.

- LEAR Credential Issuer
- LEAR Credential Signer

LEAR Credential Issuer

Description

The `LEAR Credential Issuer` is the main application that manages the credential flow. We assume here that it is specialised in creating LEAR Credentials, though it could be used for other types of credentials. In this context, we will use the term `LEAR Credential Issuer` and `Credential Issuer` as interchangeable.

For the explanation, we are going to assume the issuance flow described above and a given set of actors. However, the flows can be adapted to other scenarios.

The main actors are:

Appointed employee
: This is the employee that will receive the LEAR Credential and that has been nominated or appointed by the organisation to perform some role in DOME on behalf of the organisation.

HR employee
: The employee from the Human Resources department of the organisation that introduces the Appointed employee data in the Credential Issuer application.

Legal Representative
: The natural person that is the official legal representative of the organisation.

Obtaining an eIDAS certificate

Before starting the process, the legal representative should have an eIDAS certificate. This is the same certificate that can be used to sign documents in PDF form. The legal representative will be signing the LEAR Credential in a similar way to signing a PDF in her machine, except she will use a special program provided by DOME instead of Acrobat Reader. The technical requirements for signing LEAR Credentials are essentially the same as for signing a PDF. More details about this later.

Introduction of data about the Appointed Employee

The HR employee uses an HTML form provided by the LEAR Credential Issuer application to input the required data about the employee. The application enables also to provide such data with a YAML file, to facilitate automation of the process.

The required data includes name, surname, contact data (phone and company email), and the roles that the employee is authorised to perform. For simplicity we assume here the role `onboarder`, but the HR employee can specify a list of roles relevant for DOME.

Once the data is completed, the HR employee confirms the operation and the LEAR Credential Issuer notifies the Appointed Employee using the company email provided.

The Appointed employee receives the Credential Offer

The employee receives an email from the LEAR Credential Issuer with the proper instructions, including a unique `transaction code` that the employee requires to start the process for receiving the LEAR Credential.

The Appointed employee enters into the HTML portal provided by the LEAR Credential Issuer (the URL of the portal is well-known, but it is also described in the email).

The portal does not require the Appointed employee to be pre-registered in the application, because the unique `transaction code` received via email is used to access its Credential Offer.

Once the employee enters the `transaction code` in the portal, a QR code is displayed with the content of Credential Offer (compliant with the OpenID4VCI protocol).

The employee scans the QR code with her Wallet. She can use the Wallet provided by DOME, or any other which is compatible. This includes the possibility that the company provides employees with its own Wallet, which could even be a branded version of the DOME Wallet.

The Wallet of the Appointed employee

The Appointed employee should have a Wallet compatible with the OpenID4VCI specifications, in particular capable of the subset of functionalities specified in the DOME profile.

The employee uses the Wallet to scan the QR code presented by the LEAR Credential Issuer containing the Credential Offer. After the employee reviews the request in her Wallet and providing explicit confirmation, the Wallet generates a private/public key pair according to the `did:key` specification, and sends this generated `did:key` to the LEAR Credential Issuer following the OpenID4VCI specifications.

The LEAR Credential Issuer replies to the Wallet with an OpenID4VCI Access Token to be used later when the credential has been signed by the legal representative.

The LEAR Credential Issuer notifies via email to the legal representative (her email is pre-registered in the application, as the contact person in the organisation capable of signing the LEAR Credentials).

LEAR Credential Signer

Description

This is a simple program provided by DOME that should be installed locally in the PC of the legal representative and that performs the actual signing of the LEAR Credential (there are versions for Windows, Mac and Linux). Alternatively, any organisation can develop an equivalent program themselves if they wish, because it performs standard JAdES signatures and uses documented APIs of the LEAR Credential Issuer program.

The LEAR Credential Signer supports the following mechanisms to access the eIDAS certificate and sign the credential:

1. **PKCS#12** which defines a file format commonly used to store X.509 private key accompanying public key certificates, protected by symmetrical password.
2. **MS CAPI** which is the Microsoft interface to communicate with SmartCards and Windows keyring.
3. **Apple Keystore** allowing to access a Keychain store in a MacOS environment.
4. **PKCS#11** is widely used to access smart cards and HSMs in different operating systems and environments.

The functionalities of the LEAR Credential Signer are described below.

The legal representative starts the program

When the legal representative receives the email notification that a LEAR Credential needs her signature, she starts the LEAR Credential Signer program previously installed in her machine.

The program asks the legal representative for a unique transaction code received in the email. This transaction code is different from the one received by the Appointed employee, but it is related to the same transaction (the specific LEAR Credential being created).

The program invokes an API provided by the LEAR Credential Issuer to retrieve the LEAR CRedential that has to be signed. The API accepts the unique transaction code received from the legal representative.

The program displays the information for the retrieved LEAR Credential and requests confirmation to continue.

The legal representative signs the Credential

After confirmation, the LEAR Credential Signer uses the standard APIs (PKCS#12, MS CAPI, etc.) to perform the signature. During this process, the program requests from the legal representative the password or other authentication mechanism that the actual protocol requires to confirm the signature. For example, with PKCS#12 the legal representative has to provide the symmetrical password that protects the file containing the X.509 certificate.

Sending the signed credential to the LEAR Credential Signer

After the signature is performed, the program asks for another confirmation from the legal representative to continue with the process.

Then the LEAR Credential Signer program invokes another API provided by the LEAR Credential Issuer server to send the signed credential.

LEAR Issuer receives the credentials

When the Issuer receives the signed Credential from the LEAR Credential Signer, it makes the Credential available for retrieval by the Appointed employee. It also notifies via email to the involved parties (Appointed employee, legal representative and HR employee).

When the Appointed employee receives the notification, she uses her Wallet to restart the issuance process.

The Wallet uses the Access Token received in the first phase of the process to request the Credential using the OpenID4VCI protocol. After the protocol is executed, the Wallet has the LEAR Credential signed by the legal representative, ready to be used for authentication into DOME.