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.

Revision #2
Created 10 November 2025 15:11:58 by Roger Miret
Updated 10 November 2025 15:18:41 by Roger Miret