Signing the LEAR Credential

We start describing at a high level a typical local signature process when the legal representative signs a PDF document, because it is very familiar and will serve as the base to describe the signature of a Verifiable Credential to generate the LEAR Credential, highlighting the similarities and differences.

An imaginary (but typical) PDF signing process goes like this:

1. Somebody in another department of the company prepares a PDF document with the appropriate content. If it is a document related to an employee, it may be the HR department the one that prepares a Word document including some relevant employee information.
2. The HR department sends to the employee the Word document so the employee can complete the document with some information that the HR department did not have. The employee returns the document to the HR department.
3. The HR department exports the Word document to PDF format and sends the file electronically to the legal representative for signature. It may be sent by email, or in more sophisticated companies the document is managed by a document processing system, and it is made available for signature according to a specified workflow.
4. The legal representative opens the PDF document in Acrobat Reader or any other application capable of signing PDFs.
5. The legal representative instructs Acrobat Reader to digitally sign the document, and the program uses the corresponding operating system APIs to access the keyring or filesystem where the certificate is stored securely. Normally, this requires the legal representative to authenticate with the keyring.
6. Acrobat Reader reads the certificate and its associated private key and performs the signature. Acrobat Reader then asks the legal representative to save the signed file.
7. The legal representative sends the signed PDF back to HR, so they can provide the document to the employee, together with whatever instructions are appropriate.

When creating the LEAR Credential, the flow is very similar:

1. Somebody in another department of the company prepares a JSON document with the format of a Verifiable Credential, with the appropriate content. In the case of a LEAR Credential, it may be the HR department the one that prepares the JSON document, including the relevant employee information. The HR department uses a special program called Credential Issuer to generate this version of the Credential and interact with the employee Wallet. The company can implement its own Issuer if they want, or they can simply use the Issuer provided by DOME As-A-Service.
2. The HR department, using the Credential Issuer, sends the Credential to the employee Wallet. The employee can use any Wallet complying with the EDIW standards (OpenID4VCI), including the one provided by DOME. The Wallet, following the OpenID4VCI protocol, generates a pair of private/public keys and sends back the Credential and the public key to HR (again, following the OpenID4VCI protocol). The private key remains always in control of the user and nobody else knows about it.
3. The Credential Issuer notifies automatically to the legal person that there is a document to be signed.
4. The legal representative opens a local program installed in her computer (the equivalent to Acrobat Reader), and reviews the Credential to be signed. This local program is called Credential Signer and is provided by DOME for Windows, Mac and Linux, but the company can develop or buy their own. The Credential Signer uses the APIs of the Credential Issuer to retrieve the Credential to be signed (there may be more than one for different employees).
5. The legal representative instructs the Credential Signer to digitally sign the document, and the program uses the corresponding operating system APIs to access the keyring or filesystem where the certificate is stored securely. Normally, this requires the legal representative to authenticate with the keyring.
6. The Credential Signer reads the certificate and its associated private key and performs the signature. The resulting file is now a LEAR Credential.
7. After confirmation by the legal representative, the Credential Signer sends the LEAR Credential back to the Credential Issuer, which notifies HR and the employee that the Credential is ready. The employee

uses her Wallet to retrieve the LEAR Credential from the Credential Issuer, again using the OpenID4VCI protocol.

Revision #1
Created 10 November 2025 23:39:51 by Roger Miret
Updated 10 November 2025 23:40:00 by Roger Miret