FoC Project 2024-25

Digital Signature Server

An organization implements a Digital Signature Service (DSS), a trusted third party that creates public-private key pairs, stores them and generates digital signatures on the behalf of the organization's employees.

Organization’s employees are registered off-line. At registration, an employee receives the DSS’ public key and a password that has to be changed at the first login. An employee maintains the public key of the server.

After securely connecting to the DSS, a user may invoke the following operations request.

- **CreateKeys** which creates and stores a pair of private and public keys on behalf of the invoking user. If a key pair is already existing for the user, the operation has no effect.
- **SignDoc** which returns the digital signature on the document specified as argument. The service digitally signs the document on the invoking user’s behalf and returns him/her the resulting digital signature.
- **GetPublicKey** which returns the public key of the user specified as argument.
- **DeleteKeys** which deletes the key pair of the invoking user. After a key pair has been deleted, an user cannot create a new one unless (s)he is (off-line) registered again.

Users interact with the DSS through a secure channel that must be established before issuing operations. A user authenticates the service by means of the service’s public key. A user authenticates to the service by means of her/his password. The secure channel must fulfill perfect forward secrecy (PFS), integrity, no-replay and non-malleability.

The server stores private keys of users in their encrypted form.

Project report must contain:

- Specifications and design choices with particular reference to the authentication protocol between a user and the service.
- Format of all the exchanged messages.
- Sequence Diagrams of every used communication protocol (Application Level).