Security of Computer Systems

Project Report

Authors:
Name1, Surname1, ID
Name2, Surname2, ID

Version: 1.0

*** * * REMOVE * * ***

During realization of the project please extend the document, do not create separate documents control and submission term.

*** * * REMOVE * * ***

Versions

Version	Date	Description of changes
1.0	17.04.2024	Creation of the project, implementation of base algorithms

1. Project – control term

1.1 Description

Tool for Emulating the Qualified Electronic Signature using Python in Pycharm environment.

1.2 Results

In the project so far, we have accomplished the following:
Implemented RSA key pair generation for user A. Developed a function to derive an AES key from the user's PIN number. Created a GUI interface to allow the user to select a PDF document for signing. Signed the selected PDF document using the RSA private key. Derived an AES key from the user's PIN and encrypted the private key with it. Allowed the user to choose the pendrive directory for saving the encrypted private key.

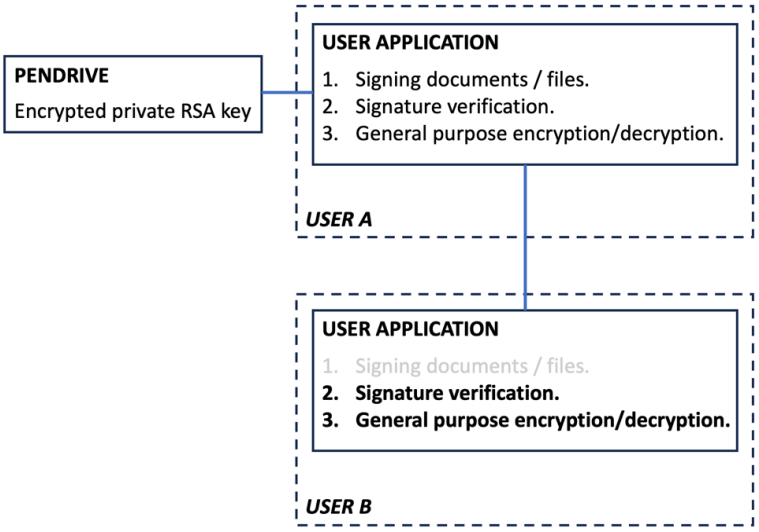

Fig. 1 – Block diagram..

1.3 Summary

Moving forward, we still need to complete the following tasks:

Implementing functionality for verifying the electronic signature. Designing and developing the user interface for signature verification. Testing the application thoroughly to ensure functionality and security. Documenting the project, including technical specifications, usage instructions, and any other relevant information. Potentially optimising and refactoring the codebase for better performance and maintainability. Considering additional security measures, such as password protection for the pendrive or encryption of the entire pendrive contents.