**Security of Computer Systems**

**Project Report**

Authors:

Tomasz, Sankowski, 193363

Piotr, Sulewski, 192594

Version: 1.0

**Versions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of changes |
| 1.0 | 01.04.2025 | Creation of the document |
| 1.1 | … | … |

1. **Project**
   1. ***Description***

The goal of this project is to develop an application that emulates a qualified electronic signature according to a simplified PAdES standard. The application allows users to sign PDF documents using a 4096-bit RSA private key, which is securely stored on a USB drive. When generating a new private key, the user sets a PIN, which is then hashed using SHA-256 along with a randomly generated salt to enhance security. The resulting hash is used to encrypt the private key with the AES-256 algorithm. Additionally, a randomly generated initialization vector (IV) is used during encryption, further strengthening security. Both the salt and the IV are stored next to the encrypted private key to ensure proper decryption.

To sign a document, the user provides the correct PIN, which is hashed again using the stored salt, allowing the application to reconstruct the encryption key. This key is then used along with the stored IV to decrypt the private key. If the provided PIN is incorrect, the resulting key will be invalid, making decryption unsuccessful. The application automatically detects USB drives and checks for the presence of a private key. Once the correct PIN is entered, the user can select any PDF file on their computer and sign it.

The signing process involves computing the hash of the PDF file (excluding metadata) and embedding the hash, along with the user’s name and signing date, into the new PDF metadata. This creates a signed duplicate of the original file. When generating a private key, the user also selects a storage location for the corresponding public key. The public key is used within the application to verify the PDF signature. During verification, the application recomputes the PDF hash and decrypts the signed hash from the document using the sender’s public key. If the decrypted hash matches the newly computed one, the signature is confirmed as valid.

Additionally, the project includes documentation generated with Doxygen and a GitHub repository containing the source code and commit history.

Obraz zawierający tekst, Czcionka, numer, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

*Screen of running application.*

* 1. ***Diagram of the application***

Obraz zawierający tekst, zrzut ekranu, diagram, Prostokąt

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

*Fig. 1 – Block diagram.*

* 1. ***Crucial code fragments***
     1. ***Generating private and public key pair:***

***Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Converting private key into PEM format:***

***Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Generating random salt and using it to hash user’s PIN***

***Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Generating random initialization vector and using it and hashed PIN to encrypt private key:***

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. ***Decrypting private key (hashing PIN using salt and then decrypting encrypted key). If wrong PIN is provided, decryption will create invalid PEM key which will throw an exception:***

***Obraz zawierający tekst, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Hashing PDF without metadata and signing the hash with decrypted private key:***

***Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Add metadata with signature, signer name and signing date to new, signed PDF:***

***Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Hashing signed PDF file without metadata:***

***Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* + 1. ***Comparing hash of PDF without metadata with hash in signed PDF metadata after decrypting it using public key:***

***Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.***

* 1. ***Summary***

The project’s code is available on GitHub repository under following link:

* <https://github.com/peterprospl12/breathing-classification-v2>

Repository is under MIT license which means it can be freely used, modified and distributed as long as the original copyright and license notice is kept.

Besides code, repository consists of documentation created using Doxygen tool. In root directory there is Doxyfile which let us automatically create documentation. Created documentation is in ./docs file. Repositorium has README file which has most of the necessary information about the project and running it.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

*Screen of documentation created using Doxygen.*

1. **Literature**

[1] Cryptography module python documentation, <https://cryptography.io/en/latest/hazmat/primitives>

[2] Doxygen documentation, <https://www.doxygen.nl/manual/>

[3] PyQt5 (GUI library) documentation, <https://www.riverbankcomputing.com/static/Docs/PyQt5/>