**Security of Computer Systems**

**Project Report**

Authors:

Jakub, Falk, 193252

Lucjan, Gackowski, 193150

Version: 1.1

**Versions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of changes |
| 1.0 | 04.04.2025 | Creation of the document |
| 1.1 | 07.04.2025 | Added github repository link in Description section and provided Performed Tests section |

1. **Project – control and final term**
   1. ***Description***

The PAdES Signature Application is a comprehensive tool that enables users to create and verify PDF Advanced Electronic Signatures with strong cryptographic security. It implements a complete workflow for generating RSA key pairs, securely storing the private key on USB storage devices protected by PIN-based AES encryption, and signing PDF documents in compliance with industry standards. The application features an intuitive graphical user interface with clear visual indicators for system status, allowing users to easily manage the entire signature process from key generation to signature verification.

Project’s GitHub [repository link](https://github.com/varrios/PAdES-application).

* 1. ***Results***
* **Key Management**
  + Implemented 4096-bit RSA key generation
  + Private keys are encrypted with AES using PIN-based security
  + Keys are properly stored (private on USB, public locally)
* **Document Operations**
  + PDF signing with proper document hashing
  + Signature verification functionality
  + Clear visual feedback during operations
* **User Interface**
  + Three-panel design (keygen, sign, verify)
  + Real-time USB detection and status display
  + Secure PIN entry with visual keypad
* **Application Architecture**
  + Multi-threaded design for responsive UI
  + Modular code structure with clear separation of concerns
  + Comprehensive error handling
* **Documentation**
  + Complete Doxygen documentation
  + Automated documentation generation via GitHub Actions
  + Code properly documented with standard tags
  1. ***Code description***

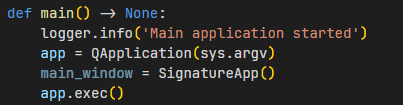
**Architecture Overview**

The PAdES Signature Application follows a modular architecture with clear separation of concerns. The codebase is organized into three primary components:

* **GUI Layer**: Contains the user interface implementation using PyQt6
* **Utility Layer**: Implements core cryptographic and file operations
* **Logger**: Handles application-wide logging

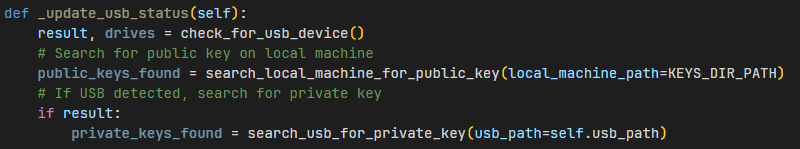
**Key Components**

* **Main Application (**main.py**) -** The entry point of the application initializes the logger and launches the main window:

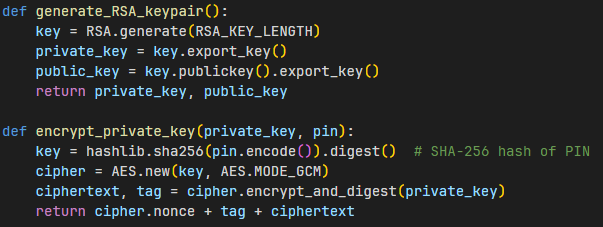


* **Signature Application (**SignatureApp.py**) -** The main application window manages three key pages:
  + Key Generation Page
  + Document Signing Page
  + Signature Verification Page

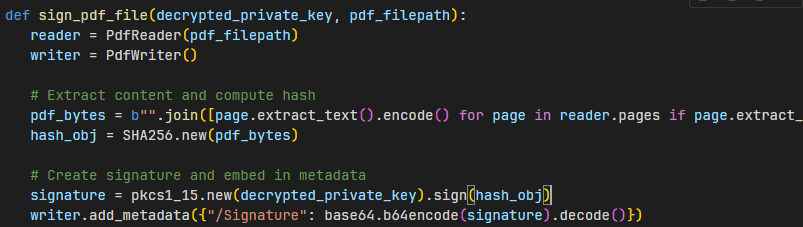
It also handles USB detection, key discovery, and page navigation:



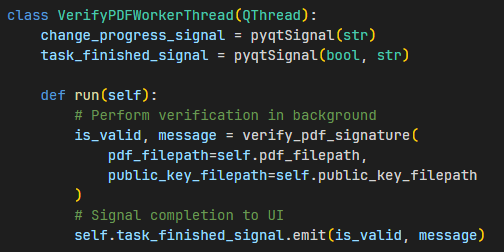
* **Cryptographic Operations (keygen.py, pdf\_sign.py) -** The core security operations are implemented in specialized modules:



* **PDF Operations (**pdf\_sign.py**) -** The PDF signing and verification uses PyPDF2 to handle the PDF files, with custom signature embedding and extraction:



* **Worker Threads (**RSAWorkerThread.py, PDFWorkerThread.py, VerifyPDFWorkerThread.py**) -** Long-running operations are executed in background threads to keep the UI responsive:



* 1. ***Performed Tests Summary***
  + Key generation with RSA 4096-bit keys
  + Private key encryption with user-defined PIN
  + Attempting private key encryption with missing or invalid PIN
  + Signing a PDF document using a valid private key with correct PIN provided
  + Attempting signing a PDF document using a valid private key with incorrect PIN provided
  + Attempting signing a PDF document using invalid or missing private key
  + Attempting signing a PDF document which already has been signed
  + Verifying a signed PDF with the correct public key
  + Attempting verifying a signed PDF with the incorrect public key
  + Attempting verifying a missing/corrupted PDF document
  + Detecting changes in a tampered signed document
  + Handling incorrect PIN entry during signing
  + USB detection and key file recognition
  + PIN input using an on-screen virtual keypad
  + Maintaining UI responsiveness during cryptographic operations
  1. ***Summary***

The PAdES Signature Application successfully implements all required functionality for creating and verifying PDF Advanced Electronic Signatures. The application features robust key management with 4096-bit RSA key pairs, PIN-protected private keys on USB devices, and local public key storage. Document operations include PDF signing and verification with proper security measures. The implementation uses a user-friendly interface with clear status indicators and multi-threaded architecture for responsive operation. The application is fully documented with Doxygen comments and includes GitHub Actions for automatic documentation generation.

1. **Literature**

[1] Doxygen docs, <https://www.doxygen.nl/manual/index.html>

[2] Wikipedia Digital Signature, <https://en.wikipedia.org/wiki/Digital_signature>

[3] Python docs, <https://docs.python.org/3/>

[4] GitHub Actions docs, <https://docs.github.com/en/actions>