Security of Computer Systems

Project Report

Authors:
Patryk Sowiński-Toczek, 191711
Arkadiusz Szamocki, 184623

Version: 1.0

Versions

Version	Date	Description of changes
1.0	13.04.2025	Powstanie dokumentu

1. Project – control term

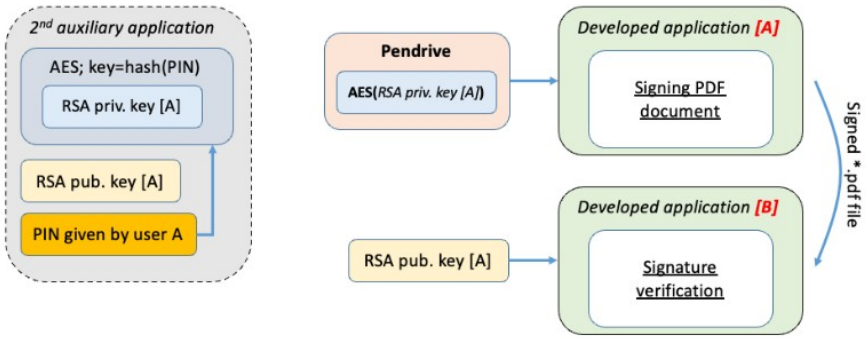
1.1 Description

W ramach zajęć projektowych koniecznym jest przygotowanie dwóch aplikacji - głównej oraz dodatkowej, którę będą umożliwiały użytkownikowi wygenerowanie pary klucza prywatnego oraz klucza publicznego (aplikacja dodatkowa), które następnie posłużą do podpisywania oraz weryfikowania plików w formacie PDF zgodnie ze standardem PAdES.

Do realizacji projektu został wykorzystany język Python wraz z interfejsem Tk (tkinter) oraz bibliotekami pycryptodome oraz cryptography.

Założenia projektu są wyszczególnione w osobnym pliku znajdującym się na platformie eNauczanie w kursie "Bezpieczeństwo Systemów Komputerowych - 2025".

Schemat docelowego projektu:



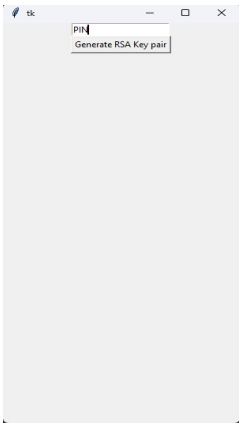
Rysunek 1 - Schemat blokowy konceptu projektu do zrealizowania

1.2 Results

Na termin kontrolny została wykonana aplikacja dodatkowa umożliwiająca generowanie pary kluczy publicznego i prywatnego z wykorzystaniem bibliotek pycryptodome oraz cryptography. Klucz prywatny został zabezpieczony z wykorzystaniem algorytmu szyfrującego AES w trybie ECB oraz algorytmu haszującego SHA-256. Interfejs aplikacji powstał w oparciu o Tkinter.

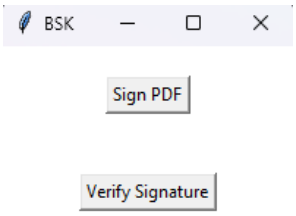
Użytkownik podaje 16 bajtowy PIN (długość jest walidowana przez aplikację), który jest przetwarzany przez funkcję skrótu SHA-256 tworząc 32 bajtowy klucz szyfrujący, przy wykorzystaniu którego klucz prywatny jest szyfrowany AES w trybie ECB.

Na dysku, w lokalizacji w której przechowywana jest aplikacja, powstają dwa pliki - encrypted - z zaszyfrowanym kluczem prywatnym, oraz encrypted.pub - z kluczem publicznym.

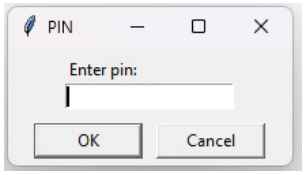


Rysunek 2 - Interfejs aplikacji dodatkowej

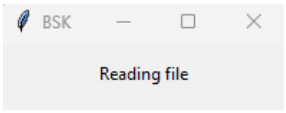
Powstał również szkielet aplikacji głównej, który umożliwia odszyfrowanie klucza prywatnego powstałego w aplikacji dodatkowej po podaniu PINu. Interfejs aplikacji powstał w oparciu o Tkinter. Przyciski "Sign PDF" oraz "Verify Signature" umożliwiają wskazania pliku w formacie pdf. W przypadku "Verify Signature", aplikacja informuje o swoim stanie (tj. wyświetla informację o odczytywaniu pliku).



Rysunek 3 - Ekran główny aplikacji



Rysunek 4 - Okno z prośba o wpisanie PINu użytkownika



Rysunek 5 - Okno informujące użytkownika o stanie aplikacji

1.3 Summary

W ramach terminu kontrolnego zajęć projektowych powstał szkielet aplikacji, która docelowo będzie służyła do podpisywania plików w formacie pdf kluczem prywatnym zgodnie ze standardem PAdES oraz weryfikowania podpisu z wykorzystaniem klucza publicznego.

Pliki źródłowe są dostępne na platformie GitHub pod adresem: https://github.com/Shubale/pdfsinger

2. Literature

[1] https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html#_pades_signature_pdf

[2] https://opensource.adobe.com/dc-acrobat-sdk-docs/pdfstandards/PDF32000_2008.pdf

[3] https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.02.01_60/en_31914201v010201p.pdf