Security of Computer Systems

Project Report

Authors:
Oskar, Wilda, 188924
Marcin, Stenka, 188985

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	18.04.2024	Creation of the document
1.1	…	…

1. Project – control term

1.1 Description

Głównym celem projektu jest stworzenie narzędzia oprogramowania do emulacji kwalifikowanego podpisu elektronicznego, na przykład do podpisywania dokumentów, a ponadto podstawowych operacji szyfrowania. Celem jest pełna emulacja procesu, w tym niezbędnego sprzętu do identyfikacji osoby.

1.2 Results

W ramach terminu kontrolnego udało nam się zrealizować podane właściwości:

1. Powstał program z interfejsem użytkownika dający takie opcje jak:
   - generowanie klucza publicznego i prywatnego użytkownika oraz podanie pinu do zaszyfrowania klucza prywatnego,
   - podanie przez użytkownika pliku, który chciałby zaszyfrować,
   - podanie przez użytkownika klucza, którym chce zaszyfrować plik,
2. Powstał program pozwalający na generowanie podpisu w postaci pliku XML zawierającego:
   - informacje o podpisanym dokumencie takie jak jego rozmiar, rozszerzenie oraz ostatnia data modyfikacji,
   - nazwę osoby podpisującej,
   - informację o użytym algorytmie hashowania,
   -timestamp,
3. Powstał program generujący parę kluczy prywatny i publiczny użytkownika i szyfrujący klucz prywatny za pomocą algorytmu AES z podaym przez użytkownika kodem PIN.

Wszytkie programy zostały napisane w języku Python z wykorzystaniem takich bibliotek jak tkinker – do stworzenia GUI oraz cryptography – do stworzenia pary kluczy oraz zaszyfrowania klucza prywatnego.

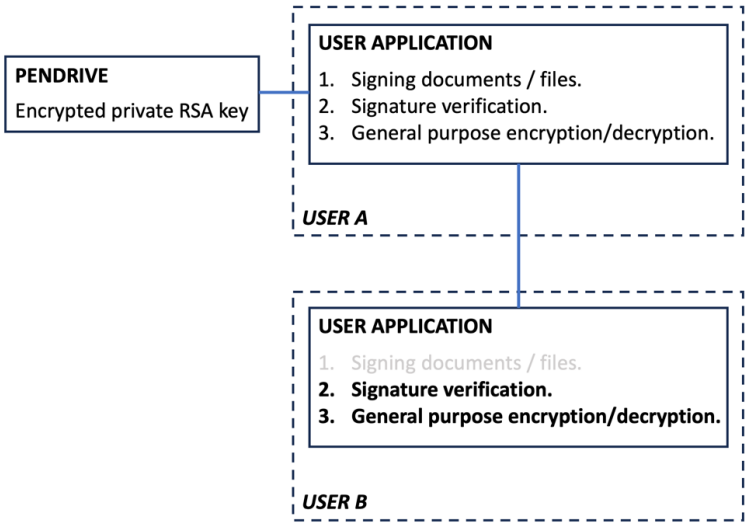

Fig. 1 – Block diagram.

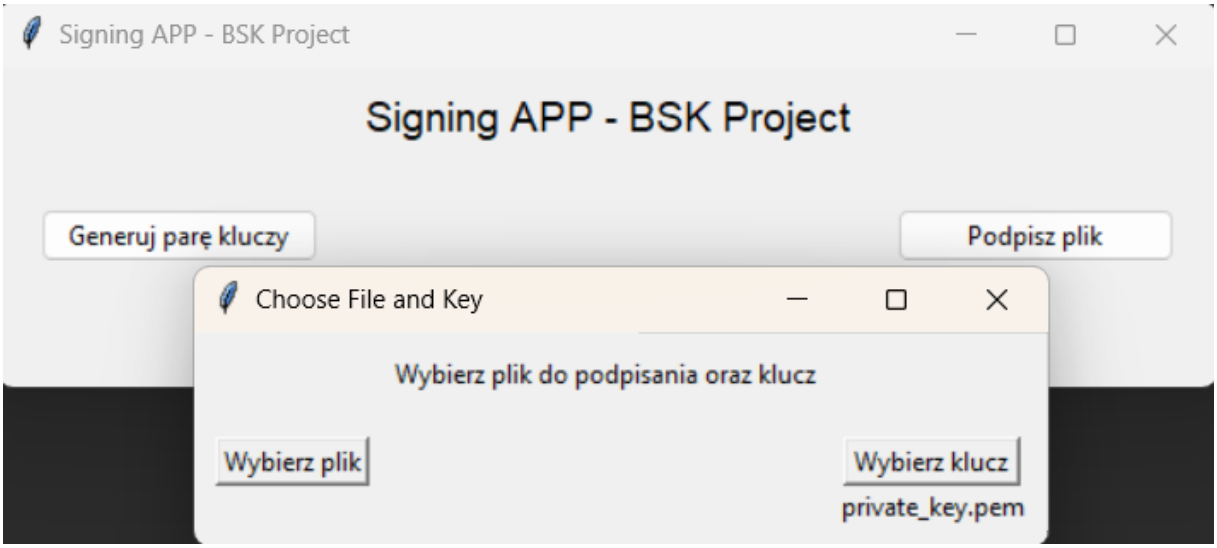

Fig. 2 – First version of GUI

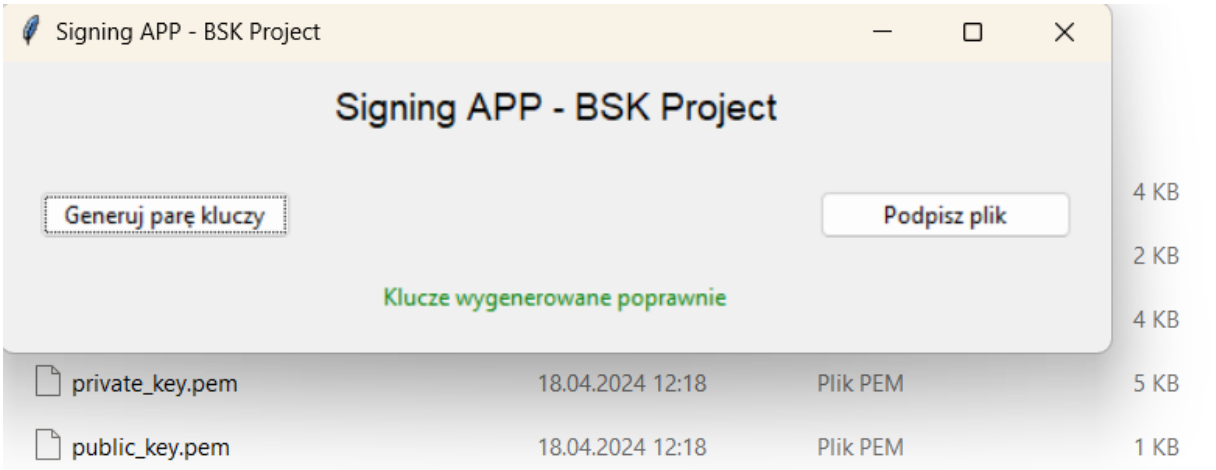

Fig. 3 – Key pair generated by User A

1.3 Summary

Elementy, które pozostały nam do wykonania do terminu końcowego to:
- tworzenie hasha wiadomości użytkownika A,
- szyfrowanie wybranej przez użytkownika A wiadomości,
- odszyfrowanie przez użytkownika B wiadomości otrzymanej od użytkownika A,
- sprawdzenie podpisu dokumentu przez użytkownika B

2. Project – Final term

2.1 Description

Content

2.2 Code Description

Content

```
/*!
  *  A list of events:
  *  <ul>
  *  <li> mouse events
  *     <ol>
  *     <li>mouse move event
  *     <li>mouse click event<br>
  *         More info about the click event.
  *     <li>mouse double click event
  *     </ol>
  *  <li> keyboard events
  *     <ol>
  *     <li>key down event
  *     <li>key up event
  *     </ol>
  *  </ul>
  *  More text here.
  */
```

List. 1 – Code listing [2].

Final Content.

2.3 Description

Content

2.4 Results

Content

2.5 Summary

Content

3. Literature

[1] Article.

[2] Online Doxygen documentation, https://www.doxygen.nl/manual/lists.html, (accessed on 18.02.2024).

[3] Book.