Security of Computer Systems

Project Report

Authors:
Paweł Wawrzyński, 193270
Filip Jezierski, 196333

Version: 1.1

Versions

Version	Date	Description of changes
1.0	08.03.2025	First version of the document, description of application for generating keys
1.1	10.04.2025	Finished section 1. Project - control term, added link to GitHub repository

1. Project – control term

1.1 Description

The main task of the project is to design and develop an application to make a qualified electronic signature according to PAdES (PDF Advanced Electronic Signature) standard concept. The project consists of two applications - main application verifying qualified electronic signatures and the other one for generating keys which are encrypted with the user's PIN number.

1.2 Results

GitHub repository

https://github.com/MrKtosiek/BSK-PDF-Signature

Technologies used

Both applications are written in Python with usage of Python Cryptography Toolkit (pycrypto) library used for encrypting data and generating RSA keys. For user interface we used ttkbootstrap library.

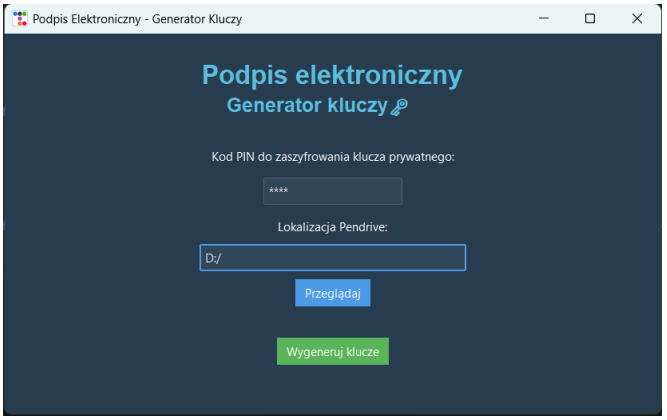
```python
import os
import hashlib
import ttkbootstrap as ttk
from ttkbootstrap.constants import *
from Crypto.PublicKey import RSA
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
from tkinter import filedialog
```

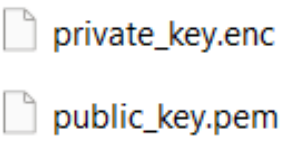
Used dependencies

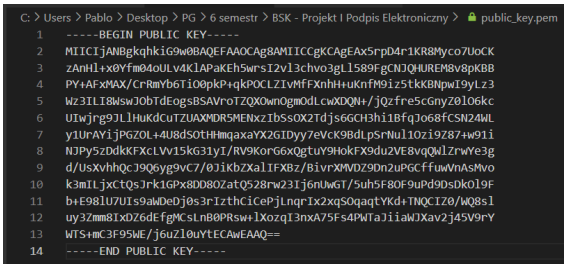
Application for generating keys

This application is used for generating a public key which is saved in the .pem format and a private key which is encrypted with the 256-bit AES cipher algorithm. The user has to enter a PIN number - it's important not to forget it because later the PIN is used to decrypt the private RSA key before signing a document.

- Encrypted private key is stored on a pendrive and can be used in order to sign a PDF document.
- Public key is used to verify the authenticity of a signed document







Application for signing PDF document and signature verification

Not implemented yet.

1.3 Summary

Both applications are simple but useful and work as intended. They allow the user to sign as well as verify the signature - it's a common practice especially if documents are important ex. VAT invoices/payment confirmations etc. After verifying the signature you can be sure that the document is legitimate.

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 01.02.2025).

[3] Book.