Security of Computer Systems

Project Report

Authors:
Franciszek, Gwarek, 193192
Maciej, Górlaczyk, 193302

Version: 1.0

Versions

Version	Date	Description of changes
1.0	14.04.2025	Creation of the document and the control term section

1. Project – control term

1.1 Description

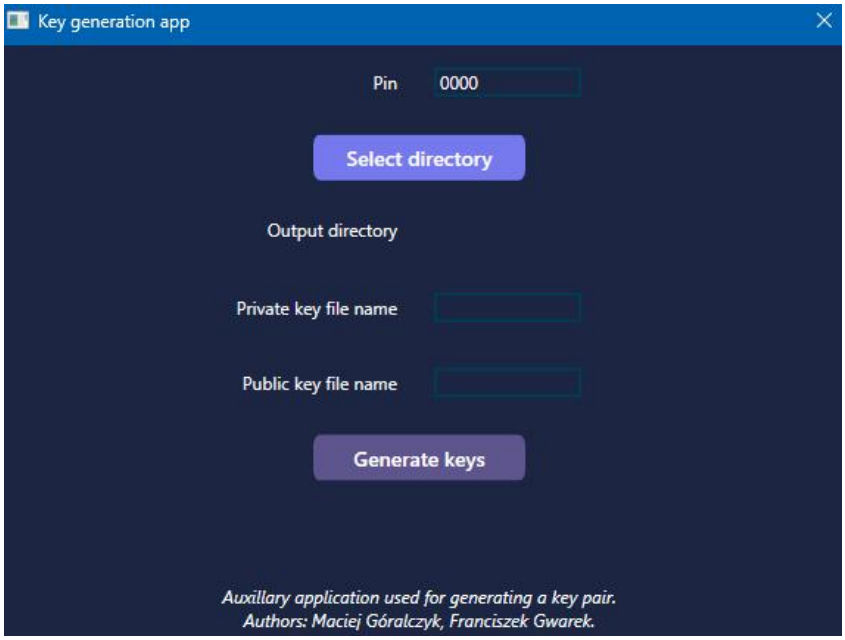
The primary goal of the first part of the project is to design and develop a supporting application that generates an RSA key pair and secures the private key using the AES algorithm, with the encryption key derived from the user's PIN. Additionally, this part includes the initial design of an application intended for creating qualified electronic signatures based on the PAdES standard concept.

1.2 Results

GitHub repository: https://github.com/Manie-K/PDF-signer

Technologies used: Both applications were written in C# using WPF and .NET. The standard *System.Security.Cryptography* library was used for generating keys and encrypting the private key.

Application for generating keys: The user provides the file save location, file names, and a PIN.
The application then generates an RSA key pair (public and private keys) using a 4096-bit key and a cryptographically secure pseudorandom number generator.
Next, the private key is encrypted using the AES algorithm with a 256-bit key derived from the hash of the user's PIN.
Both the public and private keys are saved in .key format at the location specified by the user.



Application for making qualified electronic signature: Only a basic framework is implemented.

1.3 Summary

The additional application for key generation is fully implemented and functions as intended. An initial concept and a basic framework of the main application have also been developed.

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] https://enauczanie.pg.edu.pl/moodle/pluginfile.php/2465479/mod_resource/content/6/ENG_SCS_2025_project_v1.pdf

[2] Online Doxygen documentation, https://www.doxygen.nl/manual/lists.html, (accessed on 01.02.2025).