Security of Computer Systems

Project Report

Authors:
Mikołaj, Storoniak, 188806

Version: 1.0

Versions

Version	Date	Description of changes
1.0	16.04.2024	Creation of the document

1. Project – control term

1.1 Description

The requirements for the app have been partially fulfilled – including key generation and encryption, as well as signing documents and verifying signatures. Some of the implemented functionalities are still inaccessible through the GUI and need to be used from code level. There is no support for the hardware tool yet.

1.2 Results

PyCryptodome library has been used for all cryptography functions.

The following requiremets have been implemented so far:

1. Key generation
    a. It is possible to generate a pair of keys – the length of private key is 4096 bits.
    b. During creation, the private key is encrpyted with AES algorithm, using 16-byte password.
    c. At the moment, AES algorithm works in ECB mode. This will be changed in the future.
    d. The password consists of the first 16 bytes of SHA256 hash of the PIN provided by user during creation of the key.
    e. PIN has to be at least 4 characters long.
2. Document signing
    a. The application is able to automatically get metadata about document: size, file type and last modification time
    b. Signature uses RSA algorithm
    c. Signature is generated in xml format. Apart from metadata it includes:
        i. Signed file hash
        ii. Signer’s name
        iii. Signature time
    d. During verification, the app verifies the signature, as well as the metadata: for example it is possible to check, that the signature is valid (and therefore file contents are original), but last date of modification is different than at the time of signing.
3. Graphic interface

a. So far, only key generation feature is supported.
b. Rest of the functionalities must be accessed as functions in code

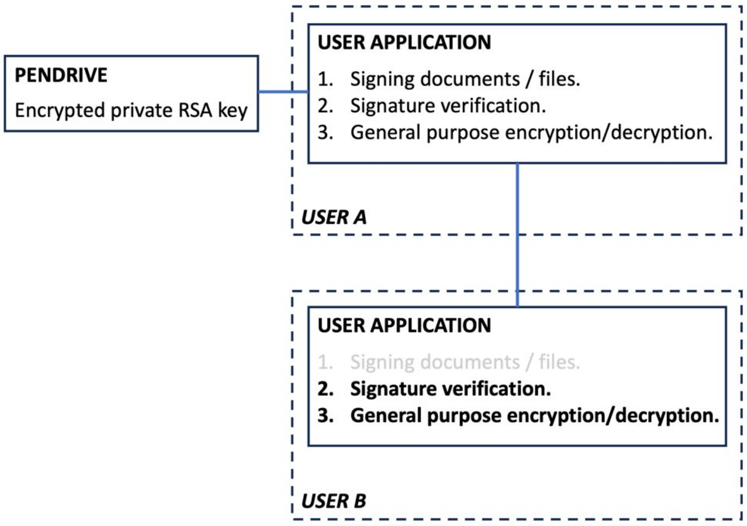
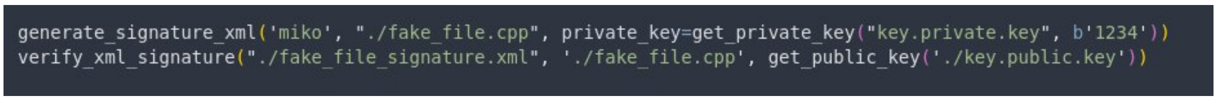
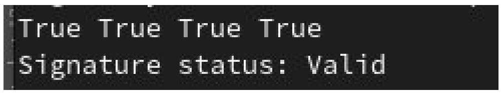

PENDRIVE
Encrypted private RSA key
USER APPLICATION
1. Signing documents / files.
2. Signature verification.
3. General purpose encryption/decryption.
USER A
USER APPLICATION
1. Signing documents / files.
2. Signature verification.
3. General purpose encryption/decryption.
USER B

Fig. 1 – Block diagram.

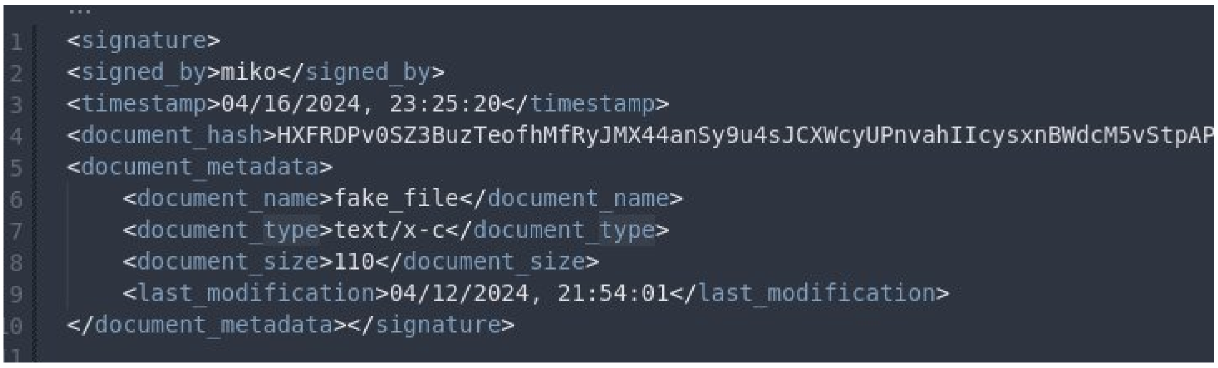


```
generate_signature_xml('miko', "./fake_file.cpp", private_key=get_private_key("key.private.key", b'1234'))
verify_xml_signature("./fake_file_signature.xml", './fake_file.cpp', get_public_key('./key.public.key'))
```



```
True True True True
Signature status: Valid
```

Fig. 2 and 3 – Signature creation and verification. True,True,True, True means, that no metadata has been altered.



```
<signature>
<signed_by>miko</signed_by>
<timestamp>04/16/2024, 23:25:20</timestamp>
<document_hash>HXFRDPv0SZ3BuzTeofhMfRyJMX44anSy9u4sJCXWcyUPnvahIIcysxnBWdcM5vStpAP
<document_metadata>
    <document_name>fake_file</document_name>
    <document_type>text/x-c</document_type>
    <document_size>110</document_size>
    <last_modification>04/12/2024, 21:54:01</last_modification>
</document_metadata></signature>
```

Fig. 4 – Signature in xml format.

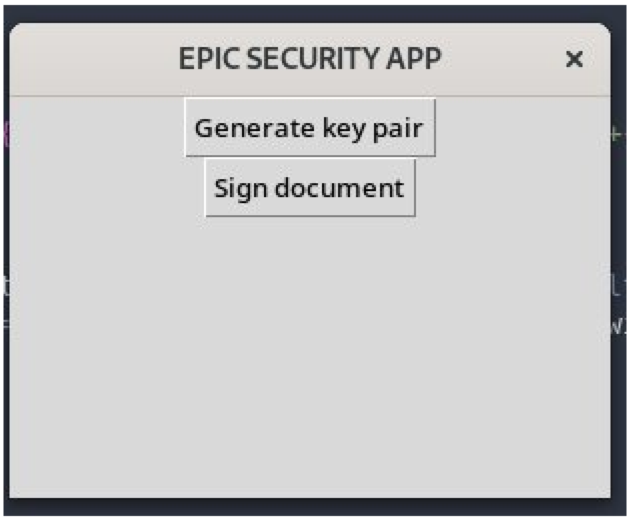
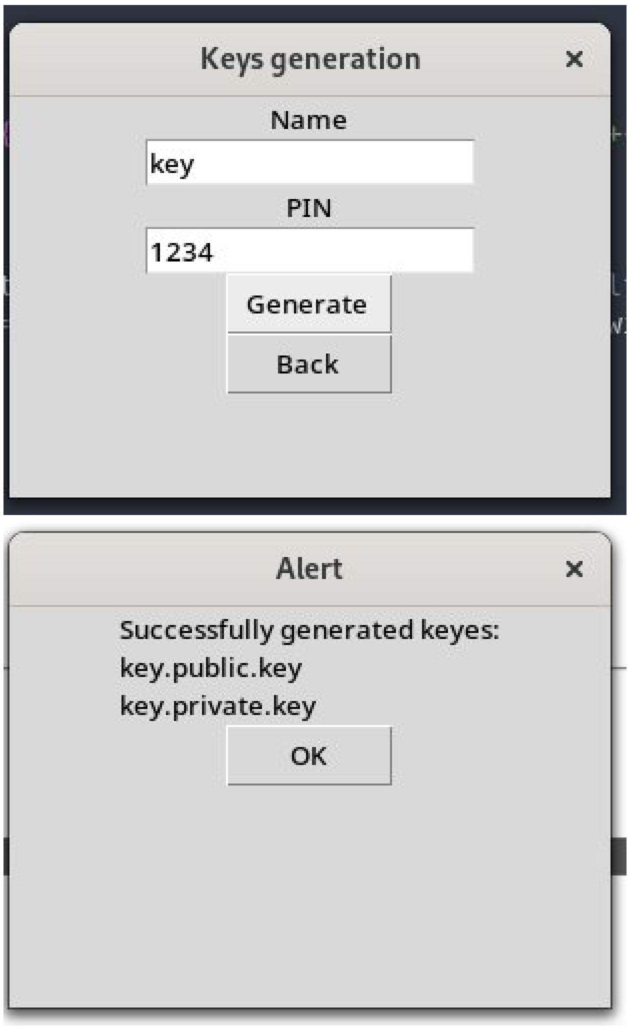


Fig. 5 – Current state of main menu



Name
key
PIN
1234

Successfully generated keyes:
key.public.key
key.private.key

Fig. 6 and 7 – Key creation.

1.3 Summary

Although a great deal of the functionalities has been implemented, there is still much work left – especially regarding GUI.

2. Project – Final term

2.1 Description

2.2 Code Description

```
/*!
  *  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://www.pycryptodome.org/https

[2] https://en.wikipedia.org/wiki/XAdES