

# Bezpieczeństwo Systemów Komputerowych

Raport projektu

Jakub Buczkowski 188894

Wersja: 1.2

# Contents

<b>1</b>	<b>Wersje</b>	<b>2</b>
<b>2</b>	<b>Opis projektu</b>	<b>2</b>
2.1	Ogólny opis	2
2.2	Szczegółowy opis	3
2.2.1	Generacja klucza RSA	3
2.2.2	Wyświetlenie kluczy RSA	3
2.2.3	Sprawdzenie zgodność klucza publicznego z prywatnym	3
2.2.4	Podpisanie pliku	3
2.2.5	Walidacja podpisu	3
2.2.6	Szyfrowanie pliku	3
2.2.7	Odszyfrowanie pliku	4
<b>3</b>	<b>Opis kodu</b>	<b>5</b>
<b>4</b>	<b>Wyniki</b>	<b>84</b>
4.1	Generowanie kluczy	84
4.1.1	Wyświetlanie kluczy*	85
4.1.2	Poprawność kluczy*	85
4.2	Podpisywanie plików	86
4.3	Szyfrowanie pliku	87
4.4	Deszyfrowanie pliku	88
4.5	Walidacja podpisu	88
<b>5</b>	<b>Podsumowanie</b>	<b>90</b>

# 1 Wersje

Wersja	Data	Opis
1.0	06.04.2024	Utworzenie dokumentu
1.1	12.04.2024	Dodanie opisu kodu
1.2	15.04.2024	Dodanie opisu projektu, wyników i podsumowania

## 2 Opis projektu

### 2.1 Ogólny opis

Celem projektu jest stworzenie aplikacji służącej do podpisywania podpisem kwalifikowanym dowolnych plików z wykorzystaniem standardu XAdES oraz ich zaszyfrowania. Schemat aplikacji przedstawiono w Figure 1

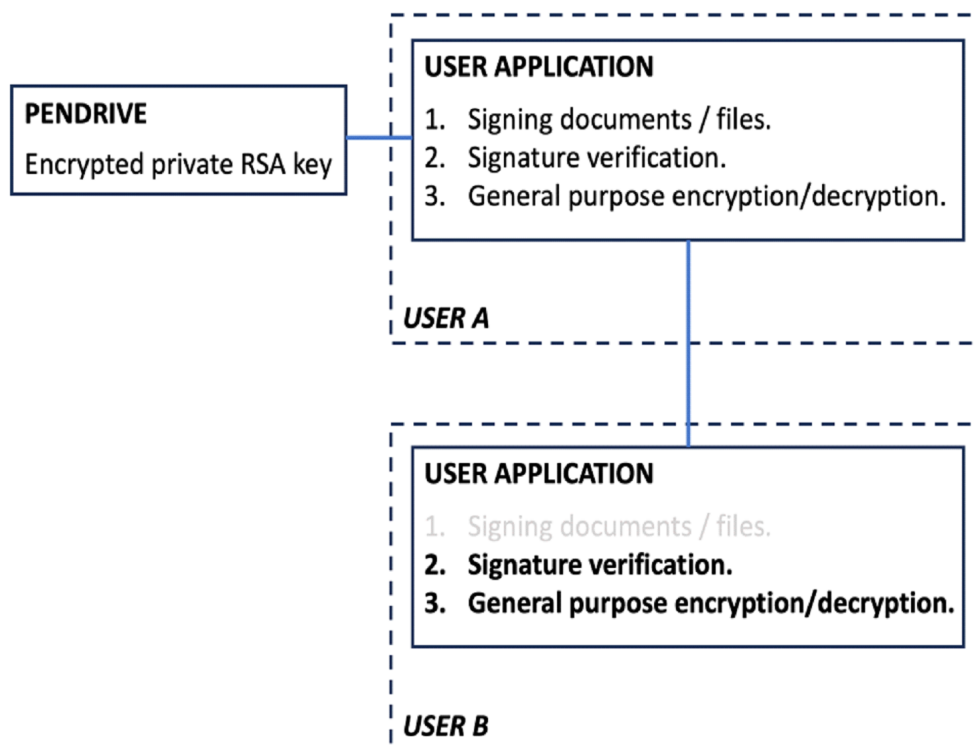


Figure 1: Diagram blokowy projektu

Aplikacja została napisana w języku Java z wykorzystaniem domyślnej biblioteki graficznej Swing i Crypto. Użytkownik **A** jest w stanie wygenerować parę kluczy **4096** bitowych **RSA** (private.key i public.key). Wybiera lokalizację ich zapisu np. pendrive. Klucz prywatny (private.key) jest dodatkowo zaszyfrowany przy pomocy algorytmu **AES**. Następnie przy pomocy tej pary kluczy jest w stanie podpisać, oraz zaszyfrować wybrany plik algorytmem **RSA**.

Użytkownik **B** może przy pomocy klucza publicznego, który otrzymał od użytkownika **A** odszyfrować podpisany plik. Do weryfikacji podpisu nie potrzebuje pliku z kluczem publicznym, ponieważ klucz publiczny zawarty jest w strukturze podpisu w znaczniku <KeyInfo>.

## 2.2 Szczegółowy opis

Aplikacja udostępnia 7 funkcji, które można wykorzystać klikając odpowiedni przycisk. Funkcje z jakich możemy skorzystać to:

1. [Generacja klucza RSA](#)
2. [Wyświetlenie kluczy RSA](#)
3. [Sprawdzenie zgodność klucza publicznego z prywatnym](#)
4. [Podpisanie pliku](#)
5. [Walidacja podpisu](#)
6. [Szyfrowanie pliku](#)
7. [Odszyfrowanie pliku](#)

### 2.2.1 Generacja klucza RSA

Funkcja na początku generuje parę kluczy 4096 bitowych RSA [3]. Wyodrębniany z tej pary jest klucz publiczny i zapisywany w pamięci, a klucz prywatny jest przekazywany do zaszyfrowania. Elementem tego szyfrowania jest wygenerowanie klucza na podstawie podanego hasła. Przy pomocy tego hasła generowany jest sekretny klucz [1], który jest potem wykorzystywany do zainicjowania algorytmu AES [2].

### 2.2.2 Wyświetlenie kluczy RSA

Funkcja składa się z dwóch etapów. Pierwszy etap to pobranie klucza publicznego, z wybranego pliku. Potem jest on dekodowany do formatu czytelного dla Javy [4]. Następnie klucz prywatny jest odszyfrowany hasłem [1] z algorytmem AES[2] i deszyfrowany do formatu czytelного dla Java [5]

### 2.2.3 Sprawdzenie zgodność klucza publicznego z prywatnym

Funkcja, która na testowych danych sprawdza czy możliwe jest odszyfrowanie za pomocą klucza publicznego, wiadomości zaszyfrowanej kluczem prywatnym. Jeżeli jest to możliwe to dana para kluczy jest zgodna. Jest to przydatna opcja przy posiadaniu dużej ilości różnych kluczy, co do których nie mamy pewności czy są parą.

### 2.2.4 Podpisanie pliku

Funkcja generuje podpis w formacie XAdES tworząc wymagane znaczniki. Podpis XAdES jest rozwinięciem formatu XMLDSIG o dodatkowe informacje zawarte w pliku podpisu i również podpisane. W tym przypadku przechowujemy dodatkowo informacje o rozmiarze, rozszerzeniu, dacie modyfikacji pliku, osobie podpisującej i czasie stworzenia podpisu. W podpisie zawarty jest hash dokumentu wygenerowany za pomocą klucza prywatnego RSA [6][7].

### 2.2.5 Walidacja podpisu

Funkcja sprawdza poprawność pliku na podstawie otrzymanego podpisu. Porównuje hash zawarty w pliku podpisu z hashem jaki wygeneruje z pliku, który jest podpisywany. Później sprawdza hash właściwości zawartych w pliku podpisu, czy nie zostały naruszone.

### 2.2.6 Szyfrowanie pliku

Funkcja szyfrująca plik przy pomocy klucza prywatnego RSA[3].

### 2.2.7 Odszyfrowanie pliku

Funkcja deszyfrująca plik przy pomocy klucza prywatnego RSA[3].

1. [PBKDF2With](#) ta część tego parametru odpowiada za generację klucza na podstawie hasła z wykorzystaniem algorytmu pseudolosowego [HmacSHA256](#)
2. [AES](#) w formie [ECB](#) z przesunięciem [PKCS5Padding](#)
3. Generuje klucze algorytmu [RSA](#) w formie [ECB](#) z przesunięciem [PKCS5Padding](#)
4. <https://docs.oracle.com/javase/8/docs/api/java/security/spec/X509EncodedKeySpec.html>
5. <https://docs.oracle.com/javase/8/docs/api/java/security/spec/PKCS8EncodedKeySpec.html>
6. [https://portal.etsi.org/webapp/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=35243](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=35243)
7. <https://docs.oracle.com/javase/8/docs/api/javax/xml/crypto/dsig/XMLSignatureFactory.html>

### 3 Opis kodu

Bezpieczeństwo Systemów Komputerowych - 2024  
1.0

Generated by Doxygen 1.10.0

<b>1 Hierarchical Index</b>	<b>1</b>
1.1 Class Hierarchy . . . . .	1
<b>2 Class Index</b>	<b>3</b>
2.1 Class List . . . . .	3
<b>3 Class Documentation</b>	<b>5</b>
3.1 org.example.controller.impl.AppController Class Reference . . . . .	5
3.1.1 Detailed Description . . . . .	5
3.1.2 Member Function Documentation . . . . .	5
3.1.2.1 decryptFile() . . . . .	5
3.1.2.2 deleteFile() . . . . .	6
3.1.2.3 encryptFile() . . . . .	6
3.1.2.4 getFileAttribute() . . . . .	6
3.1.2.5 getPrivateKey() . . . . .	6
3.1.2.6 getPublicKey() . . . . .	7
3.1.2.7 loadFile() . . . . .	7
3.1.2.8 saveFile() . . . . .	7
3.1.2.9 setRSAKeys() . . . . .	8
3.1.2.10 signFile() . . . . .	8
3.1.2.11 validateFile() . . . . .	8
3.2 org.example.app.buttons.api.DecryptFile Interface Reference . . . . .	9
3.2.1 Detailed Description . . . . .	9
3.2.2 Member Function Documentation . . . . .	9
3.2.2.1 decryptFile() . . . . .	9
3.2.2.2 selectFilePath() . . . . .	10
3.2.2.3 selectPublicKeyPath() . . . . .	10
3.3 org.example.app.buttons.impl.DecryptFileButton Class Reference . . . . .	10
3.3.1 Detailed Description . . . . .	11
3.3.2 Constructor & Destructor Documentation . . . . .	11
3.3.2.1 DecryptFileButton() . . . . .	11
3.3.3 Member Function Documentation . . . . .	11
3.3.3.1 decryptFile() . . . . .	11
3.3.3.2 printLog() . . . . .	11
3.3.3.3 selectFilePath() . . . . .	12
3.3.3.4 selectPublicKeyPath() . . . . .	12
3.4 org.example.app.buttons.api.EncryptFile Interface Reference . . . . .	12
3.4.1 Detailed Description . . . . .	13
3.4.2 Member Function Documentation . . . . .	13
3.4.2.1 collectPassword() . . . . .	13
3.4.2.2 encryptFile() . . . . .	13
3.4.2.3 selectFilePath() . . . . .	13
3.4.2.4 selectPrivateKeyPath() . . . . .	14

3.5 org.example.app.buttons.impl.EncryptFileButton Class Reference . . . . .	14
3.5.1 Detailed Description . . . . .	14
3.5.2 Constructor & Destructor Documentation . . . . .	14
3.5.2.1 EncryptFileButton() . . . . .	14
3.5.3 Member Function Documentation . . . . .	15
3.5.3.1 collectPassword() . . . . .	15
3.5.3.2 encryptFile() . . . . .	15
3.5.3.3 printLog() . . . . .	15
3.5.3.4 selectFilePath() . . . . .	16
3.5.3.5 selectPrivateKeyPath() . . . . .	16
3.6 org.example.file.funtions.EncryptingDecryptingFileFunction Class Reference . . . . .	16
3.6.1 Detailed Description . . . . .	16
3.6.2 Member Function Documentation . . . . .	16
3.6.2.1 DecryptingFile() . . . . .	16
3.6.2.2 EncryptingFile() . . . . .	17
3.7 org.example.file.data.api.FileLoader Interface Reference . . . . .	17
3.7.1 Detailed Description . . . . .	18
3.7.2 Member Function Documentation . . . . .	18
3.7.2.1 deleteFile() . . . . .	18
3.7.2.2 getFileAttribute() . . . . .	18
3.7.2.3 loadFile() . . . . .	18
3.7.2.4 saveFile() . . . . .	19
3.8 org.example.file.data.impl.FileLoaderDefault Class Reference . . . . .	19
3.8.1 Detailed Description . . . . .	20
3.8.2 Member Function Documentation . . . . .	20
3.8.2.1 deleteFile() . . . . .	20
3.8.2.2 getFileAttribute() . . . . .	20
3.8.2.3 loadFile() . . . . .	20
3.8.2.4 saveFile() . . . . .	21
3.9 org.example.file.service.api.FileSecurityService Interface Reference . . . . .	21
3.9.1 Detailed Description . . . . .	22
3.9.2 Member Function Documentation . . . . .	22
3.9.2.1 decrypte() . . . . .	22
3.9.2.2 encrypte() . . . . .	22
3.10 org.example.file.service.impl.FileSecurityServiceDefault Class Reference . . . . .	22
3.10.1 Detailed Description . . . . .	23
3.10.2 Member Function Documentation . . . . .	23
3.10.2.1 decrypte() . . . . .	23
3.10.2.2 encrypte() . . . . .	23
3.11 org.example.file.service.api.FileService Interface Reference . . . . .	24
3.11.1 Detailed Description . . . . .	24
3.11.2 Member Function Documentation . . . . .	24



3.11.2.1 delete()	24
3.11.2.2 getFileAttribute()	25
3.11.2.3 load()	25
3.11.2.4 save()	25
3.12 org.example.file.service.impl.FileServiceDefault Class Reference	26
3.12.1 Detailed Description	26
3.12.2 Member Function Documentation	26
3.12.2.1 delete()	26
3.12.2.2 getFileAttribute()	27
3.12.2.3 load()	27
3.12.2.4 save()	27
3.13 org.example.keyRSA.data.api.KeyLoader Interface Reference	28
3.13.1 Detailed Description	28
3.13.2 Member Function Documentation	28
3.13.2.1 loadKey()	28
3.13.2.2 saveKey()	29
3.14 org.example.keyRSA.data.impl.KeyLoaderDefault Class Reference	29
3.14.1 Detailed Description	29
3.14.2 Member Function Documentation	29
3.14.2.1 loadKey()	29
3.14.2.2 saveKey()	30
3.15 org.example.misc.Logger Interface Reference	30
3.15.1 Detailed Description	30
3.15.2 Member Function Documentation	31
3.15.2.1 printLog()	31
3.16 org.example.app.textFields.api.LogsField Interface Reference	31
3.16.1 Detailed Description	31
3.16.2 Member Function Documentation	32
3.16.2.1 clear()	32
3.16.2.2 print()	32
3.17 org.example.app.textFields.impl.LogsFieldComponent Class Reference	32
3.17.1 Detailed Description	32
3.17.2 Constructor & Destructor Documentation	33
3.17.2.1 LogsFieldComponent()	33
3.17.3 Member Function Documentation	33
3.17.3.1 clear()	33
3.17.3.2 print()	33
3.18 org.example.Main Class Reference	33
3.19 org.example.app.mainPanel.api.MainPanel Interface Reference	34
3.19.1 Detailed Description	34
3.19.2 Member Function Documentation	34
3.19.2.1 addComponents()	34

3.19.2.2 config()	34
3.20 org.example.app.mainPanel.impl.Panel Class Reference	35
3.20.1 Detailed Description	35
3.20.2 Constructor & Destructor Documentation	35
3.20.2.1 Panel()	35
3.20.3 Member Function Documentation	35
3.20.3.1 addComponents()	35
3.20.3.2 config()	35
3.21 org.example.app.textFields.api.PasswordInput Interface Reference	36
3.21.1 Detailed Description	36
3.21.2 Member Function Documentation	36
3.21.2.1 getPassword()	36
3.22 org.example.app.textFields.impl.PasswordInputComponent Class Reference	36
3.22.1 Detailed Description	37
3.22.2 Constructor & Destructor Documentation	37
3.22.2.1 PasswordInputComponent()	37
3.22.3 Member Function Documentation	37
3.22.3.1 getPassword()	37
3.23 org.example.keyRSA.functions.PrivateKeyDecryptorFunction Class Reference	37
3.23.1 Detailed Description	37
3.23.2 Constructor & Destructor Documentation	37
3.23.2.1 PrivateKeyDecryptorFunction()	37
3.23.3 Member Function Documentation	38
3.23.3.1 getPr()	38
3.24 org.example.keyRSA.functions.PublicKeyDecryptorFunction Class Reference	38
3.24.1 Detailed Description	38
3.24.2 Constructor & Destructor Documentation	38
3.24.2.1 PublicKeyDecryptorFunction()	38
3.24.3 Member Function Documentation	39
3.24.3.1 getKey()	39
3.25 org.example.app.buttons.api.RSAGenerate Interface Reference	39
3.25.1 Detailed Description	39
3.25.2 Member Function Documentation	39
3.25.2.1 collectPassword()	39
3.25.2.2 generateRSA()	39
3.25.2.3 selectPath()	40
3.26 org.example.app.buttons.impl.RSAGenerateButton Class Reference	40
3.26.1 Detailed Description	40
3.26.2 Constructor & Destructor Documentation	40
3.26.2.1 RSAGenerateButton()	40
3.26.3 Member Function Documentation	41
3.26.3.1 collectPassword()	41

3.26.3.2 generateRSA()	41
3.26.3.3 printLog()	41
3.26.3.4 selectPath()	42
3.27 org.example.keyRSA.functions.RSAGeneratorFunction Class Reference	42
3.27.1 Detailed Description	42
3.27.2 Constructor & Destructor Documentation	42
3.27.2.1 RSAGeneratorFunction()	42
3.28 org.example.keyRSA.service.api.RSAService Interface Reference	43
3.28.1 Detailed Description	43
3.28.2 Member Function Documentation	43
3.28.2.1 createKeys()	43
3.28.2.2 encryptPrivateKey()	43
3.28.2.3 getPublicKey()	45
3.29 org.example.keyRSA.service.impl.RSAServiceDefault Class Reference	45
3.29.1 Detailed Description	46
3.29.2 Member Function Documentation	46
3.29.2.1 createKeys()	46
3.29.2.2 encryptPrivateKey()	46
3.29.2.3 getPublicKey()	46
3.30 org.example.app.buttons.api.ShowRSAKeys Interface Reference	47
3.30.1 Detailed Description	47
3.30.2 Member Function Documentation	47
3.30.2.1 collectPassword()	47
3.30.2.2 getKeyPair()	48
3.30.2.3 selectPrivateKeyPath()	49
3.30.2.4 selectPublicKeyPath()	49
3.31 org.example.app.buttons.impl.ShowRSAKeysButton Class Reference	49
3.31.1 Detailed Description	50
3.31.2 Constructor & Destructor Documentation	50
3.31.2.1 ShowRSAKeysButton()	50
3.31.3 Member Function Documentation	50
3.31.3.1 collectPassword()	50
3.31.3.2 getKeyPair()	50
3.31.3.3 printLog()	51
3.31.3.4 selectPrivateKeyPath()	51
3.31.3.5 selectPublicKeyPath()	51
3.32 org.example.app.buttons.api.SignFile Interface Reference	52
3.32.1 Detailed Description	52
3.32.2 Member Function Documentation	52
3.32.2.1 collectPassword()	52
3.32.2.2 selectPrivateKeyPath()	52
3.32.2.3 selectPublicKeyPath()	53

3.32.2.4 selectSignedFilePath()	53
3.32.2.5 signFile()	53
3.33 org.example.app.buttons.impl.SignFileButton Class Reference	54
3.33.1 Detailed Description	54
3.33.2 Constructor & Destructor Documentation	54
3.33.2.1 SignFileButton()	54
3.33.3 Member Function Documentation	54
3.33.3.1 collectPassword()	54
3.33.3.2 printLog()	55
3.33.3.3 selectPrivateKeyPath()	55
3.33.3.4 selectPublicKeyPath()	55
3.33.3.5 selectSignedFilePath()	55
3.33.3.6 signFile()	56
3.34 org.example.signXAdES.service.api.SignService Interface Reference	56
3.34.1 Detailed Description	56
3.34.2 Member Function Documentation	57
3.34.2.1 signXAdES()	57
3.34.2.2 validate()	57
3.35 org.example.signXAdES.service.impl.SignServiceDefault Class Reference	57
3.35.1 Detailed Description	58
3.35.2 Member Function Documentation	58
3.35.2.1 signXAdES()	58
3.35.2.2 validate()	58
3.36 org.example.app.buttons.api.ValidateRSAKeys Interface Reference	59
3.36.1 Detailed Description	59
3.36.2 Member Function Documentation	59
3.36.2.1 validateKeys()	59
3.37 org.example.app.buttons.impl.ValidateRSAKeysButton Class Reference	60
3.37.1 Detailed Description	60
3.37.2 Constructor & Destructor Documentation	60
3.37.2.1 ValidateRSAKeysButton()	60
3.37.3 Member Function Documentation	61
3.37.3.1 actionPerformed()	61
3.37.3.2 validateKeys()	61
3.38 org.example.app.buttons.api.ValidateSignFile Interface Reference	61
3.38.1 Detailed Description	62
3.38.2 Member Function Documentation	62
3.38.2.1 selectSignedFilePath()	62
3.38.2.2 validateSign()	62
3.39 org.example.app.buttons.impl.ValidateSignFileButton Class Reference	63
3.39.1 Detailed Description	63
3.39.2 Constructor & Destructor Documentation	63

3.39.2.1 ValidateSignFileButton()	63
3.39.3 Member Function Documentation	63
3.39.3.1 printLog()	63
3.39.3.2 selectSignedFilePath()	64
3.39.3.3 validateSign()	64
3.40 org.example.signXAdES.functions.XAdESsignFunction Class Reference	64
3.40.1 Detailed Description	65
3.40.2 Constructor & Destructor Documentation	65
3.40.2.1 XAdESsignFunction()	65
3.40.3 Member Function Documentation	65
3.40.3.1 getSignFile()	65
3.40.3.2 signEnveloped()	65
3.41 org.example.signXAdES.functions.XAdESValidatorFunction Class Reference	66
3.41.1 Detailed Description	66
3.41.2 Constructor & Destructor Documentation	66
3.41.2.1 XAdESValidatorFunction()	66
3.41.3 Member Function Documentation	66
3.41.3.1 getValidate()	66
<b>Index</b>	<b>67</b>



# Chapter 1

## Hierarchical Index

### 1.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

org.example.controller.impl.AppController . . . . .	5
org.example.app.buttons.api.DecryptFile . . . . .	9
org.example.app.buttons.impl.DecryptFileButton . . . . .	10
org.example.app.buttons.api.EncryptFile . . . . .	12
org.example.app.buttons.impl.EncryptFileButton . . . . .	14
org.example.file.funions.EncryptingDecryptingFileFunction . . . . .	16
org.example.file.data.api.FileLoader . . . . .	17
org.example.file.data.impl.FileLoaderDefault . . . . .	19
org.example.file.service.api.FileSecurityService . . . . .	21
org.example.file.service.impl.FileSecurityServiceDefault . . . . .	22
org.example.file.service.api.FileService . . . . .	24
org.example.file.service.impl.FileServiceDefault . . . . .	26
JButton	
org.example.app.buttons.impl.DecryptFileButton . . . . .	10
org.example.app.buttons.impl.EncryptFileButton . . . . .	14
org.example.app.buttons.impl.RSAGenerateButton . . . . .	40
org.example.app.buttons.impl.ShowRSAKeysButton . . . . .	49
org.example.app.buttons.impl.ValidateRSAKeysButton . . . . .	60
org.example.app.buttons.impl.SignFileButton . . . . .	54
org.example.app.buttons.impl.ValidateSignFileButton . . . . .	63
JFrame	
org.example.app.mainPanel.impl.Panel . . . . .	35
JPanel	
org.example.app.textFields.impl.PasswordInputComponent . . . . .	36
JTextArea	
org.example.app.textFields.impl.LogsFieldComponent . . . . .	32
org.example.keyRSA.data.api.KeyLoader . . . . .	28
org.example.keyRSA.data.impl.KeyLoaderDefault . . . . .	29
org.example.misc.Logger . . . . .	30
org.example.app.buttons.impl.DecryptFileButton . . . . .	10
org.example.app.buttons.impl.EncryptFileButton . . . . .	14
org.example.app.buttons.impl.RSAGenerateButton . . . . .	40
org.example.app.buttons.impl.ShowRSAKeysButton . . . . .	49

org.example.app.buttons.impl.SignFileButton . . . . .	54
org.example.app.buttons.impl.ValidateRSAKeysButton . . . . .	60
org.example.app.buttons.impl.ValidateSignFileButton . . . . .	63
org.example.Main . . . . .	33
org.example.app.mainPanel.api.MainPanel . . . . .	34
org.example.app.mainPanel.impl.Panel . . . . .	35
org.example.app.textFields.api.PasswordInput . . . . .	36
org.example.app.textFields.impl.PasswordInputComponent . . . . .	36
org.example.keyRSA.functions.PrivateKeyDecryptorFunction . . . . .	37
org.example.keyRSA.functions.PublicKeyDecryptorFunction . . . . .	38
org.example.app.buttons.api.RSAGenerate . . . . .	39
org.example.app.buttons.impl.RSAGenerateButton . . . . .	40
org.example.keyRSA.functions.RSAGeneratorFunction . . . . .	42
org.example.keyRSA.service.api.RSAService . . . . .	43
org.example.keyRSA.service.impl.RSAServiceDefault . . . . .	45
org.example.app.buttons.api.ShowRSAKeys . . . . .	47
org.example.app.buttons.api.ValidateRSAKeys . . . . .	59
org.example.app.buttons.impl.ValidateRSAKeysButton . . . . .	60
org.example.app.buttons.impl.ShowRSAKeysButton . . . . .	49
org.example.app.buttons.api.SignFile . . . . .	52
org.example.app.buttons.impl.SignFileButton . . . . .	54
org.example.signXAdES.service.api.SignService . . . . .	56
org.example.signXAdES.service.impl.SignServiceDefault . . . . .	57
org.example.app.buttons.api.ValidateSignFile . . . . .	61
org.example.app.buttons.impl.ValidateSignFileButton . . . . .	63
org.example.signXAdES.functions.XAdESsignFunction . . . . .	64
org.example.signXAdES.functions.XadESValidatorFunction . . . . .	66
ActionListener	
org.example.app.buttons.impl.DecryptFileButton . . . . .	10
org.example.app.buttons.impl.EncryptFileButton . . . . .	14
org.example.app.buttons.impl.RSAGenerateButton . . . . .	40
org.example.app.buttons.impl.ShowRSAKeysButton . . . . .	49
org.example.app.buttons.impl.SignFileButton . . . . .	54
org.example.app.buttons.impl.ValidateRSAKeysButton . . . . .	60
org.example.app.buttons.impl.ValidateSignFileButton . . . . .	63
PropertyChangeListener	
org.example.app.textFields.api.LogsField . . . . .	31
org.example.app.textFields.impl.LogsFieldComponent . . . . .	32



## Chapter 2

# Class Index

### 2.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

org.example.controller.impl.AppController	5
org.example.app.buttons.api.DecryptFile	9
org.example.app.buttons.impl.DecryptFileButton	10
org.example.app.buttons.api.EncryptFile	12
org.example.app.buttons.impl.EncryptFileButton	14
org.example.file.funtions.EncryptingDecryptingFileFunction	16
org.example.file.data.api.FileLoader	17
org.example.file.data.impl.FileLoaderDefault	19
org.example.file.service.api.FileSecurityService	21
org.example.file.service.impl.FileSecurityServiceDefault	22
org.example.file.service.api.FileService	24
org.example.file.service.impl.FileServiceDefault	26
org.example.keyRSA.data.api.KeyLoader	28
org.example.keyRSA.data.impl.KeyLoaderDefault	29
org.example.misc.Logger	30
org.example.app.textFields.api.LogsField	31
org.example.app.textFields.impl.LogsFieldComponent	32
org.example.Main	33
org.example.app.mainPanel.api.MainPanel	34
org.example.app.mainPanel.impl.Panel	35
org.example.app.textFields.api.PasswordInput	36
org.example.app.textFields.impl.PasswordInputComponent	36
org.example.keyRSA.functions.PrivateKeyDecryptorFunction	37
org.example.keyRSA.functions.PublicKeyDecryptorFunction	38
org.example.app.buttons.api.RSAGenerate	39
org.example.app.buttons.impl.RSAGenerateButton	40
org.example.keyRSA.functions.RSAGeneratorFunction	42
org.example.keyRSA.service.api.RSAService	43
org.example.keyRSA.service.impl.RSAServiceDefault	45
org.example.app.buttons.api.ShowRSAKeys	47
org.example.app.buttons.impl.ShowRSAKeysButton	49
org.example.app.buttons.api.SignFile	52
org.example.app.buttons.impl.SignFileButton	54
org.example.signXAdES.service.api.SignService	56
org.example.signXAdES.service.impl.SignServiceDefault	57

<a href="#">org.example.app.buttons.api.ValidateRSAKeys</a>	59
<a href="#">org.example.app.buttons.impl.ValidateRSAKeysButton</a>	60
<a href="#">org.example.app.buttons.api.ValidateSignFile</a>	61
<a href="#">org.example.app.buttons.impl.ValidateSignFileButton</a>	63
<a href="#">org.example.signXAdES.functions.XAdESsignFunction</a>	64
<a href="#">org.example.signXAdES.functions.XAdESValidatorFunction</a>	66

## Chapter 3

# Class Documentation

### 3.1 org.example.controller.impl.AppController Class Reference

#### Static Public Member Functions

- static void [setRSAKeys](#) (String path, String password)
- static PrivateKey [getPrivateKey](#) (String privateKeyPath, String password)
- static PublicKey [getPublicKey](#) (String publicKeyPath)
- static void [signFile](#) (String privateKeyPath, String publicKeyPath, String signedFilePath, String password)
- static boolean [validateFile](#) (String signedFilePath)
- static void [encryptFile](#) (String privateKeyPath, String password, String filePath)
- static void [decryptFile](#) (String publicKeyPath, String filePath)
- static void [saveFile](#) (String filePath, byte[] data)
- static byte[] [loadFile](#) (String filePath)
- static boolean [deleteFile](#) (String filePath)
- static BasicFileAttributes [getFileAttribute](#) (String filePath)

#### 3.1.1 Detailed Description

Klasa kontrolera aplikacji

#### 3.1.2 Member Function Documentation

##### 3.1.2.1 decryptFile()

```
static void org.example.controller.impl.AppController.decryptFile (  
    String publicKeyPath,  
    String filePath ) [static]
```

Odszyfrowuje wybrany plik.

#### Parameters

<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
<i>filePath</i>	Ścieżka do pliku, który chcemy odszyfrować.

### 3.1.2.2 deleteFile()

```
static boolean org.example.controller.impl.AppController.deleteFile (  
    String filePath ) [static]
```

Usuwa wybrany plik.

#### Parameters

<i>filePath</i>	Ścieżka do pliku, który usuwamy.
-----------------	----------------------------------

#### Returns

Zawartość true, jeżeli plik został usunięty.

### 3.1.2.3 encryptFile()

```
static void org.example.controller.impl.AppController.encryptFile (  
    String privateKeyPath,  
    String password,  
    String filePath ) [static]
```

Szyfruje wybrany plik.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.
<i>filePath</i>	Ścieżka do pliku, który chcemy zaszyfrować.

### 3.1.2.4 getFileAttribute()

```
static BasicFileAttributes org.example.controller.impl.AppController.getFileAttribute (  
    String filePath ) [static]
```

Pobiera podstawowe metadane wybranego pliku.

#### Parameters

<i>filePath</i>	Ścieżka do pliku, z którego odczytujemy metadane.
-----------------	---

#### Returns

Zwraca podstawowe atrybuty pliku.

### 3.1.2.5 getPrivateKey()

```
static PrivateKey org.example.controller.impl.AppController.getPrivateKey (  

```

```
String privateKeyPath,  
String password ) [static]
```

Pobiera klucz prywatny.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

#### Returns

Zwraca klucz prywatny.

### 3.1.2.6 getPublicKey()

```
static PublicKey org.example.controller.impl.AppController.getPublicKey (  
String publicKeyPath ) [static]
```

Pobiera klucz publiczny.

#### Parameters

<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
----------------------	--

#### Returns

Zwraca klucz publiczny.

### 3.1.2.7 loadFile()

```
static byte[] org.example.controller.impl.AppController.loadFile (  
String filePath ) [static]
```

Wczytuje wybrany plik.

#### Parameters

<i>filePath</i>	Ścieżka do pliku, który odczytujemy.
-----------------	--------------------------------------

#### Returns

Zawartość załadowanego pliku

### 3.1.2.8 saveFile()

```
static void org.example.controller.impl.AppController.saveFile (  

```

```
String filePath,
byte[] data ) [static]
```

Zapisuje dane w wybranej lokalizacji.

#### Parameters

<i>filePath</i>	Ścieżka, w której zapisujemy plik.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

### 3.1.2.9 setRSAKeys()

```
static void org.example.controller.impl.AppController.setRSAKeys (
    String path,
    String password ) [static]
```

Tworzy i zapisuje klucz prywatny i publiczny w wybranej lokalizacji.

#### Parameters

<i>path</i>	Ścieżka do folderu zapisu kluczy.
<i>password</i>	Hasło do zaszyfrowania klucza prywatnego.

### 3.1.2.10 signFile()

```
static void org.example.controller.impl.AppController.signFile (
    String privateKeyPath,
    String publicKeyPath,
    String signedFilePath,
    String password ) [static]
```

Podpisuje wybrany plik.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

### 3.1.2.11 validateFile()

```
static boolean org.example.controller.impl.AppController.validateFile (
    String signedFilePath ) [static]
```

Sprawdza poprawność wybranego podpisu. Podpis musi znajdować się w tym samym folderze co podpisany plik.

## Parameters

<i>signedFilePath</i>	Ścieżka do pliku z podpisem.
-----------------------	------------------------------

## Returns

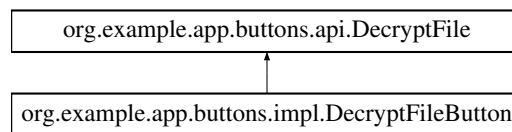
Zwraca true, jeżeli plik i podpis są poprawne.

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/controller/impl/AppController.java

## 3.2 org.example.app.buttons.api.DecryptFile Interface Reference

Inheritance diagram for org.example.app.buttons.api.DecryptFile:



## Public Member Functions

- String [selectFilePath](#) ()
- String [selectPublicKeyPath](#) ()
- void [decryptFile](#) (String publicKeyPath, String filePath)

### 3.2.1 Detailed Description

Interfejs opisujący działanie komponentu do deszyfrowania pliku

### 3.2.2 Member Function Documentation

#### 3.2.2.1 decryptFile()

```

void org.example.app.buttons.api.DecryptFile.decryptFile (
    String publicKeyPath,
    String filePath )
  
```

Funkcja odszyfrująca plik przy pomocy algorytmu RSA, na podstawie wybranego klucza publicznego.

## Parameters

<i>publicKeyPath</i>	Ścieżka do położenia klucza publicznego.
<i>filePath</i>	Ścieżka do pliku, który chcemy zaszyfrować.

Implemented in [org.example.app.buttons.impl.DecryptFileButton](#).

**3.2.2.2 selectFilePath()**

```
String org.example.app.buttons.api.DecryptFile.selectFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do zaszyfrowania.

## Returns

Ścieżka do pliku, który chcemy zaszyfrować.

Implemented in [org.example.app.buttons.impl.DecryptFileButton](#).

**3.2.2.3 selectPublicKeyPath()**

```
String org.example.app.buttons.api.DecryptFile.selectPublicKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza publicznego.

## Returns

Ścieżka do klucza publicznego.

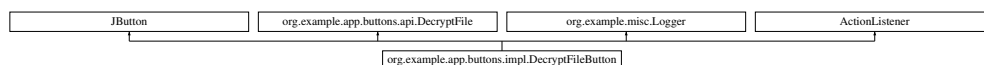
Implemented in [org.example.app.buttons.impl.DecryptFileButton](#).

The documentation for this interface was generated from the following file:

- `C:/Users/kubix23/IdeaProjects/Security_of_Computer_Systems-Project/src/main/java/org/example/app/buttons/api/DecryptFile.java`

**3.3 org.example.app.buttons.impl.DecryptFileButton Class Reference**

Inheritance diagram for `org.example.app.buttons.impl.DecryptFileButton`:





## Public Member Functions

- [DecryptFileButton](#) (PropertyChangeListener... listener)
- void **actionPerformed** (ActionEvent e)
- String [selectFilePath](#) ()
- String [selectPublicKeyPath](#) ()
- void [decryptFile](#) (String publicKeyPath, String filePath)
- void [printLog](#) (String text)

### 3.3.1 Detailed Description

Klasa opisująca działanie przycisku do deszyfrowania pliku

### 3.3.2 Constructor & Destructor Documentation

#### 3.3.2.1 DecryptFileButton()

```
org.example.app.buttons.impl.DecryptFileButton.DecryptFileButton (
    PropertyChangeListener... listener )
```

Konstruktor przycisku do deszyfrowania pliku.

#### Parameters

<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.
-----------------	--

### 3.3.3 Member Function Documentation

#### 3.3.3.1 decryptFile()

```
void org.example.app.buttons.impl.DecryptFileButton.decryptFile (
    String publicKeyPath,
    String filePath )
```

Funkcja odszyfrująca plik przy pomocy algorytmu RSA, na podstawie wybranego klucza publicznego.

#### Parameters

<i>publicKeyPath</i>	Ścieżka do położenia klucza publicznego.
<i>filePath</i>	Ścieżka do pliku, który chcemy zaszyfrować.

Implements [org.example.app.buttons.api.DecryptFile](#).

#### 3.3.3.2 printLog()

```
void org.example.app.buttons.impl.DecryptFileButton.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

#### Parameters

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

Implements [org.example.misc.Logger](#).

#### 3.3.3.3 selectFilePath()

```
String org.example.app.buttons.impl.DecryptFileButton.selectFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do zaszyfrowania.

#### Returns

Ścieżka do pliku, który chcemy zaszyfrować.

Implements [org.example.app.buttons.api.DecryptFile](#).

#### 3.3.3.4 selectPublicKeyPath()

```
String org.example.app.buttons.impl.DecryptFileButton.selectPublicKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza publicznego.

#### Returns

Ścieżka do klucza publicznego.

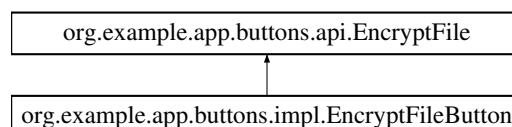
Implements [org.example.app.buttons.api.DecryptFile](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/impl/DecryptFileButton.java

## 3.4 org.example.app.buttons.api.EncryptFile Interface Reference

Inheritance diagram for `org.example.app.buttons.api.EncryptFile`:



## Public Member Functions

- String [selectFilePath](#) ()
- String [selectPrivateKeyPath](#) ()
- String [collectPassword](#) ()
- void [encryptFile](#) (String privateKeyPath, String password, String filePath)

### 3.4.1 Detailed Description

Interfejs opisujący działanie komponentu do szyfrowania pliku

### 3.4.2 Member Function Documentation

#### 3.4.2.1 collectPassword()

```
String org.example.app.buttons.api.EncryptFile.collectPassword ( )
```

Funkcja pobierająca hasło z komponentu [PasswordInput](#).

#### Returns

Wpisane hasło.

Implemented in [org.example.app.buttons.impl.EncryptFileButton](#).

#### 3.4.2.2 encryptFile()

```
void org.example.app.buttons.api.EncryptFile.encryptFile (
    String privateKeyPath,
    String password,
    String filePath )
```

Funkcja szyfrująca plik przy pomocy algorytmu RSA, na podstawie wybranego klucza prywatnego.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do położenia klucza prywatnego.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.
<i>filePath</i>	Ścieżka do pliku, który chcemy odszyfrować.

Implemented in [org.example.app.buttons.impl.EncryptFileButton](#).

#### 3.4.2.3 selectFilePath()

```
String org.example.app.buttons.api.EncryptFile.selectFilePath ( )
```

Funkcja wywołująca okienko dialogowe [JFileChooser](#) do wyboru lokalizacji pliku do odszyfrowania.

**Returns**

Ścieżka do pliku, który chcemy odszyfrować.

Implemented in [org.example.app.buttons.impl.EncryptFileButton](#).

**3.4.2.4 selectPrivateKeyPath()**

```
String org.example.app.buttons.api.EncryptFile.selectPrivateKeyPath ( )
```

Funkcja wywołująca okienko dialogowe JFileChooser do wyboru lokalizacji klucza prywatnego.

**Returns**

Ścieżka do klucza prywatnego.

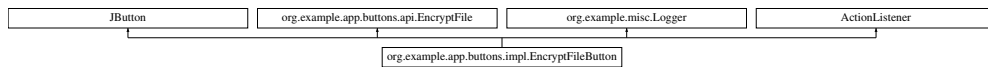
Implemented in [org.example.app.buttons.impl.EncryptFileButton](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/api/EncryptFile.java

**3.5 org.example.app.buttons.impl.EncryptFileButton Class Reference**

Inheritance diagram for org.example.app.buttons.impl.EncryptFileButton:

**Public Member Functions**

- [EncryptFileButton](#) ([PasswordInput](#) passwordComponent, PropertyChangeListener... listener)
- void **actionPerformed** (ActionEvent e)
- String [selectFilePath](#) ()
- String [selectPrivateKeyPath](#) ()
- String [collectPassword](#) ()
- void [encryptFile](#) (String privateKeyPath, String password, String filePath)
- void [printLog](#) (String text)

**3.5.1 Detailed Description**

Klasa opisująca działanie przycisku do szyfrowania pliku

**3.5.2 Constructor & Destructor Documentation****3.5.2.1 EncryptFileButton()**

```
org.example.app.buttons.impl.EncryptFileButton.EncryptFileButton (
    PasswordInput passwordComponent,
    PropertyChangeListener... listener )
```

Konstruktor przycisku do szyfrowania pliku.

## Parameters

<i>passwordComponent</i>	Komponent przechowujący informacje o hasle.
<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.

### 3.5.3 Member Function Documentation

#### 3.5.3.1 collectPassword()

```
String org.example.app.buttons.impl.EncryptFileButton.collectPassword ( )
```

Funkcja pobierające hasło z komponentu [PasswordInput](#).

## Returns

Wpisane hasło.

Implements [org.example.app.buttons.api.EncryptFile](#).

#### 3.5.3.2 encryptFile()

```
void org.example.app.buttons.impl.EncryptFileButton.encryptFile (
    String privateKeyPath,
    String password,
    String filePath )
```

Funkcja szyfrująca plik przy pomocy algorytmu RSA, na podstawie wybranego klucza prywatnego.

## Parameters

<i>privateKeyPath</i>	Ścieżka do położenia klucza prywatnego.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.
<i>filePath</i>	Ścieżka do pliku, który chcemy odszyfrować.

Implements [org.example.app.buttons.api.EncryptFile](#).

#### 3.5.3.3 printLog()

```
void org.example.app.buttons.impl.EncryptFileButton.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

## Parameters

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

Implements [org.example.misc.Logger](#).

#### 3.5.3.4 selectFilePath()

```
String org.example.app.buttons.impl.EncryptFileButton.selectFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do odszyfrowania.

##### Returns

Ścieżka do pliku, który chcemy odszyfrować.

Implements [org.example.app.buttons.api.EncryptFile](#).

#### 3.5.3.5 selectPrivateKeyPath()

```
String org.example.app.buttons.impl.EncryptFileButton.selectPrivateKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza prywatnego.

##### Returns

Ścieżka do klucza prywatnego.

Implements [org.example.app.buttons.api.EncryptFile](#).

The documentation for this class was generated from the following file:

- `C:/Users/kubix23/IdeaProjects/Security_of_Computer_Systems-Project/src/main/java/org/example/app/buttons/impl/EncryptFileButton.java`

## 3.6 org.example.file.funtions.EncryptingDecryptingFileFunction Class Reference

### Public Member Functions

- `byte[] EncryptingFile (PrivateKey privateKey, byte[] fileIn) throws NoSuchPaddingException, NoSuchAlgorithmException, InvalidKeyException, IllegalBlockSizeException, BadPaddingException`
- `byte[] DencryptingFile (PublicKey publicKey, byte[] fileIn) throws Exception`

### 3.6.1 Detailed Description

Klasa implementująca podstawowe operacje szyfrowania i deszyfrowania pliku.

### 3.6.2 Member Function Documentation

#### 3.6.2.1 DencryptingFile()

```
byte[] org.example.file.funtions.EncryptingDecryptingFileFunction.DencryptingFile (
    PublicKey publicKey,
    byte[] fileIn ) throws Exception
```

Odszyfrujemy wybrany plik.

## Parameters

<i>publicKey</i>	Klucz prywatny, którym odszyfujemy dane.
<i>fileIn</i>	Zawartość, jaką chcemy odszyfować.

## Returns

Odszyfowana zawartość.

## 3.6.2.2 EncryptingFile()

```
byte[] org.example.file.funtions.EncryptingDecryptingFileFunction.EncryptingFile (
    PrivateKey privateKey,
    byte[] fileIn ) throws NoSuchPaddingException, NoSuchAlgorithmException, InvalidKeyException,
    IllegalBlockSizeException, BadPaddingException
```

Szyfruje wybrane dane.

## Parameters

<i>privateKey</i>	Klucz prywatny, którym szyfrujemy dane.
<i>fileIn</i>	Zawartość, jaką chcemy zaszyfować.

## Returns

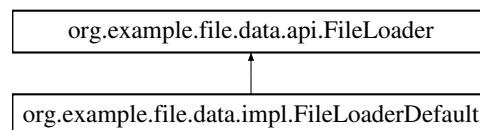
Zaszyfowana zawartość.

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/funtions/EncryptingDecryptingFileFunction.java

## 3.7 org.example.file.data.api.FileLoader Interface Reference

Inheritance diagram for org.example.file.data.api.FileLoader:



## Public Member Functions

- void [saveFile](#) (String path, byte[] data)
- BasicFileAttributes [getFileAttribute](#) (String path) throws IOException
- byte[] [loadFile](#) (String path) throws IOException
- boolean [deleteFile](#) (String path) throws IOException

### 3.7.1 Detailed Description

Interfejs dostępu do plików.

### 3.7.2 Member Function Documentation

#### 3.7.2.1 deleteFile()

```
boolean org.example.file.data.api.FileLoader.deleteFile (  
    String path ) throws IOException
```

Usuwa wybrany plik.

##### Parameters

<i>path</i>	Ścieżka do pliku, który usuwamy.
-------------	----------------------------------

##### Returns

Zawartość true, jeżeli plik został usunięty.

Implemented in [org.example.file.data.impl.FileLoaderDefault](#).

#### 3.7.2.2 getFileAttribute()

```
BasicFileAttributes org.example.file.data.api.FileLoader.getFileAttribute (  
    String path ) throws IOException
```

Pobiera podstawowe metadane wybranego pliku.

##### Parameters

<i>path</i>	Ścieżka do pliku, z którego odczytujemy metadane.
-------------	---

##### Returns

Zwraca podstawowe atrybuty pliku.

Implemented in [org.example.file.data.impl.FileLoaderDefault](#).

#### 3.7.2.3 loadFile()

```
byte[] org.example.file.data.api.FileLoader.loadFile (  
    String path ) throws IOException
```

Wczytuje wybrany plik.



## Parameters

<i>path</i>	Ścieżka do pliku, który odczytujemy.
-------------	--------------------------------------

## Returns

Zawartość załadowanego pliku

Implemented in [org.example.file.data.impl.FileLoaderDefault](#).

**3.7.2.4 saveFile()**

```
void org.example.file.data.api.FileLoader.saveFile (
    String path,
    byte[] data )
```

Zapisuje dane w wybranej lokalizacji.

## Parameters

<i>path</i>	Ścieżka, w której zapisujemy plik.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

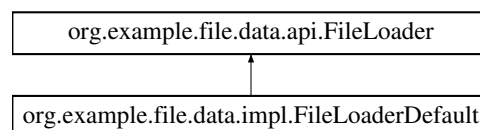
Implemented in [org.example.file.data.impl.FileLoaderDefault](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/data/api/FileLoader.java

**3.8 org.example.file.data.impl.FileLoaderDefault Class Reference**

Inheritance diagram for org.example.file.data.impl.FileLoaderDefault:

**Public Member Functions**

- void [saveFile](#) (String path, byte[] data)
- BasicFileAttributes [getFileAttribute](#) (String path) throws IOException
- byte[] [loadFile](#) (String path) throws IOException
- boolean [deleteFile](#) (String path) throws IOException

### 3.8.1 Detailed Description

Klasa odpowiedzialna za dostęp do plików.

### 3.8.2 Member Function Documentation

#### 3.8.2.1 deleteFile()

```
boolean org.example.file.data.impl.FileLoaderDefault.deleteFile (
    String path ) throws IOException
```

Usuwa wybrany plik.

##### Parameters

<i>path</i>	Ścieżka do pliku, który usuwamy.
-------------	----------------------------------

##### Returns

Zawartość true, jeżeli plik został usunięty.

Implements [org.example.file.data.api.FileLoader](#).

#### 3.8.2.2 getFileAttribute()

```
BasicFileAttributes org.example.file.data.impl.FileLoaderDefault.getFileAttribute (
    String path ) throws IOException
```

Pobiera podstawowe metadane wybranego pliku.

##### Parameters

<i>path</i>	Ścieżka do pliku, z którego odczytujemy metadane.
-------------	---

##### Returns

Zwraca podstawowe atrybuty pliku.

Implements [org.example.file.data.api.FileLoader](#).

#### 3.8.2.3 loadFile()

```
byte[] org.example.file.data.impl.FileLoaderDefault.loadFile (
    String path ) throws IOException
```

Wczytuje wybrany plik.

## Parameters

<i>path</i>	Ścieżka do pliku, który odczytujemy.
-------------	--------------------------------------

## Returns

Zawartość załadowanego pliku

Implements [org.example.file.data.api.FileLoader](#).

**3.8.2.4 saveFile()**

```
void org.example.file.data.impl.FileLoaderDefault.saveFile (
    String path,
    byte[] data )
```

Zapisuje dane w wybranej lokalizacji.

## Parameters

<i>path</i>	Ścieżka, w której zapisujemy plik.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

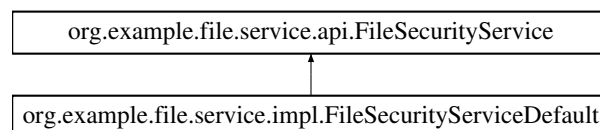
Implements [org.example.file.data.api.FileLoader](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/data/impl/FileLoaderDefault.java

**3.9 org.example.file.service.api.FileSecurityService Interface Reference**

Inheritance diagram for org.example.file.service.api.FileSecurityService:

**Public Member Functions**

- void [encrypt](#) (String privateKeyPath, String password, String filePath)
- void [decrypt](#) (String publicKeyPath, String filePath)

### 3.9.1 Detailed Description

Interfejs z podstawowymi operacjami szyfrowania i deszyfrowania pliku.

### 3.9.2 Member Function Documentation

#### 3.9.2.1 decrypte()

```
void org.example.file.service.api.FileSecurityService.decrypte (
    String publicKeyPath,
    String filePath )
```

Odszyfrowuje wybrany plik.

##### Parameters

<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
<i>filePath</i>	Ścieżka do pliku, który chcemy odszyfrować.

Implemented in [org.example.file.service.impl.FileSecurityServiceDefault](#).

#### 3.9.2.2 encrypte()

```
void org.example.file.service.api.FileSecurityService.encrypte (
    String privateKeyPath,
    String password,
    String filePath )
```

Szyfruje wybrany plik.

##### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.
<i>filePath</i>	Ścieżka do pliku, który chcemy zaszyfrować.

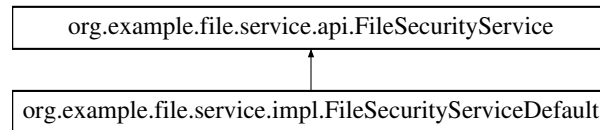
Implemented in [org.example.file.service.impl.FileSecurityServiceDefault](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/service/api/FileSecurityService.java

## 3.10 org.example.file.service.impl.FileSecurityServiceDefault Class Reference

Inheritance diagram for org.example.file.service.impl.FileSecurityServiceDefault:



### Public Member Functions

- void [encrypt](#) (String privateKeyPath, String password, String filePath)
- void [decrypt](#) (String publicKeyPath, String filePath)

### 3.10.1 Detailed Description

Klasa wywołująca podstawowe operacje szyfrowania i deszyfrowania pliku.

### 3.10.2 Member Function Documentation

#### 3.10.2.1 [decrypte\(\)](#)

```
void org.example.file.service.impl.FileSecurityServiceDefault.decrypte (
    String publicKeyPath,
    String filePath )
```

Odszyfrowuje wybrany plik.

#### Parameters

<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
<i>filePath</i>	Ścieżka do pliku, który chcemy odszyfrować.

Implements [org.example.file.service.api.FileSecurityService](#).

#### 3.10.2.2 [encrypte\(\)](#)

```
void org.example.file.service.impl.FileSecurityServiceDefault.encrypte (
    String privateKeyPath,
    String password,
    String filePath )
```

Szyfruje wybrany plik.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.
<i>filePath</i>	Ścieżka do pliku, który chcemy zaszyfrować.

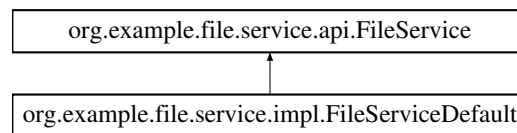
Implements [org.example.file.service.api.FileSecurityService](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/service/impl/FileSecurityServiceDefault.java

### 3.11 org.example.file.service.api.FileService Interface Reference

Inheritance diagram for org.example.file.service.api.FileService:



#### Public Member Functions

- byte[] [load](#) (String path)
- void [save](#) (String path, byte[] data)
- BasicFileAttributes [getFileAttribute](#) (String path)
- boolean [delete](#) (String path)

#### 3.11.1 Detailed Description

Interfejs serwisu odpowiedzialny za przekazanie plików.

#### 3.11.2 Member Function Documentation

##### 3.11.2.1 delete()

```
boolean org.example.file.service.api.FileService.delete (
    String path )
```

Usuwa wybrany plik.

#### Parameters

<i>path</i>	Ścieżka do pliku, który usuwamy.
-------------	----------------------------------

#### Returns

Zawartość true, jeżeli plik został usunięty.

Implemented in [org.example.file.service.impl.FileServiceDefault](#).

### 3.11.2.2 getFileAttribute()

```
BasicFileAttributes org.example.file.service.api.FileService.getFileAttribute (
    String path )
```

Pobiera podstawowe metadane wybranego pliku.

#### Parameters

<i>path</i>	Ścieżka do pliku, z którego odczytujemy metadane.
-------------	---

#### Returns

Zwraca podstawowe atrybuty pliku.

Implemented in [org.example.file.service.impl.FileServiceDefault](#).

### 3.11.2.3 load()

```
byte[] org.example.file.service.api.FileService.load (
    String path )
```

Wczytuje wybrany plik.

#### Parameters

<i>path</i>	Ścieżka do pliku, który odczytujemy.
-------------	--------------------------------------

#### Returns

Zawartość załadowanego pliku

Implemented in [org.example.file.service.impl.FileServiceDefault](#).

### 3.11.2.4 save()

```
void org.example.file.service.api.FileService.save (
    String path,
    byte[] data )
```

Zapisuje dane w wybranej lokalizacji.

#### Parameters

<i>path</i>	Ścieżka, w której zapisujemy plik.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

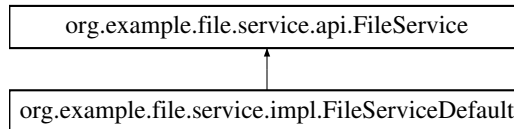
Implemented in [org.example.file.service.impl.FileServiceDefault](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/service/api/FileService.java

## 3.12 org.example.file.service.impl.FileServiceDefault Class Reference

Inheritance diagram for org.example.file.service.impl.FileServiceDefault:



### Public Member Functions

- byte[] [load](#) (String path)
- void [save](#) (String path, byte[] data)
- BasicFileAttributes [getFileAttribute](#) (String path)
- boolean [delete](#) (String path)

### 3.12.1 Detailed Description

Klasa serwisu odpowiedzialna za przekazanie plików.

### 3.12.2 Member Function Documentation

#### 3.12.2.1 delete()

```
boolean org.example.file.service.impl.FileServiceDefault.delete (
    String path )
```

Usuwa wybrany plik.

#### Parameters

<i>path</i>	Ścieżka do pliku, który usuwamy.
-------------	----------------------------------

#### Returns

Zawartość true, jeżeli plik został usunięty.

Implements [org.example.file.service.api.FileService](#).



### 3.12.2.2 getFileAttribute()

```
BasicFileAttributes org.example.file.service.impl.FileServiceDefault.getFileAttribute (
    String path )
```

Pobiera podstawowe metadane wybranego pliku.

#### Parameters

<i>path</i>	Ścieżka do pliku, z którego odczytujemy metadane.
-------------	---

#### Returns

Zwraca podstawowe atrybuty pliku.

Implements [org.example.file.service.api.FileService](#).

### 3.12.2.3 load()

```
byte[] org.example.file.service.impl.FileServiceDefault.load (
    String path )
```

Wczytuje wybrany plik.

#### Parameters

<i>path</i>	Ścieżka do pliku, który odczytujemy.
-------------	--------------------------------------

#### Returns

Zawartość załadowanego pliku

Implements [org.example.file.service.api.FileService](#).

### 3.12.2.4 save()

```
void org.example.file.service.impl.FileServiceDefault.save (
    String path,
    byte[] data )
```

Zapisuje dane w wybranej lokalizacji.

#### Parameters

<i>path</i>	Ścieżka, w której zapisujemy plik.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

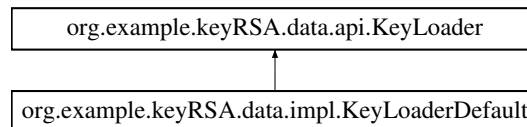
Implements [org.example.file.service.api.FileService](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/file/service/impl/File↔ServiceDefault.java

### 3.13 org.example.keyRSA.data.api.KeyLoader Interface Reference

Inheritance diagram for org.example.keyRSA.data.api.KeyLoader:



#### Public Member Functions

- void [saveKey](#) (String path, byte[] data)
- byte[] [loadKey](#) (String path) throws IOException

#### 3.13.1 Detailed Description

Interfejs dostępu do kluczy.

#### 3.13.2 Member Function Documentation

##### 3.13.2.1 loadKey()

```
byte[] org.example.keyRSA.data.api.KeyLoader.loadKey (
    String path ) throws IOException
```

Wczytuje wybrany klucz.

#### Parameters

<i>path</i>	Ścieżka do klucza, który odczytujemy.
-------------	---------------------------------------

#### Returns

Dane wybranego klucza.

Implemented in [org.example.keyRSA.data.impl.KeyLoaderDefault](#).

### 3.13.2.2 saveKey()

```
void org.example.keyRSA.data.api.KeyLoader.saveKey (
    String path,
    byte[] data )
```

Zapisuje klucz w wybranej lokalizacji.

#### Parameters

<i>path</i>	Ścieżka, w której zapisujemy klucz.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

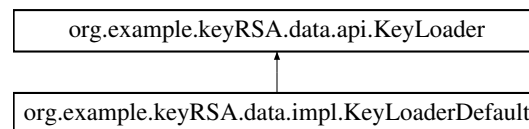
Implemented in [org.example.keyRSA.data.impl.KeyLoaderDefault](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/key↔RSA/data/api/KeyLoader.java

## 3.14 org.example.keyRSA.data.impl.KeyLoaderDefault Class Reference

Inheritance diagram for org.example.keyRSA.data.impl.KeyLoaderDefault:



#### Public Member Functions

- void [saveKey](#) (String path, byte[] data)
- byte[] [loadKey](#) (String path) throws IOException

### 3.14.1 Detailed Description

Klasa odpowiedzialna za dostęp do kluczy.

### 3.14.2 Member Function Documentation

#### 3.14.2.1 loadKey()

```
byte[] org.example.keyRSA.data.impl.KeyLoaderDefault.loadKey (
    String path ) throws IOException
```

Wczytuje wybrany klucz.

## Parameters

<i>path</i>	Ścieżka do klucza, który odczytujemy.
-------------	---------------------------------------

## Returns

Dane wybranego klucza.

Implements [org.example.keyRSA.data.api.KeyLoader](#).

**3.14.2.2 saveKey()**

```
void org.example.keyRSA.data.impl.KeyLoaderDefault.saveKey (
    String path,
    byte[] data )
```

Zapisuje klucz w wybranej lokalizacji.

## Parameters

<i>path</i>	Ścieżka, w której zapisujemy klucz.
<i>data</i>	Tablica bajtów, które chcemy zapisać.

Implements [org.example.keyRSA.data.api.KeyLoader](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/keyRSA/data/impl/KeyLoaderDefault.java

**3.15 org.example.misc.Logger Interface Reference**

Inheritance diagram for org.example.misc.Logger:

**Public Member Functions**

- void [printLog](#) (String text)

**3.15.1 Detailed Description**

Interfejs opisujący działanie funkcji rejestrującej wiadomości w komponencie do tego przeznaczonym.

## 3.15.2 Member Function Documentation

### 3.15.2.1 printLog()

```
void org.example.misc.Logger.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

#### Parameters

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

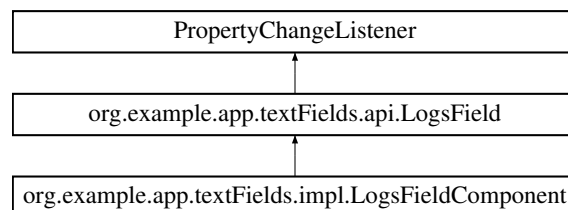
Implemented in [org.example.app.buttons.impl.DecryptFileButton](#), [org.example.app.buttons.impl.EncryptFileButton](#), [org.example.app.buttons.impl.RSAGenerateButton](#), [org.example.app.buttons.impl.ShowRSAKeysButton](#), [org.example.app.buttons.im](#) and [org.example.app.buttons.impl.ValidateSignFileButton](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/misc/Logger.↔  
java

## 3.16 org.example.app.textFields.api.LogsField Interface Reference

Inheritance diagram for org.example.app.textFields.api.LogsField:



#### Public Member Functions

- void [clear](#) ()
- void [print](#) (String text)

### 3.16.1 Detailed Description

Interfejs opisujący działanie komponentu wyświetlającego postępy aplikacji

### 3.16.2 Member Function Documentation

#### 3.16.2.1 clear()

```
void org.example.app.textFields.api.LogsField.clear ( )
```

Funkcja czyszcząca wyświetlany tekst

Implemented in [org.example.app.textFields.impl.LogsFieldComponent](#).

#### 3.16.2.2 print()

```
void org.example.app.textFields.api.LogsField.print (
    String text )
```

Funkcja wyświetla podany napis.

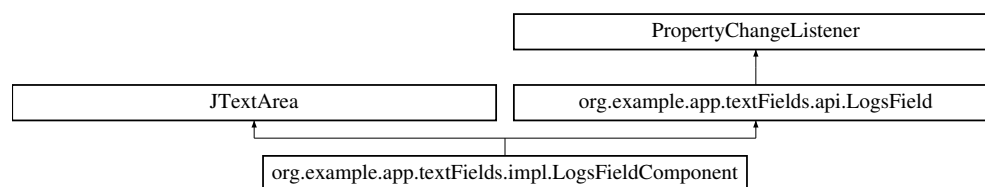
Implemented in [org.example.app.textFields.impl.LogsFieldComponent](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/textFields/api/LogsField.java

## 3.17 org.example.app.textFields.impl.LogsFieldComponent Class Reference

Inheritance diagram for org.example.app.textFields.impl.LogsFieldComponent:



#### Public Member Functions

- [LogsFieldComponent](#) ()
- void [clear](#) ()
- void [print](#) (String text)
- void **propertyChange** (PropertyChangeEvent evt)

#### 3.17.1 Detailed Description

Klasa opisująca działanie pola tekstowego wyświetlającego postępy aplikacji

## 3.17.2 Constructor & Destructor Documentation

### 3.17.2.1 LogsFieldComponent()

```
org.example.app.textFields.impl.LogsFieldComponent.LogsFieldComponent ( )
```

Konstruktor pola tekstowego do wyświetlania informacji

## 3.17.3 Member Function Documentation

### 3.17.3.1 clear()

```
void org.example.app.textFields.impl.LogsFieldComponent.clear ( )
```

Funkcja czyszcząca wyświetlany tekst

Implements [org.example.app.textFields.api.LogsField](#).

### 3.17.3.2 print()

```
void org.example.app.textFields.impl.LogsFieldComponent.print (
    String text )
```

Funkcja wyświetla podany napis.

Implements [org.example.app.textFields.api.LogsField](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/textFields/impl/LogsFieldComponent.java

## 3.18 org.example.Main Class Reference

### Static Public Member Functions

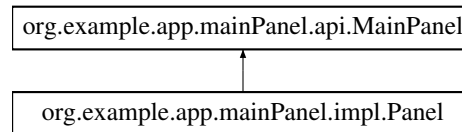
- static void **main** (String[ ] args)

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/Main.java

## 3.19 org.example.app.mainPanel.api.MainPanel Interface Reference

Inheritance diagram for org.example.app.mainPanel.api.MainPanel:



### Public Member Functions

- void [config](#) ()
- void [addComponents](#) ()

### 3.19.1 Detailed Description

Interfejs opisujący działanie głównego panelu aplikacji.

### 3.19.2 Member Function Documentation

#### 3.19.2.1 addComponents()

```
void org.example.app.mainPanel.api.MainPanel.addComponents ( )
```

Funkcja, w której dodawane są komponenty do głównego panelu.

Implemented in [org.example.app.mainPanel.impl.Panel](#).

#### 3.19.2.2 config()

```
void org.example.app.mainPanel.api.MainPanel.config ( )
```

Funkcja, w której ustawiane są opcje głównego panelu.

Implemented in [org.example.app.mainPanel.impl.Panel](#).

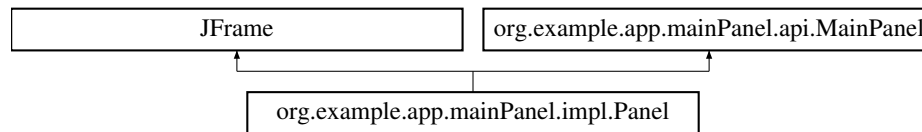
The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/mainPanel/api/MainPanel.java



## 3.20 org.example.app.mainPanel.impl.Panel Class Reference

Inheritance diagram for org.example.app.mainPanel.impl.Panel:



### Public Member Functions

- [Panel](#) () throws `HeadlessException`
- void [config](#) ()
- void [addComponents](#) ()

### 3.20.1 Detailed Description

Klasa głównego panelu aplikacji.

### 3.20.2 Constructor & Destructor Documentation

#### 3.20.2.1 Panel()

`org.example.app.mainPanel.impl.Panel.Panel ( ) throws HeadlessException`

Konstruktor głównej aplikacji

### 3.20.3 Member Function Documentation

#### 3.20.3.1 addComponents()

`void org.example.app.mainPanel.impl.Panel.addComponents ( )`

Funkcja, w której dodawane są komponenty do głównego panelu.

Implements [org.example.app.mainPanel.api.MainPanel](#).

#### 3.20.3.2 config()

`void org.example.app.mainPanel.impl.Panel.config ( )`

Funkcja, w której ustawiane są opcje głównego panelu.

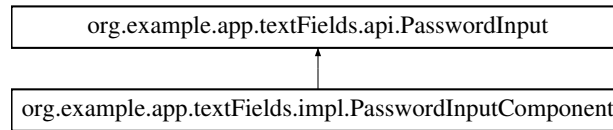
Implements [org.example.app.mainPanel.api.MainPanel](#).

The documentation for this class was generated from the following file:

- `C:/Users/kubix23/IdeaProjects/Security_of_Computer_Systems-Project/src/main/java/org/example/app/mainPanel/impl/Panel.java`

## 3.21 org.example.app.textFields.api.PasswordInput Interface Reference

Inheritance diagram for org.example.app.textFields.api.PasswordInput:



### Public Member Functions

- String [getPassword](#) ()

### 3.21.1 Detailed Description

Interfejs opisująca działanie komponentu wprowadzania hasła.

### 3.21.2 Member Function Documentation

#### 3.21.2.1 getPassword()

String org.example.app.textFields.api.PasswordInput.getPassword ( )

Pobranie wprowadzonego hasła.

#### Returns

Wpisane hasło.

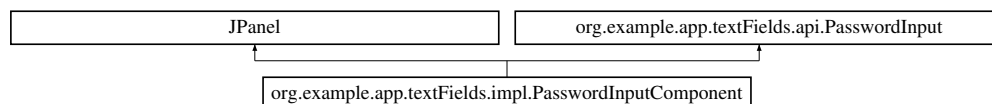
Implemented in [org.example.app.textFields.impl.PasswordInputComponent](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/textFields/api/PasswordInput.java

## 3.22 org.example.app.textFields.impl.PasswordInputComponent Class Reference

Inheritance diagram for org.example.app.textFields.impl.PasswordInputComponent:



**Public Member Functions**

- [PasswordInputComponent](#) ()
- String [getPassword](#) ()

**3.22.1 Detailed Description**

Klasa opisująca działanie panelu, który zawiera pole tekstowe do wprowadzania hasła i etykietę do tego pola.

**3.22.2 Constructor & Destructor Documentation****3.22.2.1 PasswordInputComponent()**

```
org.example.app.textFields.impl.PasswordInputComponent.PasswordInputComponent ( )
```

Konstruktor pola tekstowego do wprowadzania hasła

**3.22.3 Member Function Documentation****3.22.3.1 getPassword()**

```
String org.example.app.textFields.impl.PasswordInputComponent.getPassword ( )
```

Pobranie wprowadzonego hasła.

**Returns**

Wpisane hasło.

Implements [org.example.app.textFields.api.PasswordInput](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/textFields/impl/PasswordInputComponent.java

**3.23 org.example.keyRSA.functions.PrivateKeyDecryptorFunction Class Reference****Public Member Functions**

- [PrivateKeyDecryptorFunction](#) (String password, byte[] privateKeyAESByte)
- PrivateKey [getPr](#) ()

**3.23.1 Detailed Description**

Klasa implementująca funkcję deszyfrującą klucz prywatny.

**3.23.2 Constructor & Destructor Documentation****3.23.2.1 PrivateKeyDecryptorFunction()**

```
org.example.keyRSA.functions.PrivateKeyDecryptorFunction.PrivateKeyDecryptorFunction (
    String password,
    byte[] privateKeyAESByte )
```

Konstruktor odpowiedzialny za odszyfrowanie klucza prywatnego

## Parameters

<i>password</i>	Hasło do odszyfrowania klucza prywatnego.
<i>privateKeyAESByte</i>	Tablica bajtów klucza prywatnego.

### 3.23.3 Member Function Documentation

#### 3.23.3.1 getPr()

```
PrivateKey org.example.keyRSA.functions.PrivateKeyDecryptorFunction.getPr ( )
```

## Returns

Zwraca odszyfrowany klucz prywatny.

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/keyRSA/functions/PrivateKeyDecryptorFunction.java

## 3.24 org.example.keyRSA.functions.PublicKeyDecryptorFunction Class Reference

### Public Member Functions

- [PublicKeyDecryptorFunction](#) (byte[] publicKeyPath)
- PublicKey [getKey](#) ()

#### 3.24.1 Detailed Description

Klasa implementująca funkcję deszyfrującą klucz publiczny.

### 3.24.2 Constructor & Destructor Documentation

#### 3.24.2.1 PublicKeyDecryptorFunction()

```
org.example.keyRSA.functions.PublicKeyDecryptorFunction.PublicKeyDecryptorFunction (
    byte[] publicKeyPath )
```

Konstruktor odpowiedzialny za odszyfrowanie klucza prywatnego

## Parameters

<i>publicKeyPath</i>	Tablica bajtów klucza publicznego.
----------------------	------------------------------------

### 3.24.3 Member Function Documentation

#### 3.24.3.1 getKey()

```
PublicKey org.example.keyRSA.functions.PublicKeyDecryptorFunction.getKey ( )
```

##### Returns

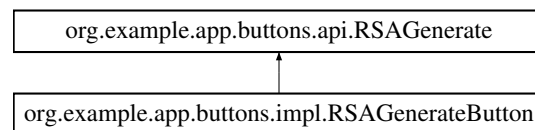
Zwraca odszyfrowany klucz publiczny.

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/keyRSA/functions/PublicKeyDecryptorFunction.java

## 3.25 org.example.app.buttons.api.RSAGenerate Interface Reference

Inheritance diagram for org.example.app.buttons.api.RSAGenerate:



### Public Member Functions

- String [selectPath](#) ()
- String [collectPassword](#) ()
- void [generateRSA](#) (String path, String password)

### 3.25.1 Detailed Description

Interfejs opisujący działanie komponentu do generowania pary kluczy RSA

### 3.25.2 Member Function Documentation

#### 3.25.2.1 collectPassword()

```
String org.example.app.buttons.api.RSAGenerate.collectPassword ( )
```

Funkcja pobierająca hasło z komponentu [PasswordInput](#).

##### Returns

Wpisane hasło.

Implemented in [org.example.app.buttons.impl.RSAGenerateButton](#).

#### 3.25.2.2 generateRSA()

```
void org.example.app.buttons.api.RSAGenerate.generateRSA (
    String path,
    String password )
```

Funkcja tworząca parę kluczy private.key i public.key w wybranej lokalizacji.

## Parameters

<i>path</i>	Ścieżka do położenia pary kluczy.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

Implemented in [org.example.app.buttons.impl.RSAGenerateButton](#).

### 3.25.2.3 selectPath()

```
String org.example.app.buttons.api.RSAGenerate.selectPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do odszyfrowania.

## Returns

Ścieżka do folderu, w którym chcemy zapisać klucze.

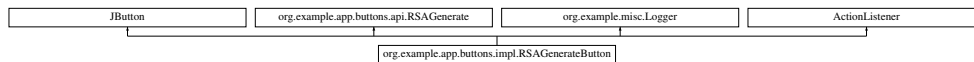
Implemented in [org.example.app.buttons.impl.RSAGenerateButton](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/api/RSAGener: java

## 3.26 org.example.app.buttons.impl.RSAGenerateButton Class Reference

Inheritance diagram for `org.example.app.buttons.impl.RSAGenerateButton`:



## Public Member Functions

- [RSAGenerateButton](#) ([PasswordInput](#) passwordComponent, [PropertyChangeListener](#)... listener)
- void [actionPerformed](#) ([ActionEvent](#) e)
- String [selectPath](#) ()
- String [collectPassword](#) ()
- void [generateRSA](#) (String path, String password)
- void [printLog](#) (String text)

### 3.26.1 Detailed Description

Klasa opisująca działanie przycisku do generowania pary kluczy RSA

### 3.26.2 Constructor & Destructor Documentation

#### 3.26.2.1 RSAGenerateButton()

```
org.example.app.buttons.impl.RSAGenerateButton.RSAGenerateButton (
    PasswordInput passwordComponent,
    PropertyChangeListener... listener )
```

Konstruktor przycisku do generowania kluczy.

## Parameters

<i>passwordComponent</i>	Komponent przechowujący informacje o hasle.
<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.

### 3.26.3 Member Function Documentation

#### 3.26.3.1 collectPassword()

```
String org.example.app.buttons.impl.RSAGenerateButton.collectPassword ( )
```

Funkcja pobierające hasło z komponentu [PasswordInput](#).

## Returns

Wpisane hasło.

Implements [org.example.app.buttons.api.RSAGenerate](#).

#### 3.26.3.2 generateRSA()

```
void org.example.app.buttons.impl.RSAGenerateButton.generateRSA (
    String path,
    String password )
```

Funkcja tworząca parę kluczy private.key i public.key w wybranej lokalizacji.

## Parameters

<i>path</i>	Ścieżka do położenia pary kluczy.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

Implements [org.example.app.buttons.api.RSAGenerate](#).

#### 3.26.3.3 printLog()

```
void org.example.app.buttons.impl.RSAGenerateButton.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

## Parameters

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

Implements [org.example.misc.Logger](#).

### 3.26.3.4 selectPath()

```
String org.example.app.buttons.impl.RSAGenerateButton.selectPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do odszyfrowania.

#### Returns

Ścieżka do folderu, w którym chcemy zapisać klucze.

Implements [org.example.app.buttons.api.RSAGenerate](#).

The documentation for this class was generated from the following file:

- `C:/Users/kubix23/IdeaProjects/Security_of_Computer_Systems-Project/src/main/java/org/example/app/buttons/impl/RSAGenerateButton.java`

## 3.27 org.example.keyRSA.functions.RSAGeneratorFunction Class Reference

### Public Member Functions

- [RSAGeneratorFunction](#) (String password)
- `byte[] getPublicKey ()`
- `byte[] getPrivateKey ()`

### 3.27.1 Detailed Description

Klasa implementująca funkcję tworzącą klucz publiczny i prywatny.

### 3.27.2 Constructor & Destructor Documentation

#### 3.27.2.1 RSAGeneratorFunction()

```
org.example.keyRSA.functions.RSAGeneratorFunction.RSAGeneratorFunction (
    String password )
```

Konstruktor odpowiedzialny za wygenerowanie klucza publicznego i prywatnego, następnie za zaszyfrowanie klucza prywatnego.

#### Parameters

<i>password</i>	Hasło do zaszyfrowania klucza prywatnego.
-----------------	---

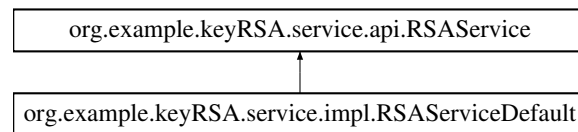
The documentation for this class was generated from the following file:



- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/keyRSA/functions/RSAgeneratorFunction.java

## 3.28 org.example.keyRSA.service.api.RSAService Interface Reference

Inheritance diagram for org.example.keyRSA.service.api.RSAService:



### Public Member Functions

- void [createKeys](#) (String pathSave, String password)
- PublicKey [getPublicKey](#) (String publicKeyPath)
- PrivateKey [encryptPrivateKey](#) (String privateKeyPath, String password)

### 3.28.1 Detailed Description

Interfejs serwisu odpowiedzialny za klucze.

### 3.28.2 Member Function Documentation

#### 3.28.2.1 createKeys()

```
void org.example.keyRSA.service.api.RSAService.createKeys (
    String pathSave,
    String password )
```

Tworzy i zapisuje klucz prywatny i publiczny w wybranej lokalizacji.

#### Parameters

<i>pathSave</i>	Ścieżka do folderu zapisu kluczy.
<i>password</i>	Hasło do zaszyfrowania klucza prywatnego.

Implemented in [org.example.keyRSA.service.impl.RSAServiceDefault](#).

#### 3.28.2.2 encryptPrivateKey()

```
PrivateKey org.example.keyRSA.service.api.RSAService.encryptPrivateKey (
    String privateKeyPath,
    String password )
```

Pobiera klucz prywatny.

## Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

## Returns

Zwraca klucz prywatny.

Implemented in [org.example.keyRSA.service.impl.RSAServiceDefault](#).

**3.28.2.3 getPublicKey()**

```
PublicKey org.example.keyRSA.service.api.RSAService.getPublicKey (
    String publicKeyPath )
```

Pobiera klucz publiczny.

## Parameters

<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
----------------------	--

## Returns

Zwraca klucz publiczny.

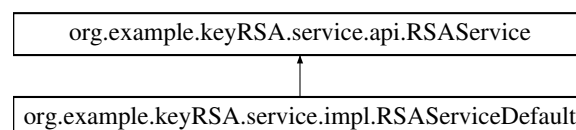
Implemented in [org.example.keyRSA.service.impl.RSAServiceDefault](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/keyRSA/service/api/RSAService.java

**3.29 org.example.keyRSA.service.impl.RSAServiceDefault Class Reference**

Inheritance diagram for org.example.keyRSA.service.impl.RSAServiceDefault:

**Public Member Functions**

- void [createKeys](#) (String pathSave, String password)
- PublicKey [getPublicKey](#) (String publicKeyPath)
- PrivateKey [encryptPrivateKey](#) (String privateKeyPath, String password)

### 3.29.1 Detailed Description

Klasa serwisu odpowiedzialny za zarządzanie kluczami.

### 3.29.2 Member Function Documentation

#### 3.29.2.1 createKeys()

```
void org.example.keyRSA.service.impl.RSAServiceDefault.createKeys (
    String pathSave,
    String password )
```

Tworzy i zapisuje klucz prywatny i publiczny w wybranej lokalizacji.

##### Parameters

<i>pathSave</i>	Ścieżka do folderu zapisu kluczy.
<i>password</i>	Hasło do zaszyfrowania klucza prywatnego.

Implements [org.example.keyRSA.service.api.RSAService](#).

#### 3.29.2.2 encryptPrivateKey()

```
PrivateKey org.example.keyRSA.service.impl.RSAServiceDefault.encryptPrivateKey (
    String privateKeyPath,
    String password )
```

Pobiera klucz prywatny.

##### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

##### Returns

Zwraca klucz prywatny.

Implements [org.example.keyRSA.service.api.RSAService](#).

#### 3.29.2.3 getPublicKey()

```
PublicKey org.example.keyRSA.service.impl.RSAServiceDefault.getPublicKey (
    String publicKeyPath )
```

Pobiera klucz publiczny.

## Parameters

<code>publicKeyPath</code>	Ścieżka do pliku z kluczem publicznym.
----------------------------	--

## Returns

Zwraca klucz publiczny.

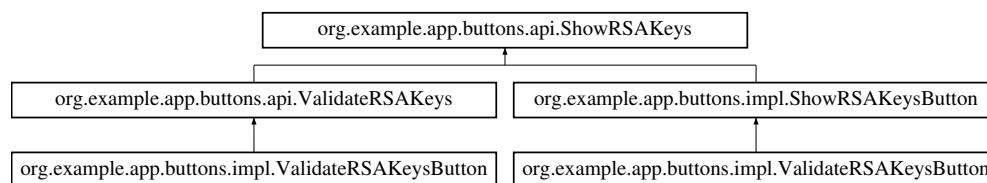
Implements [org.example.keyRSA.service.api.RSAService](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/keyRSA/service/impl/RSAServiceDefault.java

## 3.30 org.example.app.buttons.api.ShowRSAKeys Interface Reference

Inheritance diagram for org.example.app.buttons.api.ShowRSAKeys:



## Public Member Functions

- String [selectPrivateKeyPath](#) ()
- String [selectPublicKeyPath](#) ()
- KeyPair [getKeyPair](#) (String privateKeyPath, String publicKeyPath, String password)
- String [collectPassword](#) ()

### 3.30.1 Detailed Description

Interfejs opisująca działanie komponentu do wyświetlenia pary kluczy RSA

### 3.30.2 Member Function Documentation

#### 3.30.2.1 collectPassword()

```
String org.example.app.buttons.api.ShowRSAKeys.collectPassword ( )
```

Funkcja pobierające hasło z komponentu [PasswordInput](#).

## Returns

Wpisane hasło.

Implemented in [org.example.app.buttons.impl.ShowRSAKeysButton](#).

### 3.30.2.2 getKeyPair()

```
KeyPair org.example.app.buttons.api.ShowRSAKeys.getKeyPair (
    String privateKeyPath,
    String publicKeyPath,
    String password )
```

## Parameters

<i>privateKeyPath</i>	Ścieżka do położenia klucza prywatnego.
<i>publicKeyPath</i>	Ścieżka do położenia klucza publicznego.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

## Returns

Para kluczy prywatny i publiczny.

Implemented in [org.example.app.buttons.impl.ShowRSAKeysButton](#).

**3.30.2.3 selectPrivateKeyPath()**

```
String org.example.app.buttons.api.ShowRSAKeys.selectPrivateKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza prywatnego.

## Returns

Ścieżka do klucza prywatnego.

Implemented in [org.example.app.buttons.impl.ShowRSAKeysButton](#).

**3.30.2.4 selectPublicKeyPath()**

```
String org.example.app.buttons.api.ShowRSAKeys.selectPublicKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza publicznego.

## Returns

Ścieżka do klucza publicznego.

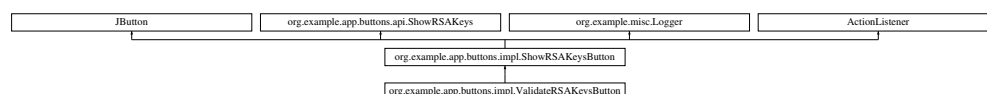
Implemented in [org.example.app.buttons.impl.ShowRSAKeysButton](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/api/ShowRSAKeys.java

**3.31 org.example.app.buttons.impl.ShowRSAKeysButton Class Reference**

Inheritance diagram for `org.example.app.buttons.impl.ShowRSAKeysButton`:



## Public Member Functions

- [ShowRSAKeysButton](#) ([PasswordInput](#) passwordComponent, [PropertyChangeListener...](#) listener)
- **ShowRSAKeysButton** ([PasswordInput](#) passwordComponent)
- void **actionPerformed** ([ActionEvent](#) e)
- String [selectPrivateKeyPath](#) ()
- String [selectPublicKeyPath](#) ()
- [KeyPair](#) [getKeyPair](#) (String privateKeyPath, String publicKeyPath, String password)
- String [collectPassword](#) ()
- void [printLog](#) (String text)

### 3.31.1 Detailed Description

Klasa opisująca działanie przycisku do wyświetlenia pary kluczy RSA

### 3.31.2 Constructor & Destructor Documentation

#### 3.31.2.1 ShowRSAKeysButton()

```
org.example.app.buttons.impl.ShowRSAKeysButton.ShowRSAKeysButton (
    PasswordInput passwordComponent,
    PropertyChangeListener... listener )
```

Konstruktor przycisku do wyświetlenia kluczy.

#### Parameters

<i>passwordComponent</i>	Komponent przechowujący informacje o hasle.
<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.

### 3.31.3 Member Function Documentation

#### 3.31.3.1 collectPassword()

```
String org.example.app.buttons.impl.ShowRSAKeysButton.collectPassword ( )
```

Funkcja pobierające hasło z komponentu [PasswordInput](#).

#### Returns

Wpisane hasło.

Implements [org.example.app.buttons.api.ShowRSAKeys](#).

#### 3.31.3.2 getKeyPair()

```
KeyPair org.example.app.buttons.impl.ShowRSAKeysButton.getKeyPair (
    String privateKeyPath,
    String publicKeyPath,
    String password )
```



## Parameters

<i>privateKeyPath</i>	Ścieżka do położenia klucza prywatnego.
<i>publicKeyPath</i>	Ścieżka do położenia klucza publicznego.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

## Returns

Para kluczy prywatny i publiczny.

Implements [org.example.app.buttons.api.ShowRSAKeys](#).

**3.31.3.3 printLog()**

```
void org.example.app.buttons.impl.ShowRSAKeysButton.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

## Parameters

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

Implements [org.example.misc.Logger](#).

**3.31.3.4 selectPrivateKeyPath()**

```
String org.example.app.buttons.impl.ShowRSAKeysButton.selectPrivateKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza prywatnego.

## Returns

Ścieżka do klucza prywatnego.

Implements [org.example.app.buttons.api.ShowRSAKeys](#).

**3.31.3.5 selectPublicKeyPath()**

```
String org.example.app.buttons.impl.ShowRSAKeysButton.selectPublicKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza publicznego.

## Returns

Ścieżka do klucza publicznego.

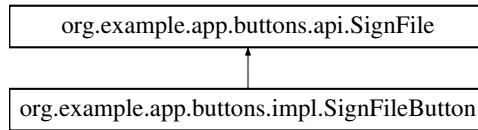
Implements [org.example.app.buttons.api.ShowRSAKeys](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/impl/ShowRSAKeysButton.java

## 3.32 org.example.app.buttons.api.SignFile Interface Reference

Inheritance diagram for org.example.app.buttons.api.SignFile:



### Public Member Functions

- String [selectPrivateKeyPath](#) ()
- String [selectPublicKeyPath](#) ()
- String [selectSignedFilePath](#) ()
- void [signFile](#) (String privateKeyPath, String publicKeyPath, String signedFilePath, String password)
- String [collectPassword](#) ()

### 3.32.1 Detailed Description

Interfejs opisujący działanie komponentu do podpisywania plików.

### 3.32.2 Member Function Documentation

#### 3.32.2.1 collectPassword()

```
String org.example.app.buttons.api.SignFile.collectPassword ( )
```

Funkcja pobierająca hasło z komponentu [PasswordInput](#).

#### Returns

Wpisane hasło.

Implemented in [org.example.app.buttons.impl.SignFileButton](#).

#### 3.32.2.2 selectPrivateKeyPath()

```
String org.example.app.buttons.api.SignFile.selectPrivateKeyPath ( )
```

Funkcja wywołująca okienko dialogowe [JFileChooser](#) do wyboru lokalizacji klucza prywatnego.

#### Returns

Ścieżka do klucza prywatnego.

Implemented in [org.example.app.buttons.impl.SignFileButton](#).

**3.32.2.3 selectPublicKeyPath()**

```
String org.example.app.buttons.api.SignFile.selectPublicKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza publicznego.

**Returns**

Ścieżka do klucza publicznego.

Implemented in [org.example.app.buttons.impl.SignFileButton](#).

**3.32.2.4 selectSignedFilePath()**

```
String org.example.app.buttons.api.SignFile.selectSignedFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do podpisania.

**Returns**

Ścieżka do pliku, który chcemy podpisać.

Implemented in [org.example.app.buttons.impl.SignFileButton](#).

**3.32.2.5 signFile()**

```
void org.example.app.buttons.api.SignFile.signFile (
    String privateKeyPath,
    String publicKeyPath,
    String signedFilePath,
    String password )
```

Funkcja tworząca podpis w formacie XAdES.

**Parameters**

<i>privateKeyPath</i>	Ścieżka do położenia klucza prywatnego.
<i>publicKeyPath</i>	Ścieżka do położenia klucza publicznego.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

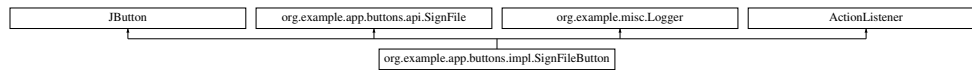
Implemented in [org.example.app.buttons.impl.SignFileButton](#).

The documentation for this interface was generated from the following file:

- `C:/Users/kubix23/IdeaProjects/Security_of_Computer_Systems-Project/src/main/java/org/example/app/buttons/api/SignFile.java`

### 3.33 org.example.app.buttons.impl.SignFileButton Class Reference

Inheritance diagram for org.example.app.buttons.impl.SignFileButton:



#### Public Member Functions

- [SignFileButton](#) ([PasswordInput](#) passwordComponent, [PropertyChangeListener](#)... listener)
- void **actionPerformed** ([ActionEvent](#) e)
- String [selectPrivateKeyPath](#) ()
- String [selectPublicKeyPath](#) ()
- String [selectSignedFilePath](#) ()
- void [signFile](#) (String privateKeyPath, String publicKeyPath, String signedFilePath, String password)
- String [collectPassword](#) ()
- void [printLog](#) (String text)

#### 3.33.1 Detailed Description

Klasa opisująca działanie przycisku do podpisywania plików.

#### 3.33.2 Constructor & Destructor Documentation

##### 3.33.2.1 SignFileButton()

```
org.example.app.buttons.impl.SignFileButton.SignFileButton (
    PasswordInput passwordComponent,
    PropertyChangeListener... listener )
```

Konstruktor przycisku do podpisywania plików.

##### Parameters

<i>passwordComponent</i>	Komponent przechowujący informacje o hasle.
<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.

#### 3.33.3 Member Function Documentation

##### 3.33.3.1 collectPassword()

```
String org.example.app.buttons.impl.SignFileButton.collectPassword ( )
```

Funkcja pobierające hasło z komponentu [PasswordInput](#).

**Returns**

Wpisane hasło.

Implements [org.example.app.buttons.api.SignFile](#).

**3.33.3.2 printLog()**

```
void org.example.app.buttons.impl.SignFileButton.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

**Parameters**

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

Implements [org.example.misc.Logger](#).

**3.33.3.3 selectPrivateKeyPath()**

```
String org.example.app.buttons.impl.SignFileButton.selectPrivateKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza prywatnego.

**Returns**

Ścieżka do klucza prywatnego.

Implements [org.example.app.buttons.api.SignFile](#).

**3.33.3.4 selectPublicKeyPath()**

```
String org.example.app.buttons.impl.SignFileButton.selectPublicKeyPath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji klucza publicznego.

**Returns**

Ścieżka do klucza publicznego.

Implements [org.example.app.buttons.api.SignFile](#).

**3.33.3.5 selectSignedFilePath()**

```
String org.example.app.buttons.impl.SignFileButton.selectSignedFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do podpisania.

**Returns**

Ścieżka do pliku, który chcemy podpisać.

Implements [org.example.app.buttons.api.SignFile](#).

### 3.33.3.6 signFile()

```
void org.example.app.buttons.impl.SignFileButton.signFile (
    String privateKeyPath,
    String publicKeyPath,
    String signedFilePath,
    String password )
```

Funkcja tworząca podpis w formacie XAdES.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do położenia klucza prywatnego.
<i>publicKeyPath</i>	Ścieżka do położenia klucza publicznego.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

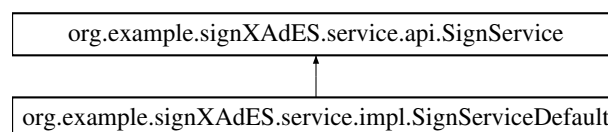
Implements [org.example.app.buttons.api.SignFile](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/impl/SignFileButton.java

## 3.34 org.example.signXAdES.service.api.SignService Interface Reference

Inheritance diagram for org.example.signXAdES.service.api.SignService:



### Public Member Functions

- void [signXAdES](#) (String privateKeyPath, String publicKeyPath, String signedFilePath, String password)
- boolean [validate](#) (String signedFilePath)

### 3.34.1 Detailed Description

Interfejs serwisu odpowiedzialny za podpis w formacie XAdES.

## 3.34.2 Member Function Documentation

### 3.34.2.1 signXAdES()

```
void org.example.signXAdES.service.api.SignService.signXAdES (
    String privateKeyPath,
    String publicKeyPath,
    String signedFilePath,
    String password )
```

Podpisuje wybrany plik.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

Implemented in [org.example.signXAdES.service.impl.SignServiceDefault](#).

### 3.34.2.2 validate()

```
boolean org.example.signXAdES.service.api.SignService.validate (
    String signedFilePath )
```

Sprawdza poprawność wybranego podpisu. Podpis musi znajdować się w tym samym folderze co podpisany plik.

#### Parameters

<i>signedFilePath</i>	Ścieżka do pliku z podpisem.
-----------------------	------------------------------

#### Returns

Zwraca true, jeżeli plik i podpis są poprawne.

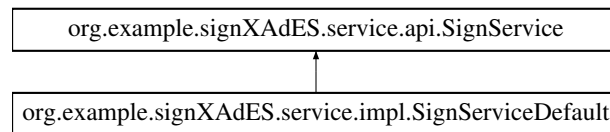
Implemented in [org.example.signXAdES.service.impl.SignServiceDefault](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/signXAdES/service/api/SignService.java

## 3.35 org.example.signXAdES.service.impl.SignServiceDefault Class Reference

Inheritance diagram for org.example.signXAdES.service.impl.SignServiceDefault:



### Public Member Functions

- void [signXAdES](#) (String privateKeyPath, String publicKeyPath, String signedFilePath, String password)
- boolean [validate](#) (String signedFilePath)

### 3.35.1 Detailed Description

Klasa serwisu implementująca zarządzanie podpisami XAdES.

### 3.35.2 Member Function Documentation

#### 3.35.2.1 signXAdES()

```
void org.example.signXAdES.service.impl.SignServiceDefault.signXAdES (
    String privateKeyPath,
    String publicKeyPath,
    String signedFilePath,
    String password )
```

Podpisuje wybrany plik.

#### Parameters

<i>privateKeyPath</i>	Ścieżka do pliku z kluczem prywatnym.
<i>publicKeyPath</i>	Ścieżka do pliku z kluczem publicznym.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>password</i>	Hasło do odszyfrowania klucza prywatnego.

Implements [org.example.signXAdES.service.api.SignService](#).

#### 3.35.2.2 validate()

```
boolean org.example.signXAdES.service.impl.SignServiceDefault.validate (
    String signedFilePath )
```

Sprawdza poprawność wybranego podpisu. Podpis musi znajdować się w tym samym folderze co podpisany plik.

#### Parameters

<i>signedFilePath</i>	Ścieżka do pliku z podpisem.
-----------------------	------------------------------



**Returns**

Zwraca true, jeżeli plik i podpis są poprawne.

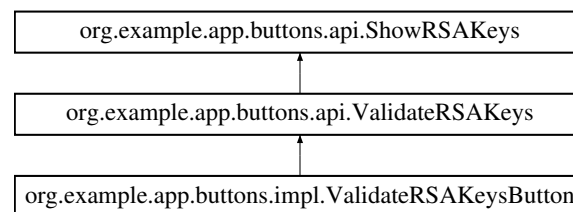
Implements [org.example.signXAdES.service.api.SignService](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/signXAdES/service/impl/SignServiceDefault.java

## 3.36 org.example.app.buttons.api.ValidateRSAKeys Interface Reference

Inheritance diagram for org.example.app.buttons.api.ValidateRSAKeys:

**Public Member Functions**

- boolean [validateKeys](#) (KeyPair keyPair)

### Public Member Functions inherited from [org.example.app.buttons.api.ShowRSAKeys](#)

- String [selectPrivateKeyPath](#) ()
- String [selectPublicKeyPath](#) ()
- KeyPair [getKeyPair](#) (String privateKeyPath, String publicKeyPath, String password)
- String [collectPassword](#) ()

### 3.36.1 Detailed Description

Interfejs opisujący działanie komponentów do sprawdzania poprawności kluczy RSA.

### 3.36.2 Member Function Documentation

#### 3.36.2.1 validateKeys()

```
boolean org.example.app.buttons.api.ValidateRSAKeys.validateKeys (
    KeyPair keyPair )
```

Funkcja sprawdzająca zgodność klucza prywatnego i publicznego.



## Parameters

<i>passwordComponent</i>	Komponent przechowujący informacje o hasle.
<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.

### 3.37.3 Member Function Documentation

#### 3.37.3.1 actionPerformed()

```
void org.example.app.buttons.impl.ValidateRSAKeysButton.actionPerformed (
    ActionEvent e )
```

Reimplemented from [org.example.app.buttons.impl.ShowRSAKeysButton](#).

#### 3.37.3.2 validateKeys()

```
boolean org.example.app.buttons.impl.ValidateRSAKeysButton.validateKeys (
    KeyPair keyPair )
```

Funkcja sprawdzająca zgodność klucza prywatnego i publicznego.

## Parameters

<i>keyPair</i>	Para kluczy publiczny i prywatny.
----------------	-----------------------------------

## Returns

Zwraca true, jeżeli para kluczy jest zgodna?

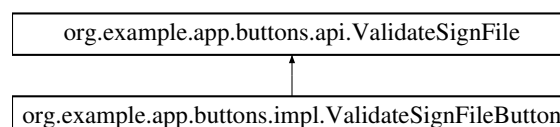
Implements [org.example.app.buttons.api.ValidateRSAKeys](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/impl/ValidateRSAKeysButton.java

## 3.38 org.example.app.buttons.api.ValidateSignFile Interface Reference

Inheritance diagram for org.example.app.buttons.api.ValidateSignFile:



## Public Member Functions

- String [selectSignedFilePath](#) ()
- boolean [validateSign](#) (String signedFilePath)

### 3.38.1 Detailed Description

Interfejs opisujący działanie komponentu do sprawdzania poprawności podpisu i pliku podpisywanego.

### 3.38.2 Member Function Documentation

#### 3.38.2.1 [selectSignedFilePath\(\)](#)

```
String org.example.app.buttons.api.ValidateSignFile.selectSignedFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do podpisania.

#### Returns

Ścieżka do pliku, który chcemy podpisać.

Implemented in [org.example.app.buttons.impl.ValidateSignFileButton](#).

#### 3.38.2.2 [validateSign\(\)](#)

```
boolean org.example.app.buttons.api.ValidateSignFile.validateSign (
    String signedFilePath )
```

Funkcja sprawdzająca poprawność podpisu i pliku. Podpis musi znajdować się w tym samym folderze co podpisany plik

#### Parameters

<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
-----------------------	--

#### Returns

Zwraca true, jeżeli podpis jest poprawny?

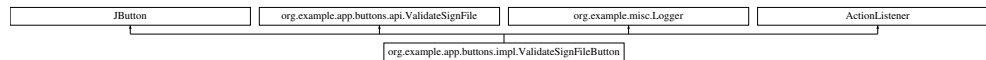
Implemented in [org.example.app.buttons.impl.ValidateSignFileButton](#).

The documentation for this interface was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/api/ValidateSignFile.java

## 3.39 org.example.app.buttons.impl.ValidateSignFileButton Class Reference

Inheritance diagram for org.example.app.buttons.impl.ValidateSignFileButton:



### Public Member Functions

- [ValidateSignFileButton](#) (PropertyChangeListener... listener)
- void **actionPerformed** (ActionEvent e)
- String [selectSignedFilePath](#) ()
- boolean [validateSign](#) (String signedFilePath)
- void [printLog](#) (String text)

### 3.39.1 Detailed Description

Klasa opisująca działanie przycisku do sprawdzania poprawności podpisu i pliku podpisywanego.

### 3.39.2 Constructor & Destructor Documentation

#### 3.39.2.1 ValidateSignFileButton()

```
org.example.app.buttons.impl.ValidateSignFileButton.ValidateSignFileButton (
    PropertyChangeListener... listener )
```

Konstruktor przycisku do sprawdzania poprawności.

#### Parameters

<i>listener</i>	Kolekcja komponentów nasłuchujących akcje.
-----------------	--

### 3.39.3 Member Function Documentation

#### 3.39.3.1 printLog()

```
void org.example.app.buttons.impl.ValidateSignFileButton.printLog (
    String text )
```

Funkcji rejestrującej wiadomości w komponencie.

#### Parameters

<i>text</i>	Tekst wysyłanej wiadomości.
-------------	-----------------------------

Implements [org.example.misc.Logger](#).

### 3.39.3.2 selectSignedFilePath()

```
String org.example.app.buttons.impl.ValidateSignFileButton.selectSignedFilePath ( )
```

Funkcja wywołująca okienko dialogowe `JFileChooser` do wyboru lokalizacji pliku do podpisania.

#### Returns

Ścieżka do pliku, który chcemy podpisać.

Implements [org.example.app.buttons.api.ValidateSignFile](#).

### 3.39.3.3 validateSign()

```
boolean org.example.app.buttons.impl.ValidateSignFileButton.validateSign (
    String signedFilePath )
```

Funkcja sprawdzająca poprawność podpisu i pliku. Podpis musi znajdować się w tym samym folderze co podpisany plik

#### Parameters

<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
-----------------------	--

#### Returns

Zwraca true, jeżeli podpis jest poprawny?

Implements [org.example.app.buttons.api.ValidateSignFile](#).

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/app/buttons/impl/ValidateSignFileButton.java

## 3.40 org.example.signXAdES.functions.XAdESsignFunction Class Reference

### Public Member Functions

- [XAdESsignFunction](#) (PublicKey publicKey, PrivateKey privateKey, String signedFilePath, BasicFileAttributes basicFileAttribute) throws Exception
- byte[] [getSignFile](#) ()
- Document [signEnveloped](#) (Document sign, PrivateKey privateKey, PublicKey publicKey, Path signedFilePath, BasicFileAttributes basicFileAttribute) throws Exception

### 3.40.1 Detailed Description

Klasa implementująca metody tworzące podpis w formacie XAdES.

### 3.40.2 Constructor & Destructor Documentation

#### 3.40.2.1 XAdESsignFunction()

```
org.example.signXAdES.functions.XAdESsignFunction.XAdESsignFunction (
    PublicKey publicKey,
    PrivateKey privateKey,
    String signedFilePath,
    BasicFileAttributes basicFileAttribute ) throws Exception
```

Konstruktor tworzy klasę Dokument, generuje w niej podpis XAdES i zamienia na tablicę bajtów.

##### Parameters

<i>publicKey</i>	Klucz publiczny.
<i>privateKey</i>	Klucz prywatny.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>basicFileAttribute</i>	Zwraca podstawowe atrybuty pliku.

### 3.40.3 Member Function Documentation

#### 3.40.3.1 getSignFile()

```
byte[] org.example.signXAdES.functions.XAdESsignFunction.getSignFile ( )
```

##### Returns

Tablica bajtów podpisu.

#### 3.40.3.2 signEnveloped()

```
Document org.example.signXAdES.functions.XAdESsignFunction.signEnveloped (
    Document sign,
    PrivateKey privateKey,
    PublicKey publicKey,
    Path signedFilePath,
    BasicFileAttributes basicFileAttribute ) throws Exception
```

Funkcja generująca podpis XAdES.

##### Parameters

<i>sign</i>	Klasa reprezentująca Dokument
<i>publicKey</i>	Klucz publiczny.
<i>privateKey</i>	Klucz prywatny.
<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>basicFileAttribute</i>	Zwraca podstawowe atrybuty pliku.

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/signXAdES/functions/XAdESsignFunction.java

### 3.41 org.example.signXAdES.functions.XadESValidatorFunction Class Reference

#### Public Member Functions

- [XadESValidatorFunction](#) (byte[] signedFile, String signedFilePath) throws IOException, SAXException, MarshalException, XMLSignatureException, ParserConfigurationException, NoSuchProviderException
- Boolean [getValidate](#) ()

#### 3.41.1 Detailed Description

Klasa implementująca metody weryfikacji podpisu XAdES.

#### 3.41.2 Constructor & Destructor Documentation

##### 3.41.2.1 XadESValidatorFunction()

```
org.example.signXAdES.functions.XadESValidatorFunction.XadESValidatorFunction (
    byte[] signedFile,
    String signedFilePath ) throws IOException, SAXException, MarshalException, XMLSignatureException,
ParserConfigurationException, NoSuchProviderException
```

Konstruktor tworzy klasę Dokument i sprawdza poprawność podpisu.

#### Parameters

<i>signedFilePath</i>	Ścieżka do pliku, który chcemy podpisać.
<i>signedFile</i>	Tablica bajtów podpisanego pliku.

#### 3.41.3 Member Function Documentation

##### 3.41.3.1 getValidate()

```
Boolean org.example.signXAdES.functions.XadESValidatorFunction.getValidate ( )
```

#### Returns

Zawraca true, jeżeli podpis i plik są zgodne.

The documentation for this class was generated from the following file:

- C:/Users/kubix23/IdeaProjects/Security\_of\_Computer\_Systems-Project/src/main/java/org/example/signXAdES/functions/XadESValidatorFunction.java



# Index

actionPerformed  
    org.example.app.buttons.impl.ValidateRSAKeysButton, 61

addComponents  
    org.example.app.mainPanel.api.MainPanel, 34  
    org.example.app.mainPanel.impl.Panel, 35

clear  
    org.example.app.textFields.api.LogsField, 32  
    org.example.app.textFields.impl.LogsFieldComponent, 33

collectPassword  
    org.example.app.buttons.api.EncryptFile, 13  
    org.example.app.buttons.api.RSAGenerate, 39  
    org.example.app.buttons.api.ShowRSAKeys, 47  
    org.example.app.buttons.api.SignFile, 52  
    org.example.app.buttons.impl.EncryptFileButton, 15  
    org.example.app.buttons.impl.RSAGenerateButton, 41  
    org.example.app.buttons.impl.ShowRSAKeysButton, 50  
    org.example.app.buttons.impl.SignFileButton, 54

config  
    org.example.app.mainPanel.api.MainPanel, 34  
    org.example.app.mainPanel.impl.Panel, 35

createKeys  
    org.example.keyRSA.service.api.RSAService, 43  
    org.example.keyRSA.service.impl.RSAServiceDefault, 46

decrypt  
    org.example.file.service.api.FileSecurityService, 22  
    org.example.file.service.impl.FileSecurityServiceDefault, 23

decryptFile  
    org.example.controller.impl.AppController, 5

decryptFile  
    org.example.app.buttons.api.DecryptFile, 9  
    org.example.app.buttons.impl.DecryptFileButton, 11

DecryptFileButton  
    org.example.app.buttons.impl.DecryptFileButton, 11

delete  
    org.example.file.service.api.FileService, 24  
    org.example.file.service.impl.FileServiceDefault, 26

deleteFile  
    org.example.controller.impl.AppController, 6  
    org.example.file.data.api.FileLoader, 18  
    org.example.file.data.impl.FileLoaderDefault, 20

DecryptingFile  
    org.example.file.funtions.EncryptingDecryptingFileFunction, 16

encrypt  
    org.example.file.service.api.FileSecurityService, 22  
    org.example.file.service.impl.FileSecurityServiceDefault, 23

encryptFile  
    org.example.controller.impl.AppController, 6

encryptFile  
    org.example.app.buttons.api.EncryptFile, 13  
    org.example.app.buttons.impl.EncryptFileButton, 15

EncryptFileButton  
    org.example.app.buttons.impl.EncryptFileButton, 14

EncryptingFile  
    org.example.file.funtions.EncryptingDecryptingFileFunction, 17

encryptPrivateKey  
    org.example.keyRSA.service.api.RSAService, 43  
    org.example.keyRSA.service.impl.RSAServiceDefault, 46

generateRSA  
    org.example.app.buttons.api.RSAGenerate, 39  
    org.example.app.buttons.impl.RSAGenerateButton, 41

getFileAttribute  
    org.example.controller.impl.AppController, 6  
    org.example.file.data.api.FileLoader, 18  
    org.example.file.data.impl.FileLoaderDefault, 20  
    org.example.file.service.api.FileService, 24  
    org.example.file.service.impl.FileServiceDefault, 26

getKey  
    org.example.keyRSA.functions.PublicKeyDecryptorFunction, 39

getKeyPair  
    org.example.app.buttons.api.ShowRSAKeys, 47  
    org.example.app.buttons.impl.ShowRSAKeysButton, 50

getPassword  
    org.example.app.textFields.api.PasswordInput, 36

org.example.app.textFields.impl.PasswordInputComponent, 37  
 getPrivateKey  
   org.example.controller.impl.AppController, 6  
 getPublicKey  
   org.example.controller.impl.AppController, 7  
   org.example.keyRSA.service.api.RSAService, 45  
   org.example.keyRSA.service.impl.RSAServiceDefault, 46  
 getSignFile  
   org.example.signXAdES.functions.XAdESsignFunction, 65  
 getValidate  
   org.example.signXAdES.functions.XAdESValidatorFunction, 66  
 load  
   org.example.file.service.api.FileService, 25  
   org.example.file.service.impl.FileServiceDefault, 27  
 loadFile  
   org.example.controller.impl.AppController, 7  
   org.example.file.data.api.FileLoader, 18  
   org.example.file.data.impl.FileLoaderDefault, 20  
 loadKey  
   org.example.keyRSA.data.api.KeyLoader, 28  
   org.example.keyRSA.data.impl.KeyLoaderDefault, 29  
 LogsFieldComponent  
   org.example.app.textFields.impl.LogsFieldComponent, 33  
 org.example.app.buttons.api.DecryptFile, 9  
   decryptFile, 9  
   selectFilePath, 10  
   selectPublicKeyPath, 10  
 org.example.app.buttons.api.EncryptFile, 12  
   collectPassword, 13  
   encryptFile, 13  
   selectFilePath, 13  
   selectPrivateKeyPath, 14  
 org.example.app.buttons.api.RSAGenerate, 39  
   collectPassword, 39  
   generateRSA, 39  
   selectPath, 40  
 org.example.app.buttons.api.ShowRSAKeys, 47  
   collectPassword, 47  
   getKeyPair, 47  
   selectPrivateKeyPath, 49  
   selectPublicKeyPath, 49  
 org.example.app.buttons.api.SignFile, 52  
   collectPassword, 52  
   selectPrivateKeyPath, 52  
   selectPublicKeyPath, 52  
   selectSignedFilePath, 53  
   signFile, 53  
 org.example.app.buttons.api.ValidateRSAKeys, 59  
   validateKeys, 59  
 org.example.app.buttons.api.ValidateSignFile, 61  
   selectSignedFilePath, 62  
   validateSign, 62  
 org.example.app.buttons.impl.DecryptFileButton, 10  
   decryptFile, 11  
   DecryptFileButton, 11  
   printLog, 11  
   selectFilePath, 12  
   selectPublicKeyPath, 12  
 org.example.app.buttons.impl.EncryptFileButton, 14  
   collectPassword, 15  
   encryptFile, 15  
   EncryptFileButton, 14  
   printLog, 15  
   selectFilePath, 16  
   selectPrivateKeyPath, 16  
 org.example.app.buttons.impl.RSAGenerateButton, 40  
   collectPassword, 41  
   generateRSA, 41  
   printLog, 41  
   RSAGenerateButton, 40  
   selectPath, 41  
 org.example.app.buttons.impl.ShowRSAKeysButton, 49  
   collectPassword, 50  
   getKeyPair, 50  
   printLog, 51  
   selectPrivateKeyPath, 51  
   selectPublicKeyPath, 51  
   ShowRSAKeysButton, 50  
 org.example.app.buttons.impl.SignFileButton, 54  
   collectPassword, 54  
   printLog, 55  
   selectPrivateKeyPath, 55  
   selectPublicKeyPath, 55  
   selectSignedFilePath, 55  
   signFile, 55  
   SignFileButton, 54  
 org.example.app.buttons.impl.ValidateRSAKeysButton, 60  
   actionPerformed, 61  
   validateKeys, 61  
   ValidateRSAKeysButton, 60  
 org.example.app.buttons.impl.ValidateSignFileButton, 63  
   printLog, 63  
   selectSignedFilePath, 64  
   validateSign, 64  
   ValidateSignFileButton, 63  
 org.example.app.mainPanel.api.MainPanel, 34  
   addComponents, 34  
   config, 34  
 org.example.app.mainPanel.impl.Panel, 35  
   addComponents, 35  
   config, 35  
   Panel, 35  
 org.example.app.textFields.api.LogsField, 31

- clear, [32](#)
- print, [32](#)
- org.example.app.textFields.api.PasswordInput, [36](#)
  - getPassword, [36](#)
- org.example.app.textFields.impl.LogsFieldComponent, [32](#)
  - clear, [33](#)
  - LogsFieldComponent, [33](#)
  - print, [33](#)
- org.example.app.textFields.impl.PasswordInputComponent, [36](#)
  - getPassword, [37](#)
  - PasswordInputComponent, [37](#)
- org.example.controller.impl.AppController, [5](#)
  - decryptFile, [5](#)
  - deleteFile, [6](#)
  - encryptFile, [6](#)
  - getFileAttribute, [6](#)
  - getPrivateKey, [6](#)
  - getPublicKey, [7](#)
  - loadFile, [7](#)
  - saveFile, [7](#)
  - setRSAKeys, [8](#)
  - signFile, [8](#)
  - validateFile, [8](#)
- org.example.file.data.api.FileLoader, [17](#)
  - deleteFile, [18](#)
  - getFileAttribute, [18](#)
  - loadFile, [18](#)
  - saveFile, [19](#)
- org.example.file.data.impl.FileLoaderDefault, [19](#)
  - deleteFile, [20](#)
  - getFileAttribute, [20](#)
  - loadFile, [20](#)
  - saveFile, [21](#)
- org.example.file.funtions.EncryptingDecryptingFileFunction, [16](#)
  - DencryptingFile, [16](#)
  - EncryptingFile, [17](#)
- org.example.file.service.api.FileSecurityService, [21](#)
  - decrypt, [22](#)
  - encrypt, [22](#)
- org.example.file.service.api.FileService, [24](#)
  - delete, [24](#)
  - getFileAttribute, [24](#)
  - load, [25](#)
  - save, [25](#)
- org.example.file.service.impl.FileSecurityServiceDefault, [22](#)
  - decrypt, [23](#)
  - encrypt, [23](#)
- org.example.file.service.impl.FileServiceDefault, [26](#)
  - delete, [26](#)
  - getFileAttribute, [26](#)
  - load, [27](#)
  - save, [27](#)
- org.example.keyRSA.data.api.KeyLoader, [28](#)
  - loadKey, [28](#)
  - saveKey, [28](#)
- org.example.keyRSA.data.impl.KeyLoaderDefault, [29](#)
  - loadKey, [29](#)
  - saveKey, [30](#)
- org.example.keyRSA.functions.PrivateKeyDecryptorFunction, [37](#)
  - getPr, [38](#)
  - PrivateKeyDecryptorFunction, [37](#)
- org.example.keyRSA.functions.PublicKeyDecryptorFunction, [38](#)
  - getKey, [39](#)
  - PublicKeyDecryptorFunction, [38](#)
- org.example.keyRSA.functions.RSAGeneratorFunction, [42](#)
  - RSAGeneratorFunction, [42](#)
- org.example.keyRSA.service.api.RSAService, [43](#)
  - createKeys, [43](#)
  - encryptPrivateKey, [43](#)
  - getPublicKey, [45](#)
- org.example.keyRSA.service.impl.RSAServiceDefault, [45](#)
  - createKeys, [46](#)
  - encryptPrivateKey, [46](#)
  - getPublicKey, [46](#)
- org.example.Main, [33](#)
- org.example.misc.Logger, [30](#)
  - printLog, [31](#)
- org.example.signXAdES.functions.XAdESsignFunction, [64](#)
  - getSignFile, [65](#)
  - signEnveloped, [65](#)
  - XAdESsignFunction, [65](#)
- org.example.signXAdES.functions.XadESValidatorFunction, [66](#)
  - getValidate, [66](#)
  - XadESValidatorFunction, [66](#)
- org.example.signXAdES.service.api.SignService, [56](#)
  - signXAdES, [57](#)
  - validate, [57](#)
- org.example.signXAdES.service.impl.SignServiceDefault, [57](#)
  - signXAdES, [58](#)
  - validate, [58](#)
- Panel
  - org.example.app.mainPanel.impl.Panel, [35](#)
- PasswordInputComponent
  - org.example.app.textFields.impl.PasswordInputComponent, [37](#)
- print
  - org.example.app.textFields.api.LogsField, [32](#)
  - org.example.app.textFields.impl.LogsFieldComponent, [33](#)
- printLog
  - org.example.app.buttons.impl.DecryptFileButton, [11](#)
  - org.example.app.buttons.impl.EncryptFileButton, [15](#)

- org.example.app.buttons.impl.RSAGenerateButton, 41
- org.example.app.buttons.impl.ShowRSAKeysButton, 51
- org.example.app.buttons.impl.SignFileButton, 55
- org.example.app.buttons.impl.ValidateSignFileButton, selectSignedFilePath 63
- org.example.misc.Logger, 31
- PrivateKeyDecryptorFunction
  - org.example.keyRSA.functions.PrivateKeyDecryptorFunction, 37
- PublicKeyDecryptorFunction
  - org.example.keyRSA.functions.PublicKeyDecryptorFunction, 38
- RSAGenerateButton
  - org.example.app.buttons.impl.RSAGenerateButton, 40
- RSAGeneratorFunction
  - org.example.keyRSA.functions.RSAGeneratorFunction, 42
- save
  - org.example.file.service.api.FileService, 25
  - org.example.file.service.impl.FileServiceDefault, 27
- saveFile
  - org.example.controller.impl.AppController, 7
  - org.example.file.data.api.FileLoader, 19
  - org.example.file.data.impl.FileLoaderDefault, 21
- saveKey
  - org.example.keyRSA.data.api.KeyLoader, 28
  - org.example.keyRSA.data.impl.KeyLoaderDefault, 30
- selectFilePath
  - org.example.app.buttons.api.DecryptFile, 10
  - org.example.app.buttons.api.EncryptFile, 13
  - org.example.app.buttons.impl.DecryptFileButton, 12
  - org.example.app.buttons.impl.EncryptFileButton, 16
- selectPath
  - org.example.app.buttons.api.RSAGenerate, 40
  - org.example.app.buttons.impl.RSAGenerateButton, 41
- selectPrivateKeyPath
  - org.example.app.buttons.api.EncryptFile, 14
  - org.example.app.buttons.api.ShowRSAKeys, 49
  - org.example.app.buttons.api.SignFile, 52
  - org.example.app.buttons.impl.EncryptFileButton, 16
  - org.example.app.buttons.impl.ShowRSAKeysButton, 51
  - org.example.app.buttons.impl.SignFileButton, 55
- selectPublicKeyPath
  - org.example.app.buttons.api.DecryptFile, 10
  - org.example.app.buttons.api.ShowRSAKeys, 49
  - org.example.app.buttons.api.SignFile, 52
- org.example.app.buttons.impl.DecryptFileButton, 12
- org.example.app.buttons.impl.ShowRSAKeysButton, 51
- org.example.app.buttons.impl.SignFileButton, 55
- org.example.app.buttons.impl.ValidateSignFileButton, selectSignedFilePath
  - org.example.app.buttons.api.SignFile, 53
  - org.example.app.buttons.api.ValidateSignFile, 62
  - org.example.app.buttons.impl.SignFileButton, 55
  - org.example.app.buttons.impl.ValidateSignFileButton, 64
- setRSAKeys
  - org.example.controller.impl.AppController, 8
- ShowRSAKeysButton
  - org.example.app.buttons.impl.ShowRSAKeysButton, 50
- signEnveloped
  - org.example.signXAdES.functions.XAdESsignFunction, 65
- signFile
  - org.example.app.buttons.api.SignFile, 53
  - org.example.app.buttons.impl.SignFileButton, 55
  - org.example.controller.impl.AppController, 8
- SignFileButton
  - org.example.app.buttons.impl.SignFileButton, 54
- signXAdES
  - org.example.signXAdES.service.api.SignService, 57
  - org.example.signXAdES.service.impl.SignServiceDefault, 58
- validate
  - org.example.signXAdES.service.api.SignService, 57
  - org.example.signXAdES.service.impl.SignServiceDefault, 58
- validateFile
  - org.example.controller.impl.AppController, 8
- validateKeys
  - org.example.app.buttons.api.ValidateRSAKeys, 59
  - org.example.app.buttons.impl.ValidateRSAKeysButton, 61
- ValidateRSAKeysButton
  - org.example.app.buttons.impl.ValidateRSAKeysButton, 60
- validateSign
  - org.example.app.buttons.api.ValidateSignFile, 62
  - org.example.app.buttons.impl.ValidateSignFileButton, 64
- ValidateSignFileButton
  - org.example.app.buttons.impl.ValidateSignFileButton, 63
- XAdESsignFunction
  - org.example.signXAdES.functions.XAdESsignFunction, 65
- XAdESValidatorFunction
  - org.example.signXAdES.functions.XAdESValidatorFunction, 66

## 4 Wyniki

Utworzona aplikacja ma następujący interfejs graficzny.



Figure 2: Interfejs aplikacji

Można zauważyć przyciski, które wykonują funkcje opisane w punkcie 2.

Poniżej przedstawiona jest cała sekwencja podpisywania pliku razem z jego rezultatami. Warto zaznaczyć, że przed każdą operacją hasło wpisane do wygenerowania pary kluczy pozostaje to samo, aby można było odczytać zaszyfrowany klucz prywatny.

### 4.1 Generowanie kluczy

Zaczynamy od użytkownika **A**. Klikamy w przycisk "Generuj klucze RSA" i wybieramy lokalizację ich zapisu. Wygenerowane zostaną klucze w naszej lokalizacji. Aplikacja wyświetli nam komunikat o postępach pracy i o lokalizacji w której znajdują się nasze klucze.

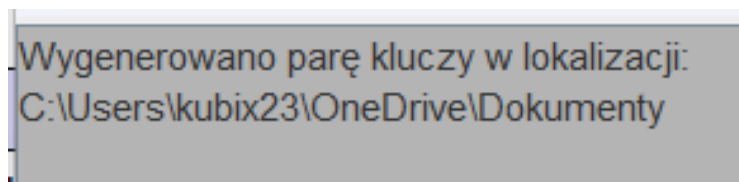


Figure 3: Logi



Figure 4: Wygenerowane klucze

#### 4.1.1 Wyświetlanie kluczy\*

**A/B** Jest to etap dodatkowy niewymagany do tworzenia podpisu. Klikamy w przycisk "Pokaż klucze RSA" i wybieramy lokalizację klucza prywatnego następnie klucza publicznego. W górnym polu tekstowym wyświetli się zawartość wybranych kluczy.



Figure 5: Fragment wygenerowanych kluczy

#### 4.1.2 Poprawność kluczy\*

**A/B** Jest to etap dodatkowy niewymagany do tworzenia podpisu. Klikamy w przycisk "Sprawdź poprawność pary kluczy" i wybieramy lokalizację klucza prywatnego następnie klucza publicznego. W górnym polu tekstowym wyświetli się informacja o poprawności kluczy.

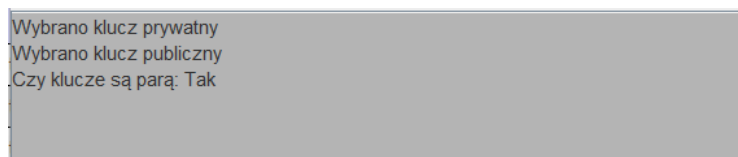
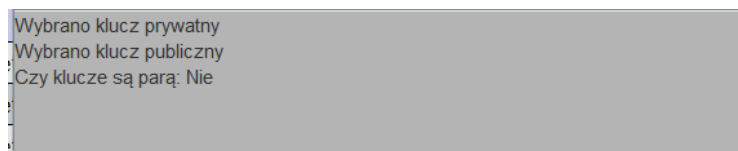


Figure 6: Poprawna para kluczy

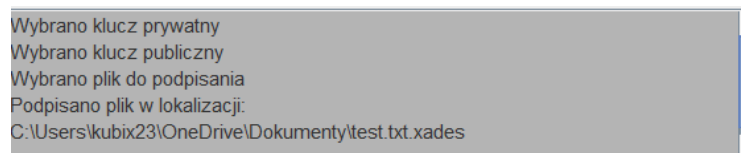


```
Wybrano klucz prywatny
Wybrano klucz publiczny
Czy klucze są parą: Nie
```

Figure 7: Niepoprawna para kluczy

## 4.2 Podpisywanie plików

**A** Klikamy w przycisk "Podpisz plik". Wybieramy lokalizację klucza prywatnego następnie klucza publicznego i podpisujemy przez nas plik. Na potrzeby demonstracji utworzony jest plik test.txt z zawartością "test test" W górnym okienku wyświetli się informacja o wygenerowanym podpisie.



```
Wybrano klucz prywatny
Wybrano klucz publiczny
Wybrano plik do podpisania
Podpisano plik w lokalizacji:
C:\Users\kubix23\OneDrive\Dokumenty\test.txt.xades
```

Figure 8: Logi



```

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  <ds:SignedInfo>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512" />
    <ds:Reference Id="Reference-a16d1372-b2d4-4294-845c-d0035673ea74" URI="test.txt">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>A//fRSdt04/6x5sOnGwU2J2RE614PVkiWA9MZqMwVZE=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
      URI="#SignedProperties-7602d28c-64aa-48a9-b96e-0d1b4471a4b8">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <ds:DigestValue>L21JsB13a18uyhwPnFP85JD4+qq18CYBbuU42XB5hM8=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    W/I5S9kHwmaXabjzubfDB/hyhmVQyXkKzFp/WAveaEbhNrNkAk+XYAeoHTuo/ee/CxbAsrT16PB85Y3dmH6y+uIah
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:KeyValue>
      <ds:RSAKeyValue>
        <ds:Modulus>
          qwlmoOU9xj/pnv3+cm00B2nWC3TkWKGC6bjoIr5cPONrWKK75cWIazYhCBxdCGvKE3XaljXmeKx433
        </ds:Modulus>
        <ds:Exponent>AQAB</ds:Exponent>
      </ds:RSAKeyValue>
    </ds:KeyValue>
  </ds:KeyInfo>
  <ds:Object>
    <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
      Target="#Signature-d022c6f1-9e53-4342-bfaf-e1ed904dddf6">
      <xades:SignedProperties Id="SignedProperties-7602d28c-64aa-48a9-b96e-0d1b4471a4b8">
        <xades:SignedSignatureProperties>
          <xades:SigningTime>2024-04-15T20:53:19</xades:SigningTime>
          <xades:SignerRole>
            <xades:ClaimedRoles>kubix23</xades:ClaimedRoles>
          </xades:SignerRole>
        </xades:SignedSignatureProperties>
        <xades:SignedDataObjectProperties>
          <xades:DataObjectFormat
            ObjectReference="#Reference-a16d1372-b2d4-4294-845c-d0035673ea74">
            <xades:MimeType>text/plain</xades:MimeType>
            <xades:Description>Size:9; Filename:test.txt;
              Date_of_modification:2024-04-15T18:52:04.649423Z </xades:Description>
            </xades:DataObjectFormat>
          </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
      </xades:QualifyingProperties>
    </ds:Object>
  </ds:Signature>

```

Figure 9: Wygenerowany podpis

### 4.3 Szyfrowanie pliku

A Klikamy w przycisk "Szyfruj plik". Wybieramy lokalizację klucza prywatnego i plik do zaszyfrowania. Wyświetli nam się nazwa zaszyfrowywanego pliku.



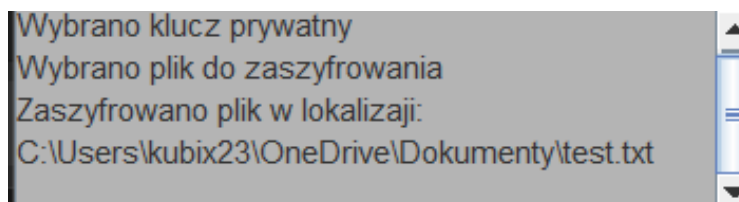


Figure 10: Logi

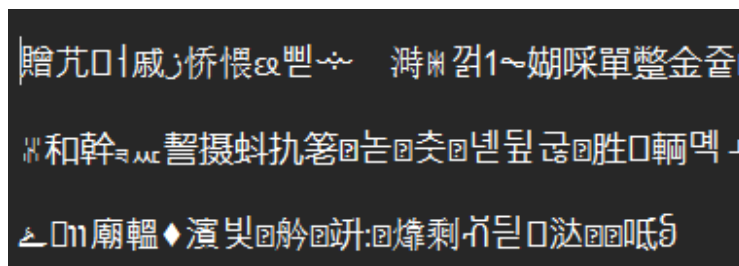


Figure 11: Fragment zaszyfrowanego pliku

#### 4.4 Deszyfrowanie pliku

W przeciwieństwie do poprzednich operacji, tą jak i resztę operacji może wykonać odbiorca pliku **B**. Klikamy w przycisk "Odszyfruj plik". Wybieramy lokalizację klucza publicznego i zaszyfrowany plik. Wyświetli nam się nazwa odszyfrowywanego pliku.

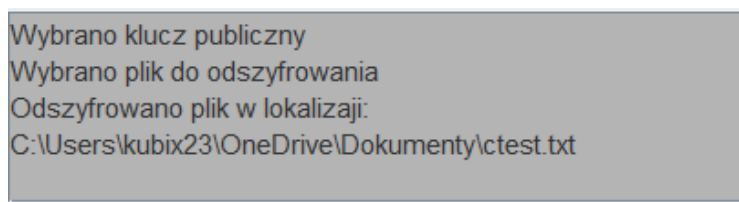


Figure 12: Logi

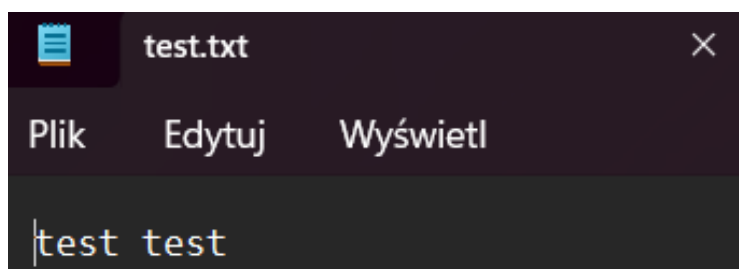


Figure 13: Odszyfrowany plik

#### 4.5 Walidacja podpisu

**B** Klikamy w przycisk "Sprawdź poprawność podpisu". Wybieramy lokalizację podpisu i upewniamy się, że podpis jest w tym samym folderze co podpis. Wyświetli nam się informacja czy plik i podpis są nienaruszone.

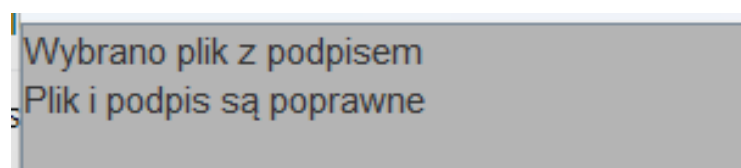


Figure 14: Nienaruszony plik i podpis

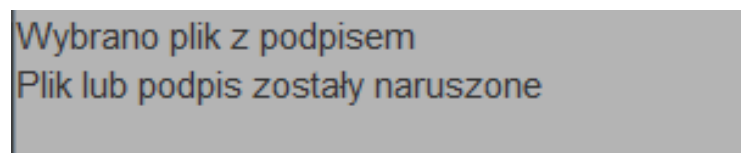


Figure 15: Naruszony plik lub podpis

## 5 Podsumowanie

W projekcie stworzona została aplikacja która pozwala na generowanie podpisu XAdES i jego weryfikację. Podpis XAdES jest powszechnie stosowany w transakcjach online, umowach elektronicznych oraz dokumentach prawnych, gdzie konieczne jest zachowanie integralności i autentyczności podpisu. Jego użycie jest często regulowane przez prawo w celu zapewnienia legalności i skuteczności.

Podpis jaki generujemy jest zgodny z unijnym standardem [https://portal.etsi.org/webapp/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=35243](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=35243). Dzięki temu jesteśmy w stanie potwierdzić poprawność naszego podpisu w zewnętrznych źródłach np. <https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation>