Пројекат из Заштите Података

Имплементиране класе:

1. *etf.openpgp.pd180205dtj180023d.AppMainFrame*
2. *etf.openpgp.pd180205dtj180023d.AddKeyDialog*
3. *etf.openpgp.pd180205dtj180023d.ChooseKeyDialog*
4. *etf.openpgp.pd180205dtj180023d.DeleteExportKeyDialog*
5. *etf.openpgp.pd180205dtj180023d.EncryptionDialog*
6. *etf.openpgp.pd180205dtj180023d.DecryptionDialog*
7. *etf.openpgp.pd180205dtj180023d.ImportKeyDialog*
8. *etf.openpgp.pd180205dtj180023d.Main*
9. *etf.openpgp.pd180205dtj180023d.MyKeyRing*
10. *etf.openpgp.pd180205dtj180023d.PGPAuthenticator*
11. *etf.openpgp.pd180205dtj180023d.PGPEncryptor*
12. *etf.openpgp.pd180205dtj180023d.PGPLiterator*
13. *etf.openpgp.pd180205dtj180023d.PGPProtocol*
14. *etf.openpgp.pd180205dtj180023d.Util*
15. *etf.openpgp.pd180205dtj180023d.PGPException*

Опис Метода:

etf.openpgp.pd180205dtj180023d.AppMainFrame

1. *AppMainFrame()*
   Конструктор sa креирање неопходних дијалога, учитавања кључева и исцртавање екрана
2. *void removeRow(int i)*
   Метода коришћена за додавање елемената у јавни и приватни прстен кључева
3. *void addKeyRing(MyKeyRing keyRing)*
   Метода коришћена за додавање кључева у колекцију кључева

etf.openpgp.pd180205dtj180023d.AddKeyDialog

1. *AddKeyDialog(Frame frame)*
   Конструктор за исцртавање екрана

Алгоритам коришћен за генерисање кључева је *RSA*, где је модуо једнак 65537. Генерисан је један пар кључева који се додаје у колекцију кључева

etf.openpgp.pd180205dtj180023d.ChooseKeyDialog

1. ChooseKeysDialog(Dialog owner, boolean ispublic)
   Конструктор за исцртавање екрана

Одабир приватних и јавних кључева који се користе у енкрипцији и потписивању.

etf.openpgp.pd180205dtj180023d.DeleteExportKeyDialog

1. *DeleteExportKeyDialog (Frame frame)*
   Конструктор за исцртавање екрана
2. *void setValues(MyKeyRing keyring, int id)*
   Постављање вредности које се приказују на екрану, које корисник може да сачува или да обрише

Приликом чувања кључева они се чувају са именом корисника и временом креирања. Приликом брисања кључ се потпуно уклања.

etf.openpgp.pd180205dtj180023d.DecryptionDialog

1. *DecryptionDialog(Frame owner)*
   Конструктор за исцртавање екрана
2. *void setValues(MyKeyRing keyring, int id)*
   Постављање вредности које се приказују на екрану, које корисник може да сачува или да обрише

Класа предтсавља интерфејс за покретање примања поруке (омогућава одабир, одабир фајла који се прима, унос passphrase лозинки за коришћење потребних приватних кључева и покретање примања поруке).

etf.openpgp.pd180205dtj180023d.EncryptionDialog

1. *EncryptionDialog(Frame owner)*
   Конструктор за исцртавање екрана

2. *void setEncryptionKeyRings(List<MyKeyRing> rings)*
   Постављање одабраних јавних кључева за енкриптовање.
3. *void setSignatureKeyRing(MyKeyRing ring)*
   Постављање одабраниог приватног кључа за потписивање.

Класа предтсавља интерфејс за покретање слања поруке (омогућава одабир опција: шифровање, потписивање, компресија и компатибилност, одабир фајла који се шаље, одабир кључева за шифрвање и потписивање, симетричног алгоритма за потписивање и покретање енкрипције одабраног фајла=.

etf.openpgp.pd180205dtj180023d.ImportKeyDialog

1. *ImportKeyDialog(Frame frame)*
   Конструктор за исцртавање екрана
2. *void setAll()*
   Неоходно позивање ове методе за сетовање почетног екрана

Приликом увоза кључева неопходно је да корисник учита и приватни и јавни кључ.

etf.openpgp.pd180205dtj180023d.MyKeyRing

1. *MyKeyRing(PGPPublicKeyRing, PGPSecretKeyRing)*
   Конструктор за креирање омотача који садржи јавни и приватни кључ
2. *void saveKey()*
   Неоходно позивање ове методе за сетовање почетног екрана
3. *void writeToFile()*
   Метода коришћена за записивање кључа у фајл

etf.openpgp.pd180205dtj180023d.PGPAuthenticator

1. *static void configureAuthentication(PGPSecretKey key, String password, OutputStream stream) throws IOException, PGPException*
   Конфигурисање заглавља за аутентикацију. Провера валидности шифре приватног кључа. Дефинисање коришћених алгоритама.
2. *static void updateSignature(byte[] buffer, int size)*
   Ажурирање стварних података који се потписују.
3. *public static void encode(OutputStream os).*
   Енкодовање потписа на крај поруке.
4. *static ValidationOutput validate(PGPOnePassSignatureList header, PGPSignatureList signatures, List<PGPPublicKey> publicKeys,*

ByteArrayOutputStream content) throws IOException, org.bouncycastle.openpgp.PGPException
Валидација потписа. Укључује препознавање јавног кључа корисника који је потписао поруку и проверу потписа дешифровањем, рачунањем хеша и поређењем.

5. *public static class ValidationOutput*
   Повратна вредност валидације потписа. Враћа поруку о грешки и коришћени јавни кључ.

Класа енкапсулира поступке потребне за потписивање и валидацију PGP поруке.

etf.openpgp.pd180205dtj180023d.PGPEncryptor

1. *static List<OutputStream> configureEncryption(SymetricKeyAlgorithm algorythm, List<PGPPublicKey> publicKeys, OutputStream stream) throws IOException, org.bouncycastle.openpgp.PGPException*
   Конфигурисање излазног тока за енкрипцију. Постављање декоратера за сваки прослеђени јавни кључ који се користи. Постављање алгоритма за симетричног алгоритма за шифровање и генератора сесијских кључева.
2. *static DecriptionOutput executeDecryption(PGPEncryptedDataList header, List<PGPSecretKey> secrets, PGPProtocol.Callback callback)*
   Декрипција поруке. Препознавање и одабир приватног кључа на основу информације у заглављу. Покретање уноса шифре за одговарајући кључ и њена валидација.
3. static class DecriptionOutput
   Повратна вредност дешифровања. Враћа поруку о грешки и улазни стрим декриптованих података.
4. *enum SymetricKeyAlgorithm*
   Алгоритам симетричног шифровања

Класа енкапсулира поступке потребне за енкрипцију и декрипцију поруке.

etf.openpgp.pd180205dtj180023d.PGPLiterator

1. *static OutputStream configureLiteralBlock(OutputStream stream, String inputFile) throws IOException*
   Конфигурисање заглавља садржаја поруке.
2. *static void copyData(OutputStream stream, ByteArrayOutputStream content,PGPLiteralData data)*

Копирање садржаја поруке у излазни фајл и стрим за проверу потписа и испис поруке на екрану.

Класа енкапсулира поступке потребне за рад са правим садржајем поруке.

etf.openpgp.pd180205dtj180023d.PGPProtocol

1. *static void sendMessage(String inputFile, PGPEncryptor.SymetricKeyAlgorithm algorithm, List<PGPOptions> options, List<MyKeyRing> publicKeyRings, MyKeyRing secretKey, String password) throws PGPException*
   Слање поруке. Укључује покретање одговарајућих акција у зависности од одабраних опција PGP протокола (енкрипције, потписивања, компресије и компатибилности), читање поруке из улазног фајла и уписивање поруке у конфигурисани енкриптовани излазни фајл. Детектовање грешака.
2. *static DecryptOutput receiveMessage (String inputFile, List<MyKeyRing> keyRings, Callback callback) throws PGPException*
   Примање поруке. Укључује покретање одговарајућих акција у зависности од препознатих заглавља PGP протокола (енкрипције, потписивања, компресије и компатибилности), извлачење поруке из енкриптованог фајла и уписивање у излазни фајл и стрим за приказ на екрану заједно са именом потписиваоца. Детектовање грешака.
3. *static class DecryptOutput*
   Повратна вредност прихватања поруке. Враћа коришћени јавни кључ пошиљаоца и стрим поруке.

Класа енкапсулира PGP протокол.

etf.openpgp.pd180205dtj180023d.Util

1. *static Object[] generateTableRow(MyKeyRing ring)*
   Форматиање реда у табели за испис кључева.

etf.openpgp.pd180205dtj180023d. PGPException

1. PGPException(String message)
   Конструктор изузетка.

Аутори:
Димитрије Панић 18/0205
Јана Тољага 18/0023