Dokumentacija projekta

Implementacija OpenPGP standarda

Milan Akik 2018/0688

Milena Đurić 2018/0630

(0688+0630)mod6+1=5

RSA za enkripciju i potpisivanje sa kljucevima velicine 1024, 2048 i 4096

3DES sa EDE konfiguracijom i 3 kljuca i IDEA

Sama dokumentacija se nalazi u podfolderu doc Eclipse projekta.

Osnovni paket je etf.openpgp.am180688ddm180630d. U njemu se nalazi klasa Main koja sadrzi main metodu. Unutar tog paketa se nalaze jos tri podpaketa: data, gui i util.

Package etf.openpgp.am180688ddm180630d

package etf.openpgp.am180688ddm180630d

Related Packages

Package	Description
etf.openpgp.am180688ddm180630d.data	
etf.openpgp.am180688ddm180630d.gui	
etf.openpgp.am180688ddm180630d.util	

Classes

Class	Description
Main	

Paket data sadrzi klase za privatni i javni kljuc i njihove prstenove i podpaketi enumerators, packet, subpacket i types.

Package etf.openpgp.am180688ddm180630d.data

package etf.openpgp.am180688ddm180630d.data

Related Packages

Package	Description
etf.openpgp.am180688ddm180630d	
etf.openpgp.am180688ddm180630d.data.enumerators	
etf.openpgp.am180688ddm180630d.data.packet	
etf.openpgp.am180688ddm180630d.data.subpacket	
etf.openpgp.am180688ddm180630d.data.types	
etf.openpgp.am180688ddm180630d.gui	
etf.openpgp.am180688ddm180630d.util	

Classes

Class	Description
PrivateKey	
PrivateKeyRing	
PublicKey	
PublicKeyRing	

Podpaket types sadrži samo jednu klasu MPI koja predstavlja MPI(Multi precision integer) iz OpenPGP standarda.

Package etf.openpgp.am180688ddm180630d.data.types

package etf.openpgp.am180688ddm180630d.data.types

Related Packages

Package	Description
etf.openpgp.am180688ddm180630d.data	
etf.openpgp.am180688ddm180630d.data.enumerators	
etf.openpgp.am180688ddm180630d.data.packet	
etf.openpgp.am180688ddm180630d.data.subpacket	

Classes

Class	Description
MPI	

Podpaket enumerators sadrži java Enumeratore za kompresione algoritme, heš algoritme, tag paketa, algoritme asimetrične enkripcije, tipove potpisa i tipove potpisnih podpaketa.

Package etf.openpgp.am180688ddm180630d.data.enumerators

package etf.openpgp.am180688ddm180630d.data.enumerators

Related Packages

Package	Description
etf.openpgp.am180688ddm180630d.data	
etf.openpgp.am180688ddm180630d.data.packet	
etf.openpgp.am180688ddm180630d.data.subpacket	
etf.openpgp.am180688ddm180630d.data.types	

Enum Classes

Class	Description
CompressionAlgorithm	
HashAlgorithm	
PacketTag	
PublicKeyAlgorithm	
SignatureSubpacketType	
SignatureType	

Podpaket packet sadrži klase Packet, PublicKeyPacket, SignaturePacket i UserIDPacket. Klasa Packet sadrži zajedničku strukturu svih paketa, dok se ostale tri klase izvode iz nje. Ostale tri klase sadrže pojedinosti svakog od tipova paketa.

Package etf.openpgp.am180688ddm180630d.data.packet

package etf.openpgp.am180688ddm180630d.data.packet

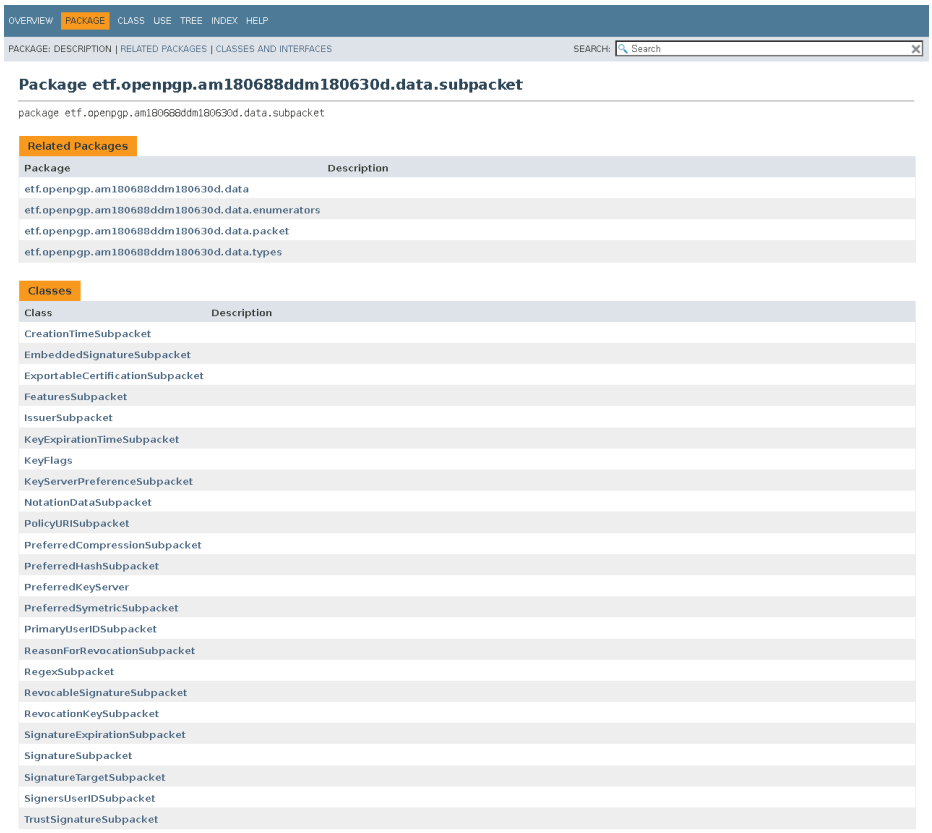
Related Packages

Package	Description
etf.openpgp.am180688ddm180630d.data	
etf.openpgp.am180688ddm180630d.data.enumerators	
etf.openpgp.am180688ddm180630d.data.subpacket	
etf.openpgp.am180688ddm180630d.data.types	

Classes

Class	Description
Packet	
PublicKeyPacket	
SignaturePacket	
UserIDPacket	

Podpaket subpacket u sebi sadrži implementiranu klasu SignatureSubpacket, kao i preostalih 23 tipova podpaketa paketa za potpisivanje. SignaturSubpacket sadrži zajedničku strukturu svih podpaketa paketa za podpisivanje.



Paket gui sadrzi jednu klasu MainMenu koja se bavi celim sistemom prozora.

Package etf.openpgp.am180688ddm180630d.gui

package etf.openpgp.am180688ddm180630d.gui

Related Packages

Package	Description
etf.openpgp.am180688ddm180630d	
etf.openpgp.am180688ddm180630d.data	
etf.openpgp.am180688ddm180630d.util	

Classes

Class	Description
MainMenu	

Paket util sadrzi 4 pomocne klase: ASCReader, CRCUtil, Radix64Util i RSAUtil. ASCReader sluzi da procita fajl koji je u Armored ASCII formatu i pretvori ga u niz bajtova i proveri njegov CRC. CRCUtil sluzi da bi se za niz bajtova izracunao CRC24-Radix64 kod opisan u RFC4880 standardu. Radix64Util ima metode za enkodovanje i dekodovanje niza bajtova u radix64 String i radix64 Stringa u niz bajtova. RSA sluzi za generisanje javnog kljuca(eksponenta i modulusa) odredjene velicine/duzine u bitovima.

Package etf.openpgp.am180688ddm180630d.util

package etf.openpgp.am180688ddm180630d.util

Related Packages

Package	Description
etf.openpgp.am180688ddm180630d	
etf.openpgp.am180688ddm180630d.data	
etf.openpgp.am180688ddm180630d.gui	

All Classes and Interfaces | **Classes** | **Enum Classes**

Class	Description
ASCReader	
ASCReader.KeyType	
CRCUtil	
Radix64Util	
RSAUtil	