Пројектни задатак 2016/2017. – појашњење метода класе *CodeV3*

Метода *loadLocalKeystore()* треба да учита локално складиште кључева и као повратну вредност врати листу *алиас*-а за парове кључева/сертификате у *keystore*-у.

Метода *resetLocalKeystore()* треба да обрише локално складиште кључева.

Метода *loadKeypair(String keypair_name)* треба да учита податке о пару кључева/сертификату који је сачуван под алиасом *keypair_name* из локалног *keystore*-а и прикаже их на графичком корисничком интерфејсу. Повратна вредност методе је целобројна вредност која означава успешност операције. Метода враћа -1 у случају грешке, 0 у случају да сертификат сачуван под тим алиасом није потписан, 1 у случају да је потписан, 2 у случају да је у питању увезени *trusted* сертификат.

Метода *saveKeypair(String keypair_name)* треба да на основу података са графичког корисничког интерфејса генерише и сачува нови пар кључева у локалном *keystore*-у под алиасом са вредношћу *keypair_name.* Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *removeKeypair(String keypair_name)* треба да из локалног *keystore*-а обрише пар кључева/сертификат који је сачуван под алиасом *keypair_name.* Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *importKeypair(String keypair_name, String file, String password)* треба да из фајла са путањом *file* учита постојећи пар кључева који је сачуван у *PKCS#12* формату и заштићен лозинком и сачува га у локални *keystore* под алиасом *keypair_name.* Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *exportKeypair(String keypair_name, String file, String password)* треба да постојећи пар кључева који је у локалном *keystore*-у сачуван под алиасом *keypair_name* извезе у фајл са путањом *file* у *PKCS#12* формату и заштити лозинком. Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *signCertificate(String issuer, String algorithm)* треба да потпише алгоритмом *algorithm* тренутно селектовани сертификат на графичком корисничком интерфејсу приватним кључем сертификата који је у локалном *keystore*-у сачуван под алиасом *issuer.* Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *importCertificate(File file, String keypair_name)* треба да из фајла *file* (екстензије .cer) учита постојећи сертификат и сачува га у локални *keystore* под алиасом *keypair_name.* Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *exportCertificate(File file, int encoding)* треба да у фајл *file* (екстензије .cer) извезе постојећи сертификат тренутно селектован на графичком корисничком интерфејсу и кодира га на начин назначен вредношћу параметра *encoding* (0 за *DER*, 1 за *PEM*). Повратна вредност методе означава успешност операције, *false* у случају грешке.

Метода *getIssuer (String keypair_name)* треба да врати податке о издавачу сертификата који је у локалном *keystore*-у сачуван под алиасом *keypair_name.*

Метода *getIssuerPyblicKeyAlgorithm (String keypair_name)* треба да врати податке о алгоритму који је коришћен за генерисање пара кључева сертификата који је у локалном *keystore*-у сачуван под алиасом *keypair_name.*

Метода *getRSAKeyLength (String keypair_name)* треба да врати дужину кључа сертификата који је у локалном *keystore*-у сачуван под алиасом *keypair_name* у случају да је алгоритам који је коришћен за генерисање пара кључева овог сертификата *''RSA''*. Користи се за проверавање дозвољених комбинација дужине кључева *RSA* алгоритма и *hash* алгоритама.

Метода *getIssuers(String keypair_name)* треба да врати листу *alias*-а свих сертификата сачуваних у локалном *keystore*-у који могу да потпишу сертификат који је у локалном *keystore*-у сачуван под алиасом *keypair_name.*

Метода *generateCSR(String keypair_name)* треба да генерише захтев за потписивање сертификата (*CSR*) који је у локалном *keystore*-у сачуван под алиасом *keypair_name.* Повратна вредност методе означава успешност операције, *false* у случају грешке.