Пројектни задатак 2017/2018.

Циљ пројектног задатка је боље разумевање структуре X.509 сертификата, као и начина њиховог генерисања и употребе. У ту сврху задатак подразумева пројектовање и имплементацију апликације са графичким корисничким интерфејсом у програмском језику *Java* која треба да омогући следеће функционалности:

- генерисање новог пара кључева за X.509 сертификат,
- извоз/увоз постојећег пара кључева за X.509 сертификат,
- преглед детаља постојећих парова кључева за X.509 сертификат,
- потписивање X.509 сертификата,
- извоз креираног X.509 сертификата.

Детаљи сваке од функционалности дефинисане су на различит начин за различите групе за израду пројекта, које су дате у наставку документа (Прилог 1). Сваки студент имплементираће пројекат у складу са поставком групе која му буде додељена. Како би студенти били фокусирани на сигурносни аспект, неће морати самостално да имплементирају графички кориснички интерфејс, већ ће им исти бити обезбеђен у облику .jar библиотеке. Упутство за коришћење .jar библиотеке дато је у наставку документа (Прилог 2).

Напомене:

1. Пројекат се ради самостално. Сви студенти који прате предмет су аутоматски пријављени за израду пројекта. Студент треба да изради пројекат из групе која се добија на следећи начин: *gr =* (*brind mod 30) + 1*, где је *gr* број групе коју студент треба да ради, а *brind* број индекса студента (нпр. студент са индексом 2017/0897 треба да ради групу 28 *= (897 mod 30) + 1*).
2. Сви предати пројекти ће бити пропуштени кроз апликацију за проверу сличности програмског кода. Уколико се провером установи да су два или више предатих пројеката са већим степеном сличности од дозвољеног, сви аутори ће бити пријављени дисциплинској комисији Факултета.

3. Није дозвољено коришћење готових алата за рад са сертификатима (нпр. *keytool*) у реализацији пројекта.

4. Крајњи рок за завршетак пројектног задатка је 13.06.2018. након чега ће бити организоване одбране пројеката. Одбрана је предвиђена за 15.06.2018. и по потреби 16.06.2018. У случају да буде више од 10 заинтересованих студената за ранију одбрану пројекта, она може бити организована 28.05.2018. или 29.05.2018. за те студенте.

5. Пројекат се предаје најкасније 48 сати пре одбране као ZIP архива на начин који ће студентима благовремено бити саопштен.

6. Пројекат носи 20 поена. Од тога 15 поена је могуће освојити за исправно реализован пројекат одбрањен на усменој одбрани, док се преосталих 5 поена може освојити успешном реализацијом модификације на самој одбрани пројекта. Иста правила важе и у предроку (уколико буде организован).

7. Корисни ресурси за пројекат:

    a. https://www.ietf.org/rfc/rfc5280.txt

    b. https://docs.oracle.com/javase/7/docs/api/java/security/package-summary.html

    c. https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html

    d. https://www.bouncycastle.org/

8. За сва питања и нејасноће у вези пројекта писати на majav@etf.rs, pavle.vuletic@etf.bg.ac.rs или zarko@etf.rs.

Прилог 1. Детаљи неопходних функционалности распоређени по групама

Група 1.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа издаваоца сертификата (authority key identifier), алтернативна имена корисника (subject alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 2.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа власника сертификата (subject key identifier), алтернативна имена корисника (subject alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 3.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа издаваоца сертификата (authority key identifier), алтернативна имена корисника (subject alternative name) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 4.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа власника сертификата (subject key identifier), алтернативна имена издаваоца сертификата (issuer alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 5.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа издаваоца сертификата (authority key identifier), алтернативна имена издаваоца сертификата (issuer alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 6.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа власника сертификата (subject key identifier), алтернативна имена издаваоца сертификата (issuer alternative name) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 7.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа власника сертификата (subject key identifier), додатне атрибуте корисника (subject directory attributes) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 8.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа издаваоца сертификата (authority key identifier), додатне атрибуте корисника (subject directory attributes) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 9.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификатор кључа издаваоца сертифката (authority key identifier), додатне атрибуте корисника (subject directory attributes) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 10.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена корисника (subject alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 11.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена корисника (subject alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 12.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена корисника (subject alternative name) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 13.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена издаваоца сертификата (issuer alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 14.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена издаваоца сертификата (issuer alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 15.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена издаваоца сертификата (issuer alternative name) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 16.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), додатне атрибуте корисника (subject directory attributes) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 17.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), додатне атрибуте корисника (subject directory attributes) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 18.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), додатне атрибуте корисника (subject directory attributes) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 19.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), алтернативна имена корисника (subject alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 20.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), алтернативна имена корисника (subject alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 21.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), алтернативна имена корисника (subject alternative name) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 22.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), алтернативна имена издаваоца сертификата (issuer alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 23.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), алтернативна имена издаваоца сертификата (issuer alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 24.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), алтернативна имена издаваоца сертификата (issuer alternative name) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 25.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), додатне атрибуте корисника (subject directory attributes) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 26.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), додатне атрибуте корисника (subject directory attributes) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 27.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), додатне атрибуте корисника (subject directory attributes) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 28.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само DSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: идентификаторе кључева (key identifiers), алтернативна имена корисника (subject alternative name) и основна ограничења (basic constraints). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 29.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: коришћење кључа (key usage), алтернативна имена издаваоца сертификата (issuer alternative name) и проширено коришћење кључа (extended key usage). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се за одабрани пар кључева генерише захтев за потписивање сертификата (CSR) у PKCS #10 формату (екстензија .csr). За све парове кључева који имају право да потписују друге сертификате (CA услов) омогућити да могу да потпишу претходно генерисане захтеве за потписивање сертификата. Процедура је да се у овом случају најпре учитају све информације из захтева за потписивање сертификата, осим екстензија, затим се омогући измена оних параметара за које је задужен сертификациони ауторитет и након тога потврди потписивање захтева. Резултат ове радње је креирање CA reply фајла у PKCS #7 формату (екстензија .p7b), који је након тога могуће увести за одговарајући пар кључева, чиме он добија потпис.

За креиране X.509 сертификате потребно је омогућити извоз сертификата или читавог ланца (уколико је могуће) у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Група 30.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само EC алгоритам (са свим дужинама кључа подржаним у графичком корисничком интерфејсу) у комбинацији са свим варијантама хеш алгоритама подржаним у графичком корисничком интерфејсу. Кориснику треба понудити да унесе следеће информације: величину кључа, верзију сертификата, период важења, серијски број и информације о кориснику (CN, OU, O, L, ST, C). Треба подржати само верзију 3 сертификата. Кориснику треба понудити да опционо може да унесе и следеће екстензије: полисе сертификата (certificate policies), додатне атрибуте корисника (subject directory attributes) и ограничавање било које полисе (inhibit any policy). Омогућити за екстензије да се означи да ли су критичне или не. Корисник треба да има могућност да у апликацији сачува генерисани пар кључева под жељеним именом.

Приликом извоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји) и унесе лозинку којом ће заштити фајл. Приликом увоза пара кључева за X.509 сертификат кориснику треба омогућити да одабере фајл за увоз и унесе лозинку којом је фајл заштићен, а затим сачува увезени пар кључева под жељеним именом. Треба подржати само PKCS #12 формат фајла (екстензија .p12).

За све постојеће парове кључева омогућити структурирани приказ свих поља дефинисаних у опису функционалности генерисања новог пара кључева за X.509 сертификат уз додатак информација о потпису за оне парове који су потписани.

Приликом потписивања X.509 сертификата потребно је омогућити да се најпре за одабрани пар кључева генерише захтев за потписивање сертификата (CSR), затим да се прикажу подаци о сертификату и на крају омогући кориснику да потпише сертификат. За CSR користити PKCS #10 формат.

За креиране X.509 сертификате потребно је омогућити извоз сертификата у base-64 енкодираном X.509 формату (PEM) и бинарном формату (DER) (у оба случаја екстензија фајла је .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Прилог 2. Упутство за коришћење .jar библиотеке за креирање пројекта

Студентима су на располагању две библиотеке *jdatepicker-1.3.4.jar* и *X509_2018.jar* помоћу којих треба реализовати апликацију за генерисање и потписивање *X509* сертификата. Библиотеке треба учитати у оквиру новокреираног *java* пројекта подешавањем *java build path*-а у конфигурацији пројекта.

Осим библиотека потребно је направити и *config.txt* фајл у оквиру кога се налази конфигурација за групу коју студент треба да имплементира. У овом фајлу треба набројати који алгоритам и које екстензије треба да буду подржани у графичком корисничком интерфејсу (раздвајати их новим редом). Вредности параметара су: *DSA, RSA* и *EC* за алгоритме; *authority key identifier, subject key identifier, key usage, certificate policies, subject alternative name, issuer alternative name, subject directory attributes, basic constraints, name constraints, extended key usage* и *inhibit any policy* за екстензије; треба навести и *extensions rules* параметар који омогућава да се у графичком корисничком интерфејсу аутоматски успоставе сва додатна правила која важе приликом постављања екстензија. Приликом учитавања фајла, апликација не прави разлику између малих и великих слова, а није битан ни редослед навођења. При покретању апликације у оквиру командне линије треба задати путању до овог фајла.

Након тога треба креирати пакет *implementation* и у оквиру њега класу *MyCode* која треба да буде изведена из класе *x509.v3.CodeV3*. Ова класа је дата у оквиру пакета *x509.v3* у библиотеци *X509_2018.jar*. У склопу решавања пројектног задатка потребно је имплементирати наслеђене методе. Дозвољено је уводити нове класе, по потреби. Улазна тачка програма налази се у класи *X509* у библиотеци *X509_2018.jar*.

На располагању је и *ETFrootCA.p12* који треба учитати у апликацију по завршетку пројекта и који се може користити као ауторитет за потписивање сертификата (шифра је *root*).