Пројектни задатак 2015/2016.

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 и
- извоз креираног X.509 сертификата.

Приликом генерисања новог пара кључева за X.509 сертификат треба подржати само RSA алгоритам у комбинацији са SHA-1 алгоритмом. 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, E). Верзију сертификата треба ограничити само на v3. Кориснику треба понудити да опционо може да унесе и следеће екстензије: основна ограничења (basic constraints), алтернативна имена издаваоца сертификата (issuer alternative name) и коришћење кључа (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). Фајл приликом извоза треба заштити AES алгоритмом.

За све постојеће парове кључева омогућити структуирани 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 (екстензија .cer). Кориснику омогућити да одабере путању до фајла за извоз (креира фајл, ако не постоји).

Напомене:

1. Пројекат се ради самостално за студенте мастер студија, а у групама од максимално два члана или самостално за студенте основних студија. Студенти мастер студија су аутоматски пријављени за израду пројекта. Студенти основних студија треба да се пријаве путем Moodle-a (http://elearning.rcub.bg.ac.rs/moodle/) најкасније до 03.05.2016. до 20:00.

2. Крајњи рок за завршетак пројектног задатка је 19.06.2016. након чега ће бити организоване одбране пројеката. Одбрана је предвиђена за 20.06.2016. и по потреби 21.06.2016. У случају да буде више од 10 заинтересованих група за ранију одбрану пројекта, она може бити организована 02.06.2016. или 03.06.2016. за те студенте.

3. Пројекат се предаје најкасније 24 сата пре одбране као ZIP архива слањем на мејл zarko@etf.rs.

4. 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

5. За сва питања и нејасноће у вези пројекта писати на zarko@etf.rs.