

Пројектни задатак 2016/2017. – јавни тест

За потребе провере валидности сертификата креираних апликацијом коју студенти израде у оквиру пројекта, обезбеђена је клијент/сервер апликација која успоставља сигурну SSL конекцију коришћењем генерисаног сертификата. Упутство за конфигурисање ове апликације дато је у наставку документа.

Потребно је најпре увести пар кључева који је достављен у оквиру материјала за израду пројекта (*ETFrootCA.p12*, шифра је *root*) у своју апликацију. Затим је потребно у својој апликацији направити нов пар кључева и искористити приватни кључ из увезеног пара (*ETFrootCA.p12*) за потписивање новог пара кључева. На крају потребно је извести тако потписани пар кључева у фајл (*.p12*).

Сада треба покренути апликацију која је достављена (*SSLConnection.jar*). Клијент је имплицитно конфигурисан тако да има сертификат *ETFrootCA*, па је у апликацији потребно само увести претходно формиран пар кључева коришћењем опције *Import keypair (.p12)* на серверу и након тога у случају да је све исправно клијент и сервер ће разменити поруке. У супротном биће исписана грешка која се догодила.