Математички факултет
Универзитета у Београду

МОЛБА ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Реализација сервиса за издавање дигиталних сертификата и протокола за проверу валидности издатих сертификата.

Значај теме и области:

Имајући у виду степен коришћења интернет комуникације у данашњем добу, проблем безбедности интернет комуникације постаје изузетно значајан.

Слој сигурних сокета (Secure Socket Layer - SSL) је сигурносни протокол за комуникацију на интернету, посебно у случају услуга веба које се односе на електронску трговину и електронско банкарство. Већина веб сервера и веб прегледача подржава SSL као, де факто, стандард безбедне комуникације између клијента и сервера. За успешно функционисање SSL-а неопходно је да успешно функционише инфраструктура јавних кључева (Public Key Infrastructure - PKI).

За успешно коришћење PKI битан је ентитет ауторизован за издавање дигиталних сертификата (Certification Authority - CA), чија је главна улога да дигитално потписује и издаје јавне кључеве везане за одређеног корисника. Једна од најважнијих операција коју треба да реализује PKI, поред издавања сертификата, је провера валидности издатих сертификата.

Специфични циљ рада:

С обзиром на значај проблема сигурности електронске комуникације и на значај PKI, у раду ће се разматрати које захтеве треба да испуњава робустан CA и описати дизајн и имплементација серверске апликација за CA реализоване тако да испуњава претходно дефинисане захтеве.

У оквиру рада на тези биће реализована серверска апликација која има функционалност CA.

У опису карактеристика и реализације сервиса, који представља CA, посебна пажња ће бити посвећена операцијама издавања дигиталног сертификата и провере валидности издатог сертификата.

Надаље, мастер рад ће садржати и детаљни опис примене сертификата у циљу постизања сигурности комуникације са веб сервисима.

План је да се серверска апликација за CA реализује коришћењем Јава технологија (JavaEE и оквир за развој Spring) уз примену обрасца дизајна „модел-поглед-контролер“ (MVC).

Остале битне информације:

Провера валидности издатих сертификата се реализује помоћу протокола OCSP.

Јелена Тодоровић, 1042/2011, Математика, Инф.
(име и презиме студ., бр. инд., ознака програма и модула)

_____
(својеручни потпис студента)

_____
(датум подношења молбе)

Сагласан ментор проф. др Владимир Филиповић

_____
(својеручни потпис ментора)

Чланови комисије

1. проф. др Душан Тошић
2. проф. др Миодраг Живковић

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____
(*шеф катедре*)

_____
(*датум одобравања молбе*)