УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 01.12.2020. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Алексе Радовановића под насловом „Анализа PKCS 11 стандарда и имплементација одабраних криптографских операција у сагласности са стандардом“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Алекса Радовановић је рођен 23.04.1996. године у Београду. Завршио је основну школу „Ђуро Стругар" у Београду као ђак генерације. Уписао је Девету гимназију „Михаило Петровић Алас“ у Београду, коју је завршио као вуковац. Електротехнички факултет уписао је 2015. године. Дипломирао је у року као студент на Одсеку за рачунарску технику и информатику 2019. године са просечном оценом 8,22. Дипломски рад одбранио је 2019. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за рачунарску технику и информатику уписао је у октобру 2019. године. Положио је све испите са просечном оценом 9,20. Запослен је у струци на позицији софтвер инжењера преко годину дана.

2. Опис мастер рада

Мастер рад обухвата 45 страна, са укупно 28 слика, 10 табела и 63 референце. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак слика, списак табела и прилог са кодом коришћеним за тестове перформанси.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Уведен је појам *PKCS #11* стандарда и *HSM* (*Hardware Security Module*) уређаја.

У другом поглављу су наведени и објашњени основни појмови стадарда, са посебним освртом на делове који су од значаја за разумевање имплементације реализоване апликације.

У трећем поглављу је описана општа архитектура једног *HSM* уређаја. Дати су неки од стандарда које овакви уређаји морају да испуњавају, као и сигурносни проблеми софтверске имплементације и на који начин су они решени у хардверским модулима.

У четвртом поглављу детаљно је објашњена имплементација једног банкарског портала који омогућава слање и читање безбедних порука (трансакција) коришћењем *HSM* уређаја, према *PKCS #11* стандарду. Описана је и поставка машине на којој апликација ради, као и алати, симулатори и библиотеке који су коришћени за имплементацију.

Тестови перформанси *HSM* уређаја који су пронађени у доступној литератури изложени су у петом поглављу. У овом поглављу приказани су и резултати тестова перформанси имплементиране апликације који су спроведени коришћењем симулатора, правог *HSM* уређаја и софтверске криптографије.

Шесто поглавље је закључак у оквиру кога је описан значај описаног решења и могућа даља унапређења. Резимирани су резултати рада и изазови приликом пројектовања.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Алексе Радовановића се бави изучавањем *PKCS #11* стандарда у криптографији, који је предвиђен за коришћење са хардверским криптографским уређајима (нпр. *HSM*, паметне картице и сл.). У оквиру рада је направљено поређење оваквог приступа криптографије са софтверском имплементацијом. На примеру веб апликације је приказано како користити ову врсту криптографије, као алтернативу уобичајеној софтверски реализованој криптографији.

Основни доприноси рада су: 1) теоретско објашњење апстракција које стандард *PKCS #11* нуди, као и начина функционисања хардверских криптографских модула и њихових предности; 2) пројектовање, имплементација и тестирање апликације за обављање криптографских операција и комуникацију са хардверским криптографским уређајима у сагласности са *PKCS #11* стандардом; 3) поређење перформанси имплементиране апликације који су спроведени коришћењем симулатора, правог *HSM* уређаја и софтверске криптографије.

4. Закључак и предлог

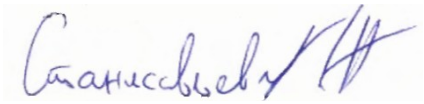
Кандидат Алекса Радовановић је у свом мастер раду успешно имплементирао апликацију која приказује реалну употребу стандарда *PKCS #11* за комуникацију са хардверским криптографским уређајима. О стандарду, имплементацији и самим *HSM* уређајима има мало јавно доступне документације, па овај рад може олакшати разумевање истих заинтересованима.

Кандидат је исказао самосталност и систематичност у свом поступку.

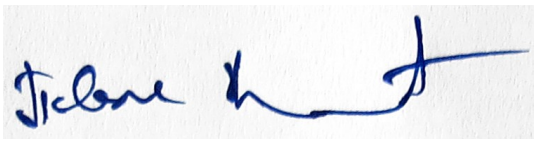
На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Алексе Радовановића под насловом „Анализа PKCS 11 стандарда и имплементација одабраних криптографских операција у сагласности са стандардом“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 16.12.2020. године

Чланови комисије:



Др Жарко Станисављевић, ванредни професор



Др Павле Вулетић, ванредни професор