



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 именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Василија Долића под насловом „Дистрибуција и складиштење криптографског материјала потребног за комуникацију паметних електричних бројила“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Василије Долић је рођен 19.04.1994. године у Београду. Завршио је основну школу „Десанка Максимовић“ у Земуну. Уписао је Земунску гимназију, коју је завршио са одличним успехом. Електротехнички факултет у Београду уписао је 2013. године. Дипломирао је на одсеку за рачунарску технику и информатику 2018. године са просечном оценом на испитима 8.29, на дипломском 10. Мастер студије на Електротехничком факултету у Београду је уписао 2018. на Модулу за рачунарску технику и информатику. Положио је све испите са просечном оценом 9,20.

2. Опис мастер рада

Мастер рад обухвата 44 стране, са укупно 26 слика и 18 референци. Рад садржи увод, 7 поглавља и закључак (укупно 9 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљене су значај и историја развоја бројила, основе паметне електричне мреже и DLMS/COSEM (Device Language Message Specification/Companion Specification for Energy Metering) протокола за комуникацију паметних електричних бројила.

У другом поглављу је дат преглед паметне електричне мреже и њених делова. Описани су паметно електрично бројило и његове најбитније функционалности, концентратор података и његова улога као део паметне електричне мреже и централни систем за приступ подацима који управља и конфигурише бројила унутар мреже.

У трећем поглављу је дат кратак опис DLMS/COSEM протокола и његових делова. Описан је начин моделовања података унутар протокола, као и структуру порука и њихов транспорт унутар истог.

Четврто поглавље описује аутентификационе механизме и криптографске алгоритме који се користе у DLMS/COSEM протоколу, као јако битан део протокола јер обезбеђују сигурност и поверљивост података на бројилу и током њиховог транспорта у комуникацији.

У оквиру петог поглавља су описани захтеви и услови које пројектовани систем мора да задовољи. Такође, наведени су и сви типови кључева (као и њихова намена) који ће се складиштити у систему.

У шестом поглављу је дат опис система за дистрибуцију и складиштење криптографског материјала. Описана је структура базе података и сви подаци који ће се у њој складиштити. Такође, описана је и архитектура система и његових слојева: слој за приступ подацима, бизнис логика и REST API слој. У овом поглављу се описују и аутентификација и ауторизација корисника у систему, као и алгоритам за генерисање и упис нових кључева на бројила.

Поглавље седам приказује главне функционалности које овај систем пружа апликацијама које је користе: дохватање кључева из система, генерисање нових кључева, додавање нових кључева у систем и брисање кључева из система.

Поглавље осам описује апликацију за администрацију система, која се користи за контролу и измене унутар система, као и опис REST захтева преко којих се приступа систему, са датим примерима коришћења.

Девето поглавље је закључак у оквиру кога је описан значај описаног решења и могућа даља унапређења истог.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Василија Долића се бави проблематиком дистрибуирања и складиштења криптографског материјала потребног за комуникацију паметних електричних бројила.

Пројектовани систем који се користи за сигурно и поуздано складиштење криптографских кључева, који се користе у комуникацији бројила са концентратором и/или централним системом за приступ подацима, дефинисаних по DLMS/COSEM протоколу имплементирана је користећи .Net Core алат са SQL Server базом података.

Систем описан у раду задовољава тренутно тржиште паметних електричних бројила. Овај систем на ефикасан начин омогућава свим апликацијама написаним у сврху комуникације са паметним бројилима по DLMS/COSEM протоколу да поуздано складиште и када је то потребно приступе криптографском материјалу који им је потребан за комуникацију.

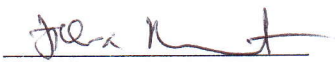
4. Закључак и предлог

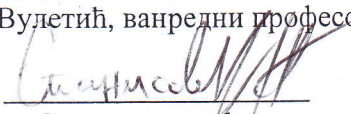
Кандидат Василије Долић је у свом мастер раду успешно решио проблем дистрибуирања и складиштења криптографског материјала потребног за комуникацију паметних електричних бројила. Развијени систем омогућава сигурно и поуздано складиштење криптографског материјала, као и његово брзо и поуздано дистрибуирање. Захваљујући томе комуникација са паметним електричним бројилима се може неометано одвијати и подаци који се у њој налазе су минимално угрожени. Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Василија Долића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 28.08.2020. године

Чланови комисије:


Др Павле Вулетић, ванредни професор


Др Жарко Станисављевић, доцент