Analiza različitih mehanizama za licenciranje softverskih modula u automobilskoj industriji

Kraus, Filip

SVEUČILIŠTE JOSIPA JURJA STORSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK
Sveučilišni studij

ANALIZA RAZLIČITIH MEHANIZAMA ZA LICENCIRANJE SOFTVERSKIH MODULA U AUTOMOBILSKOJ INDUSTRIJI

Diplomski rad

Filip Kraus

Osijek, 2017.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za imenovanje Povjerenstva za obranu diplomskog rada

Osijek, 21.09.2017.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu diplomskog rada

Ime i prezime studenta:	Filip Kraus
Studij, smjer:	Diplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	D 778 R, 09.10.2015.
OIB studenta:	58455550341
Mentor:	Doc.dr.sc. Mario Vranješ
Sumentor:	
Sumentor iz tvrtke:	Ivan Lovas
Predsjednik Povjerenstva:	Izv. prof. dr. sc. Marijan Herceg
Član Povjerenstva:	Doc.dr.sc. Ratko Grbić
Naslov diplomskog rada:	Analiza različitih mehanizama za licenciranje softverskih modula u automobilskoj industriji
Znanstvena grana rada:	**Obradba informacija (zn. polje računarstvo)**
Zadatak diplomskog rada:	U automobilskoj industriji upravljačke jedinice ECU (engl. Electronic Control Unit) često sadrže više različitih funkcionalnosti. Proizvođači takvih upravljačkih jedinica imaju potrebu kontrolirati distribuciju funkcionalnosti među svojim korisnicima u cilju ponude različitih varijanti istog proizvoda uz minimalne izmjene proizvodnog procesa i minimalne troškove. Predmet ovog rada je analiza različitih tehnika za licenciranje modula, kako softverskih tako i hardverskih. Također analiza obuhvaća kripto analizu ponuđenih rješenja, mogućnost upravljanja njima, ažuriranje licenci kao i cijenu implementacije. Rezultati analize trebaju pružiti uvid u prednosti i mane predloženih rješenja. (sumentor Ivan Lovas, Institut RT-RK Osijek, Cara Hadrijana 10b)
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	21.09.2017.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 25.09.2017.

Ime i prezime studenta:	Filip Kraus
Studij:	Diplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	D 778 R, 09.10.2015.
Ephorus podudaranje [%]:	1

Ovom izjavom izjavljujem da je rad pod nazivom**: Analiza različitih mehanizama za licenciranje softverskih modula u automobilskoj industriji**

izrađen pod vodstvom mentora Doc.dr.sc. Mario Vranješ

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

Razvojem elektroindustrije i programabilnih čipova dolazi doba gdje se isti uređaj može programirati s različitim radnim funkcijama ili izmjenama, ovisno o željama korisnika. Pri tome proizvođači ne žele da sve funkcionalnosti budu jednako naplaćene pa je potrebno određene funkcionalnosti dizajnirati kao modularne konstrukcije i pružati samo one koje je korisnik platio. Takav sustav djelovanja naziva se licenciranje proizvoda i vrlo često se povezuje s metodama šifriranja podataka, kako bi se održala sigurnost njegovog korištenja.

Ovim diplomskim radom obrađena je tema, u suradnji s tvrtkom „Institut RT-RK Osijek“, u sklopu koje je zadatak provesti analizu različitih mogućnosti licenciranja programskih modula prilagođenih za strojnu uporabu u automobilskoj industriji. Rad se dotiče metoda šifriranja podataka radi bolje sigurnosti i sprječavanja zlouporabe ovlasti. Analiza se provodila nad nekoliko tehnika i metoda koje mogu služiti kao sustav licenciranja uz dodatnu postavu sigurnosnih mjera šifriranjem podataka. Dakako, cilj nije samo pronaći najbolje rješenje problema, nego pronaći ono optimalno u vidu zahtjeva i procedura same tvrtke. Prilikom pronalaska i odabira najisplativije metode licenciranja uređaja treba se dizajnirati i izraditi nezavisna programska struktura, koja je spremna za daljinju uporabu kao sredstvo licenciranja određenih uređaja.

U sljedećim poglavljima se detaljnije opisuju: teorijske podloge tehnika licenciranja, detaljna analiza navedenih metoda, odabir najpovoljnijeg rješenja i sažeto objašnjene strukture potrebne za izradu ove teme.

2. PROBLEM LICENCIRANJA

U automobilskoj industriji upravljačke jedinice (engl. *Electronic Control Unit* - ECU) često sadrže više različitih funkcionalnosti. Proizvođači takvih upravljačkih jedinica imaju potrebu kontrolirati distribuciju funkcionalnosti među svojim korisnicima, a sve u cilju ponude različitih varijanti istog proizvoda uz minimalne troškove i izmjene proizvodnog procesa. Stoga je potrebno pronaći i analizirati najbolja tehnička rješenja za rješavanje problema licenciranja. U narednim se potpoglavljima prvo navode i uspoređuju različite metode pomoću kojih se rješavaju ti problemi.

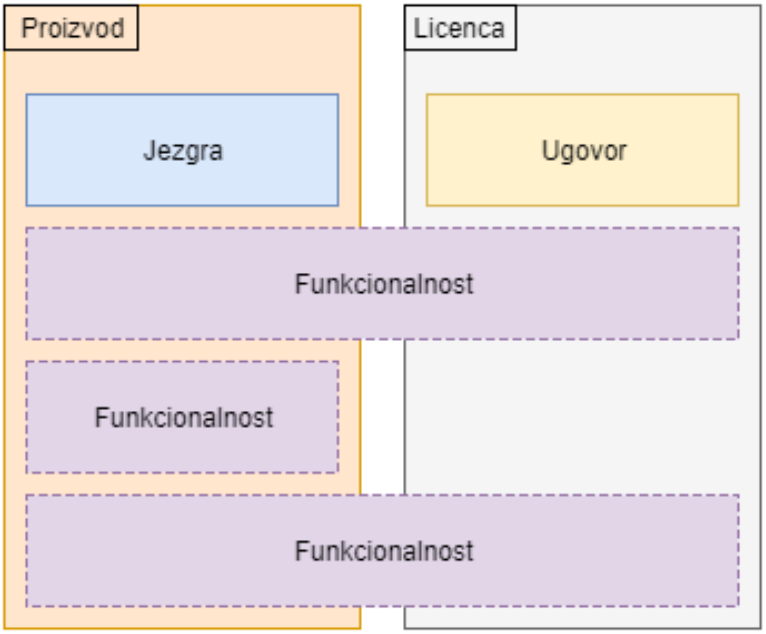
2.1. Pojam licence

Licenca je pravna dozvola za korištenje i posjedovanje usluga ili proizvoda. Dobiva se sporazumom stranke koja posjeduje licencu i stranke koja ju potražuje, putem međusobno potpisanog ugovora o pravima korištenja. Dobivenim pravima stranci se omogućuje dozvola preko licence da koristi ugovorene usluge ili proizvode. Stranke koje izdaju licence rade to kako bi omogućile drugima aktivnosti nad svojim proizvodima ili uslugama koje su inače zabranjene. Time mogu: održavati svoja prava, zahtjevati plaćanje naknade nad dijelovima ili cjelokupnim uslugama te tražiti stupanj kontrole potreban za korištenje [1].

Održavanjem svojih prava podrazumijeva se da sve uporabe bez licence stranka koja je njezin vlasnik može tretirati kao kršenje intelektualnog vlasništva i shodno tome podnijeti sudsku tužbu. Postojanje različitih licenci omogućuje fleksibilniji pristup tržištu i potrebama kupaca, npr. raspodjelom usluge na više dijelova dodatno se pridonosi zahtjevima za selektivno naplaćivanje i otvara mogućnost pretplate; pruža se prilika za postavljanje uvjeta kontrole i ograničenja ugovaranja, poput vremenskog trajanja licence, kako bi se povećala vrijednost licence, promijenili tržišni uvjeti ili osiguralo ograničenje van isteka sporazuma. Slikom 2.1. demonstriran je primjer licenciranja pojedinih funkcionalnosti proizvoda. Proizvod sadrži osnovne funkcionalnosti dostupne svima, kao i one specijalizirne, od kojih su neke, zaštićene licencom. Licenca sadrži sklopljeni ugovor o pravima i načinu korištenja odabranih funkcionalnosti.

Osim pravnog sporazuma o formiranju licence u formulu se mora uključiti i sâmo projektiranje proizvoda, pogotovo fizičkih uređaja. Problem pri licenciranju različitih funkcionalnosti uređaja jako ovisi o ograničenosti resursa, troškova i cijelom procesu njegovog nastanka: strojnoj

strukturi, programskoj strukturi, otvorenosti ili zatvorenosti rada sustava, mogućnosti daljnje nadogradnje i sl. Strojna struktura ograničena je svojim fizičkim granicama, dok programska ovisi o konstrukciji i modularnosti kôda kojeg je moguće specijalizirati kao samostalnu funkcionalnost. Međusobno povezane, vrednuju se prema otvorenosti od strane korisnika ili servisera, a s druge prema mogućnosti promjene unutar konstrukcije ili kôda, bila to nadogradnja novije verzije ili cjelokupna mogućnost povezivanja sa stranim proizvodima.



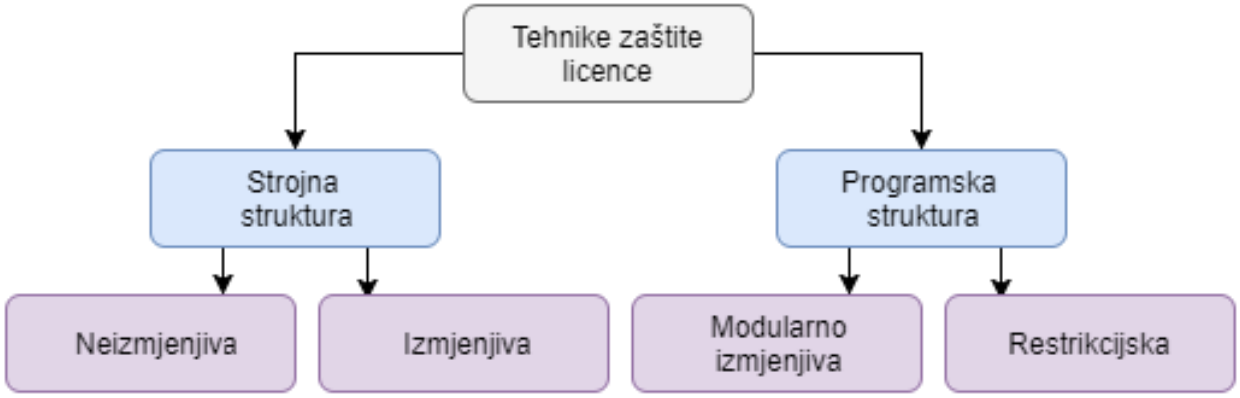
Sl. 2.1. *Primjer dodjele licence pojedinim funcionalnostima proizvoda uz dodatno ugovorene poslove.*

Navedene stavke utječu na tehnike zaštite licenci koje je važno dobro definirati. Dobro dizajnirani i modularno konstruirani uređaji imaju bolje mogućnosti provedbe licenciranja i promjene licence, što očekuje svaki proizvođač.

2.2. Tehnike zaštite licence

Zaštita licence pojam je osiguravanja zabrane nedozvoljenog korištenja aktivnosti od strane stranke koja nema ugovorenu pripadajuću licencu. Vrlo često nije dovoljno samo pravno ugovoriti i dodijeliti licencu zbog mogućih stranih upada u sustav i izmjena prava korištenja. Naravno uočavanje takvih radnji omogućuje podizanje tužbe, ali vrlo često takva lažiranja su neprimjetna i teško ih je uočiti. Stoga se prilikom dizajna uređaja treba unijeti zaštita licence.

Prvi korak prilikom odabira zaštite licenci započinje odabirom tehnike. One su temelj izrade licencnog sustava nad kojim se grade daljnje mjere. Tehnike licenciranja ovise o uređaju i korištenom programskom kôdu. Stoga se u ovoj fazi mora skupiti što više informacija o uređaju kako bi se mogla odabrati najefikasnija metoda. U ovu računicu ulaze odluke proizvođača koje su postavljene zbog ograničenosti raspoloživih resursa. Tehnike licenciranja mogu se razvrstati na strojnu i programskoj strukturu, no zbog specifičnosti zadane teme zadatka ovaj rad se više zasniva na programskoj strukturi (Sl. 2.2.).



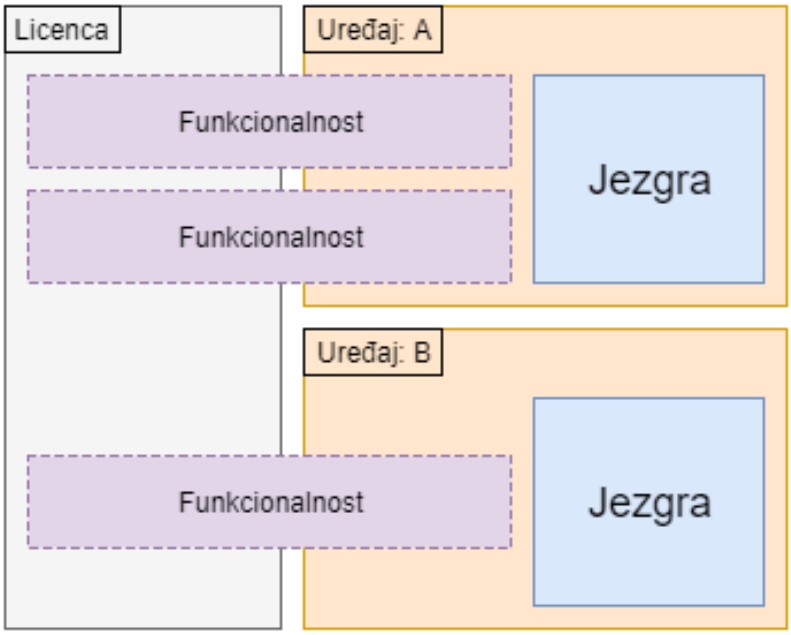
Sl. 2.2. *Raspodjela tehnika licenciranja.*

2.2.1. Strojne strukture

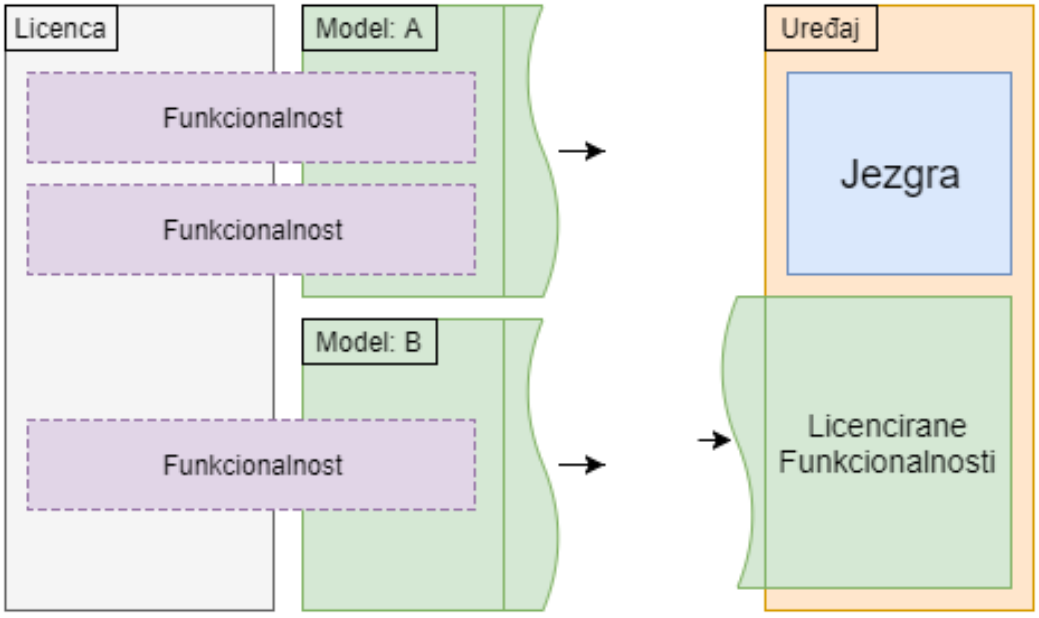
Najjednostavnija metoda strojne strukture licenciranja je specijaliziranost u smislu sklopovske nemogućnosti korištenja nelicenciranih konstrukcija na uređaju. Time se uređaji određeni za specifične licence stavljaju na tržište kao poseban proizvod i prodaju odvojeno (Sl. 2.3.). Ovakva metoda ima najbolju zaštitu licence zbog specifičnosti obavljanja samo određenih funkcionalnosti, ali najlošiju praktičnost zbog velikih troškova izrade svih verzija uređaja i odsutnosti nadogradnje uređaja ako se želi ažurirati licenca.

Druga metoda predstavlja postojanje licenciranih konstrukcija u obliku sklopovskih priključaka koji se naknadno ugrađuju na uređaj osnovnih funkcionalnosti. Uređaj posjeduje samo jezgrene funkcionalnosti rada te ih je u mogućnosti naknadno proširivati izmjenom licencnih priključaka (Sl. 2.4.). Sklopovski priključak može sadržavati jedan ili više licenciranih modula. Ovakva metoda i dalje zahtjeva poveću razinu troškova zbog izrade sklopovskih priključaka i njihovo postavljanje na tržište, no dobiva se mogućnost ažuriranja licence uređaja bez zamjene cijelog

osnovnog uređaja, odnosno zamjenom samo sklopovskog priključka, što je puno jeftinija solucija.



Sl. 2.3. *Metoda specijaliziranih uređaja - svaki uređaj posjeduje samo postavljenu funkcionalnost bez mogućnosti izmjene.*

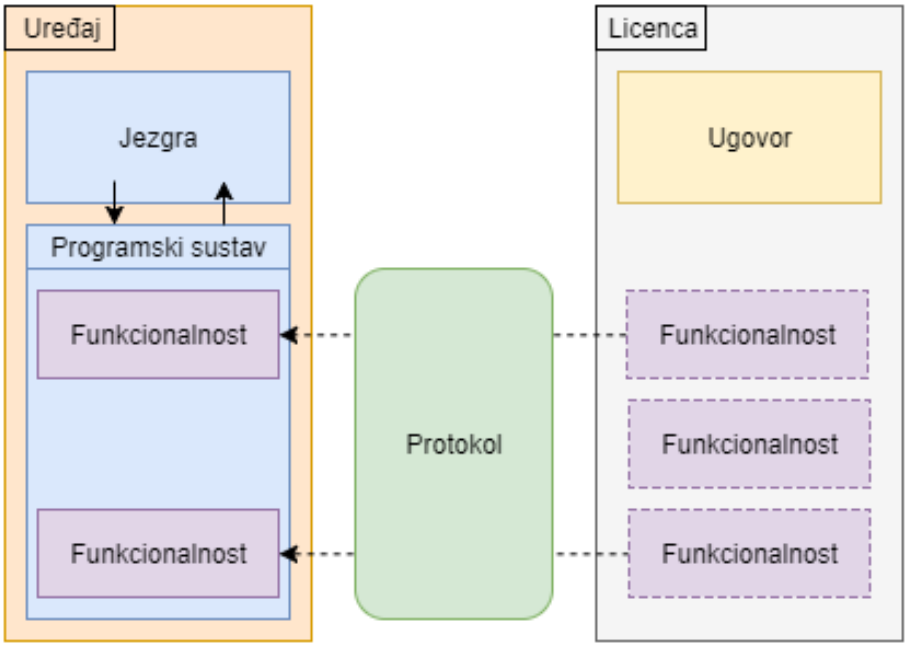


Sl. 2.4. *Metoda sklopovskih priključaka - svaki priključak posjeduje određene funkcionalnosti i samo jedan se postavlja na uređaj.*

2.2.2. Programske strukture

Spominjanjem strojnih metoda treba napomenuti da su većim strukturnim dijelom ovisne o korištenju programskih modulacija unutar samog dizajna i, pošto je programiranje modula puno jeftinije nego izrada strojnih komponenata, drugi tip metoda zaštite licence zasniva se na univerzalnoj i višenamjenskoj konstrukciji sklopovskih komponenata uređaja, gdje se programskom strukturom dizajniraju tehnike licenciranja uređaja i vrše izmjene funkcionalnosti.

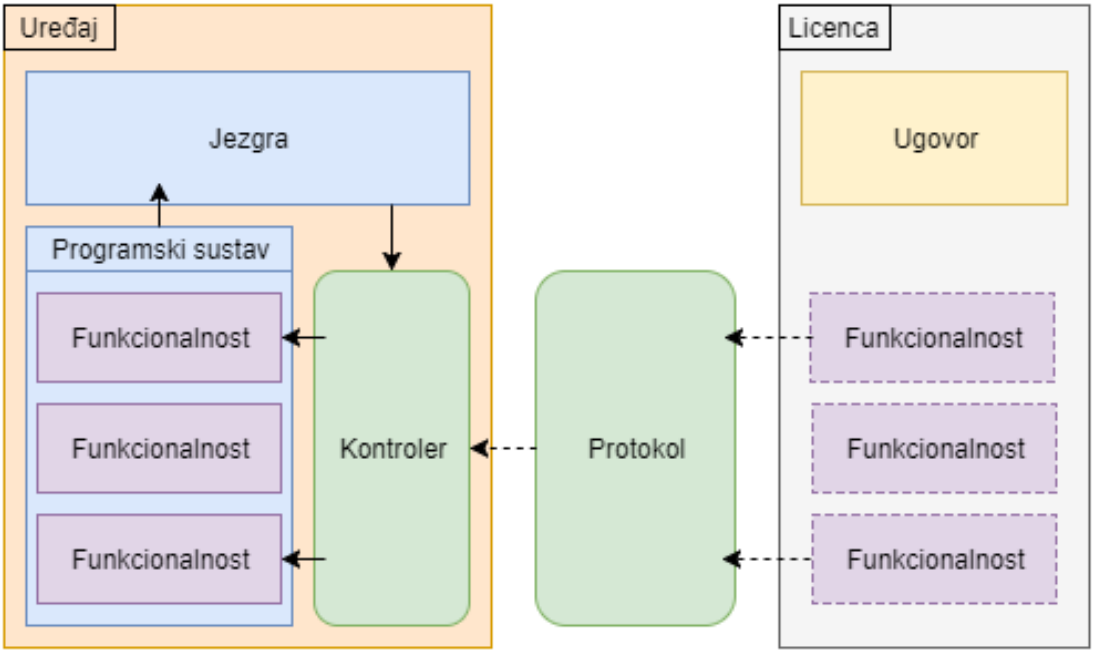
Prva metoda koristi prisutnost samo dodijeljenih programskih modula koji su dobiveni preko ažurirane licence. Programska struktura se dizajnira tako da se licence podijele na različite programske module i postavljaju u uređaj ažuriranjem preko određenih protokola (Sl. 2.5.). Ovakva metoda omogućuje dobru zaštitu licence i najefikasnija je u smislu kontrole dopuštenih prava. Jedini loš faktor predstavlja zahtijevanje puno vremena i resursa prilikom formiranja dobro dizajniranih modula, odnosno da mogu međusobno nezavisno funkcionirati. Jednom formirana struktura može omogućiti izmjenu ili ažuriranje licence uređaja s minimalnim troškovima.



Sl. 2.5. *Dodjeljivanje programskih modula ažuriranjem licence - samo se ugovorene funkcionalnosti šalju uređaju kao programski modul preko protokola.*

Druga metoda koristi ograničenje ovlasti rada nad programskim modulima uređaja preko prisutnosti licence. Uređaj sadrži kompletnu programsku strukturu sa svim licencnim modulima,

a za njihovo korištenje koristi se posebni programski kontroler koji provjerava prava ovisno o ažuriranoj licenci (Sl. 2.6.). Ažuriranje licence se vrši preko postavljenog protokola. Zaštita ovakve metode nije zagarantirana jer posjeduje sve modularne funkcionalnosti unutar samog uređaja i postoji rizik ilegalnih izmjena, no ako je sklopovska tehnologija dobro dizajnirana to će biti poprilično teško i skupo za izvesti. Ovakva metoda zahtjeva puno manje resursa za dizajn programske strukture, a time i manje troškove izrade.

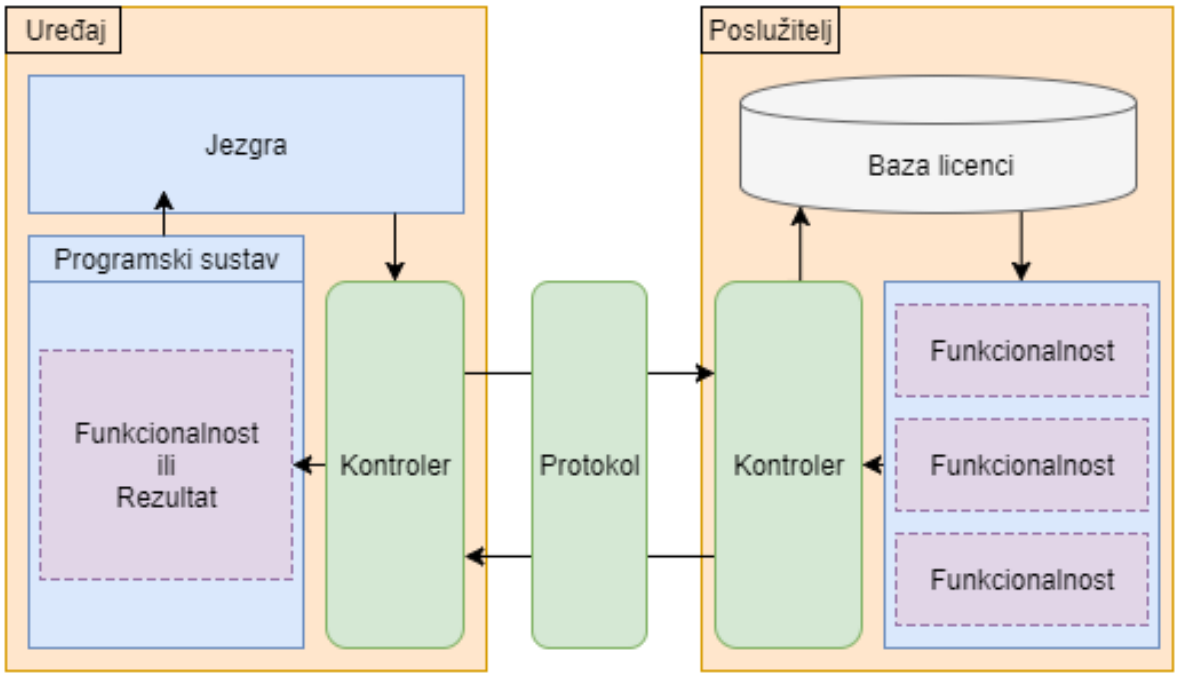


Sl. 2.6. *Ograničenje ovlasti nad programskim modulima preko kontrolera - ovisno o licenci dopuštaju se samo dozvoljene funkcionalnosti.*

Zadnji tip modulacije licence se svodi na pristup licencno odobrenim modulima preko udaljenog poslužitelja. Djeluje tako da se zahtjevani licencirani moduli mogu privremeno dobiti na korištenje, bilo da se pošalju na uređaj ili obave zadatak unutar udaljenog poslužitelja preko kontrolera unutar uređaja (Sl. 2.7.). Na kraju posla, dobiveni rezultat kontroler prosljeđuje na daljnje korištenje, a privremene nastale ostatke briše. Tako se i izbjegava zlouporaba neovlaštenih prava, no ako se želi koristiti programski modul zahtjeva se stalna veza i komunikacija s udaljenim poslužiteljem, koja zahtjeva određeni utrošak resursa za održavanje.

2.2.3. Strukture izmjene licence

Dosta veliku važnost, osim posjedovanja licence, predstavlja i potreba njene izmjene, koja se vrši preko procesa ažuriranja nakon sklopljenog novog dogovora između stranaka. Jedna od metoda protokola za izmjenu programskog modula je ažuriranje licence preko udaljenog poslužitelja, koji spajanjem na uređaj, vrši istovjetbu (engl. *identification*) vlasništva i ovjeru prava. Radi na principu prikazanom slikom 2.7. samo što se programski moduli spremaju na uređaju. Druga metoda protokola je izrada paketa s ažuriranom licencom, nakon koje se vrši slanje istog od strane proizvođača i po primitku, njegovo lokalno učitavanje na uređaj (Sl. 2.8.). Potom se vrši potvrđivanje istovjetbe vlasništva preko dobivenih podataka iz paketa. Zadovoljavanjem svih uvjeta preko bilo kojeg protokola odobrava se provođenje ažuriranja licence i omogućava korištenje njezinih novih funkcionalnosti.

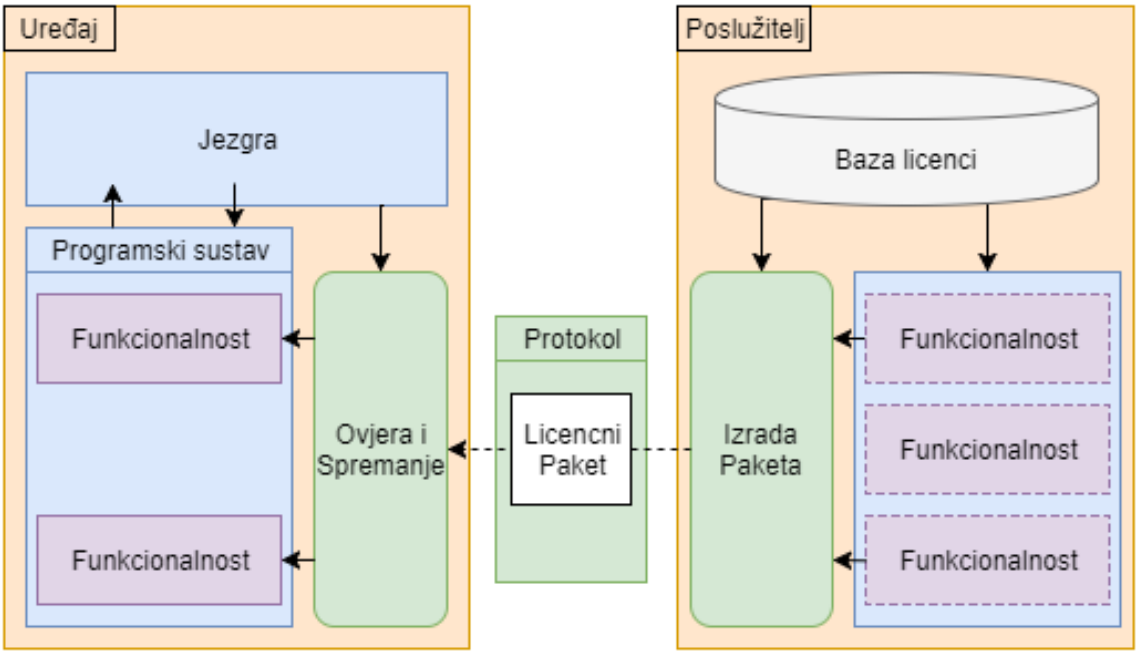


Sl. 2.7. *Obavljanje funkcionalnosti preko udaljenog poslužitelja.*

2.2.4. Usporedna analiza struktura

Usporedbom strojne i programske strukture licenciranja može se zaključiti da obje imaju prednosti i mane, a odabir ovisi o najisplativijoj soluciji tvrtke koja ih postavlja. Strojne strukture zahtijevaju veće troškove ulaganja u tržište, dok programske strukture traže više raspoloživog

vremena utrošenog u modularnost i zaštitu kôda. Zbog kompleksne građe modernih sklopovlja uređaja dosta je teško i nepraktično izložiti ga neželjenim napadima i analiziranjima, no uz to treba naglasiti da se programska struktura unutar njega treba što više ograničiti na korištenje samo-iščitne memorije (engl. *Read Only Memory* - ROM), kako bi se zabranilo neovlašteno korištenje poput izmjene algoritama ili postavki lažnih prava. Zatim treba spomenuti da se na odluku odabira strukture licenciranja trebaju nadovezati daljnji sustavi zaštite poput tehnike šifriranja ili sigurnosti kroz nejasnoću podataka.



Sl. 2.8. *Ažuriranje licence preko paketa - točnom se ovjerom licencne datoteke odobravaju nove funkcionalnosti.*

2.2.5. Sigurnost kroz nejasnoću podataka

Sigurnost kroz nejasnoću podataka (engl. *security through obscurity*) oslanjanje je na sigurnost preko tajnosti dizajna. Koristi se kao sustav zasnovan na nejasnoćama ili metodama koje bi uvodile nedostatke u procesu napada i time sprječavale uspješnost izmjene prema [2]. U praksi ovakva metoda ima ozbiljne sigurnosne propuste ako se otkrije sustav rada, no dobrom osiguranom strukturom sučelja može se dovoljno dobro čuvati tajnost dizajna.

2.3. Tehnike šifriranja licence

Tehnike šifriranja procesi su kôdiranja poruke ili informacije tako da samo ovlaštene stranke mogu njima pristupiti. Zasnovane su na procesima koji ne blokiraju neželjene promatrače, nego im onemogućuju logičku interpretaciju poruke prilikom čitanja. Logika procesa djeluje tako da se informacija, definirana kao čisti tekst (engl. *plaintext*), korištenjem standardnih algoritama i specifičnog ključa šifrira u šifrirani tekst (engl. *ciphertext*) i samo se tim ključem može dešifrirati nazad. Ključ je jedinstveni niz podataka točno određene duljune i, zbog tehničkih razloga, algoritam obično stvori vlastiti nasumično generirani ključ koji se onda koristi u daljnjim šifriranjima traženih poruka ili informacija. Algoritmi su opće poznati, a ključevi nisu te samo jedan od njih odgovara za razmjenu informacija unutar jednog kanala šifrirane komunikacije [3].

Postoje brojni algoritmi koji koriste tehnike šifriranja, a zajedno se mogu svrstati u dvije kategorije: šifriranje simetričnim ključem i šifriranje javnim ključem. Šifriranje javnim ključem se još razdvaja na digitalni potpis i sigurnosnu razmjenu ključeva.

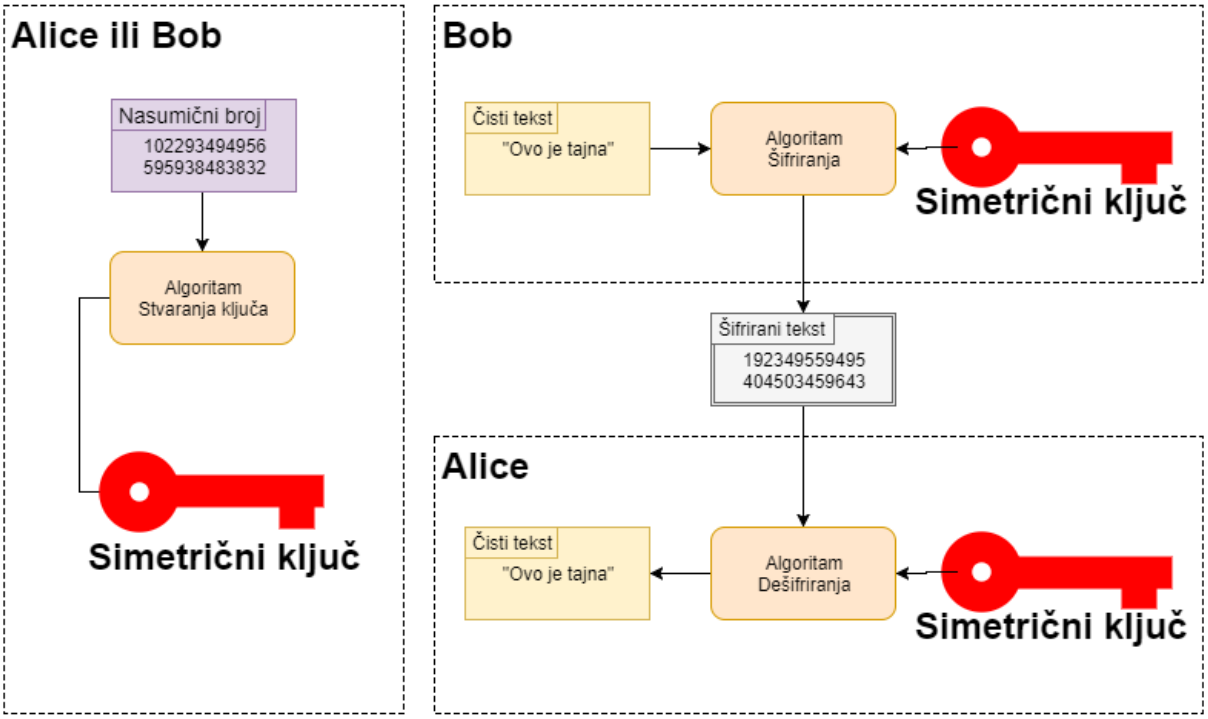
2.3.1. Algoritmi šifriranja simetričnim ključem

Algoritmi šifriranja simetričnim ključem koriste isti ključ za šifriranje čistog teksta i dešifriranje šifriranog teksta. Ključ se tretira kao zajednička tajna između dviju stranaka kako bi imali privatan protok informacija. Demonstriranjem preko slike 2.9. vidi se izmjena informacija između stranaka Alice i Boba, gdje oboje mogu stvoriti ili koristiti simetričan ključ. Bob šifrira poruku simetričnim ključem i šalje šifrirani tekst Alicei koja samo istim simetričnim ključem može pročitati poruku. Proces se može obrnuti i obje strane su na jednakoj razini vrijednosti, stoga se metoda ne može koristiti u sustavu poslužitelj-korisnik.

Standard šifriranja podataka (engl. *Data Encryption Standard* - DES) jedan je od prvih algoritama za simetrično šifriranje korišten u Sjedinjenim Američkim Državama. Dobrog je izvođenja, ali danas odbačenog zbog problema kratkog ključa koji se može brzo probiti uporabom grube sile računanja (engl. *brute force*) čime se, kao standard, počelo za testiranje dobrog algoritama gledati: mogućnosti sprječavanja probijanje njegovih ključeva i brzina izvođenja [4].

Blowfish je jedan od alternativa zastarjelom DES-u. Dizajniran od Bruce Schneiera, postavljen je u javnu domenu i otvoren svima na korištenje. Značajno poboljšanje njegovih značajki šifriranja je korištenje, o ključu ovisnih, zamjenskih blokova informacija i vrlo složenog

rasporeda ključa kojim se ojačava sigurnost šifrirane poruke i ključa. Nažalost napretkom tehnologije i brzine obrade informacija ovaj algoritam je postao nesiguran te ga je zamijenio njegov nasljednik Twofish [5].



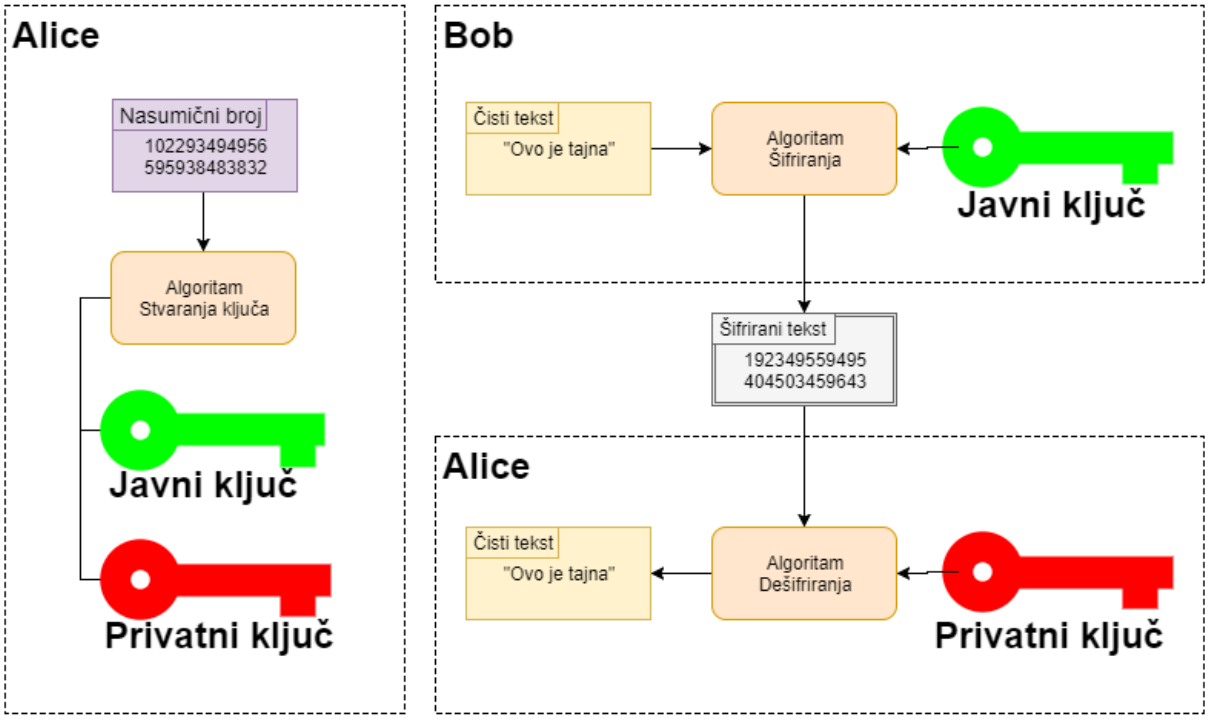
Sl. 2.9. *Proces šifriranja simetričnim ključem - Bob i Alice mogu zamijeniti mjesta.*

Usporedno prethodnom algoritmu razvija se popularniji i raširenији algoritam zvan Standard naprednog šifriranja (engl. *Advanced Encryption Standard* - AES). Osnovan od strane američkog Nacionalnog Instituta za Standarde i Tehnologiju (engl. *National Institute of Standards and Technology* - NIST), AES koristi šire zamjenske blokove informacija kao i duljune ključeva te se danas podrazumijeva kao jedan on najboljih simetričnih algoritama šifriranja. Trenutno se koristi kao državni standard pošto se dosad njegova najdulja sekvenca nije uspjela probiti uporabom grube sile računanja. AES za potrebe rada dobro djeluje na širokoj paleti sučelja i ne zahtjeva velike računalne resurse [6].

2.3.2. Algoritmi šifriranja javnim ključem

Algoritmi šifriranja javnim ključem stvaraju dva odvojena jedinstvena ključa koji djeluju tako da se s jednim samo šifriraju informacije, a s drugim samo dešifriraju. Privatni ključ zna samo vlasnik i služi za dešifriranje i ovjeru informacija, dok je javni ključ otvoren javnosti i svatko ga

može koristiti za šifriranje informacija koje onda vlasnik privatnog ključa dešifrira. Ovakav sustav može se koristiti u sustavu poslužitelj-korisnik i demonstriran je slikom 2.10.



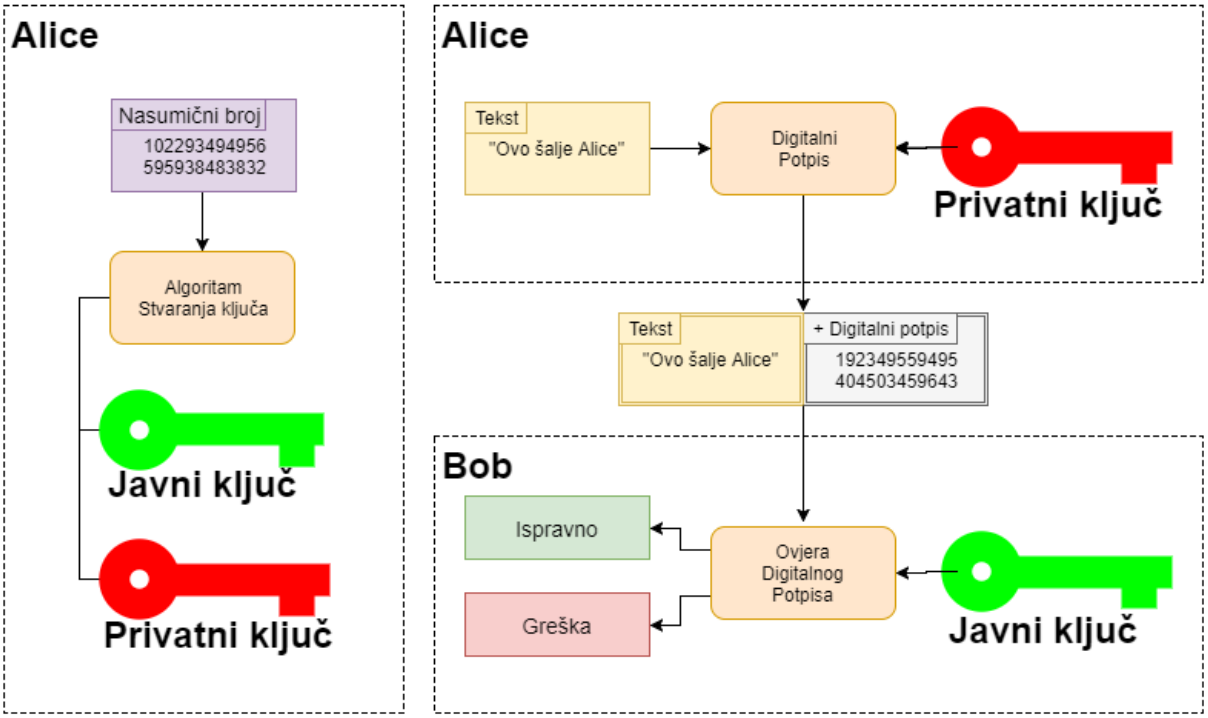
Sl. 2.10. *Proces šifriranja javnim ključem - samo Alice može dešifrirati poruke.*

Stranka Alice generira ključeve radi komuniciranja sa svojim suradnicima, u ovom slučaju s Bobom. Za generiranje ključa potreban je nasumičan velik broj kojim se stvara javni i privatni ključ. Javni ključ se prikazuje javnosti dok se privatni drži u tajnosti. U ovakvoj strukturi svi mogu šifrirati informacije javnim ključem, a samo ih privatni ključ može dešifrirati. Tako da Bob šifrira poruku preko Aliceinog javnog ključa i šalje šifriran tekst Alicei, gdje ga ona dešifrira putem svoga privatnog ključa i dobiva čisti tekst. Za dvosmjernu komunikaciju svatko radi svoj par ključeva i vrši se ista procedura.

RSA, dizajniran i nazvan po prezimenima Rona Rivesta, Adi Shamira i Leonarda Adlemana, jedan je od prvih algoritama javnih ključeva i ostao je među najboljim algoritmima današnjice. Prvobitno patentiran proizvod, istekom prava stavljen je u javnu domenu. Stvaranje ključeva radi se na bazi praktične težine faktoriziranja dva velika prosta broja, a time ti brojevi moraju biti skriveni od javnosti, inače se gubi sigurnost toga ključa. Zaštitom vrlo siguran, ali metodom deterministčan, algoritam je tijekom vremena morao uvesti dodatne tehnike nasumičnih dopuna

tekstu zbog njihovih sigurnosnih proboja usmjerenim napadima na isti šifriran tekst. Time je osigurao značbenu (engl. *semantic*) sigurnost. U pitanju rada kao algoritam šifriranja, RSA je relativno spor i ne koristi se izravno za šifriranje informacija, nego kao posrednik za izmjenu simetričnih ključeva koji su sa svojim algoritmima puno brži. Također se koristiti kao metoda digitalnog zapisa koja je opisana daljnje u tekstu [7].

Šifriranje eliptičnom krivuljom (engl. *Elliptic Curve Cryptography* - ECC) pristup je šifriranju javnim ključem baziran na algebarskoj strukturi eliptičnih krivulja nad konačnim poljima. Postoje razni algoritmi korištenja ove metode, a zaštita je zasnivana na nepovratnošti određenih matematičkih problema, gdje su oni u teoriji rješivi, ali u praksi zahtjevaju ogromne količine resursa i vremena, stoga su neisplativi. Veličinom ključa je znatno manji spram RSA, ali jednako toliko siguran za klasične probojne napade grubom silom računanja [8].



Sl. 2.11. *Proces digitalnog potpisa nad porukom - Bob ovjerava istovjetbu Aliceine poruke.*

2.3.3. Digitalni potpis

Digitalni potpis je proširenje algoritma šifriranja javnim ključem s razlikom u načinu prezentacije, gdje se uloge ključeva okreću. To je matematička metoda za ovjeravanje informacija preko dokaza, odnosno potpisa, koji pošiljateljska stranka šalje uz informaciju kao

potvrdu svoje istovjetbe vlasništva. Demonstrirano slikom 2.11. algoritam radi tako da privatnim ključem stvara digitalni potpis preko metode raspršbe (engl. *hash*) informacija ujedno s nasumičnom dopunom tekstu i time sve ostale stranke mogu potvrditi njezinu istovjetbu preko odgovarajućeg javnog ključa [9].

2.3.4. Tehnike sigurnosne razmjene ključeva

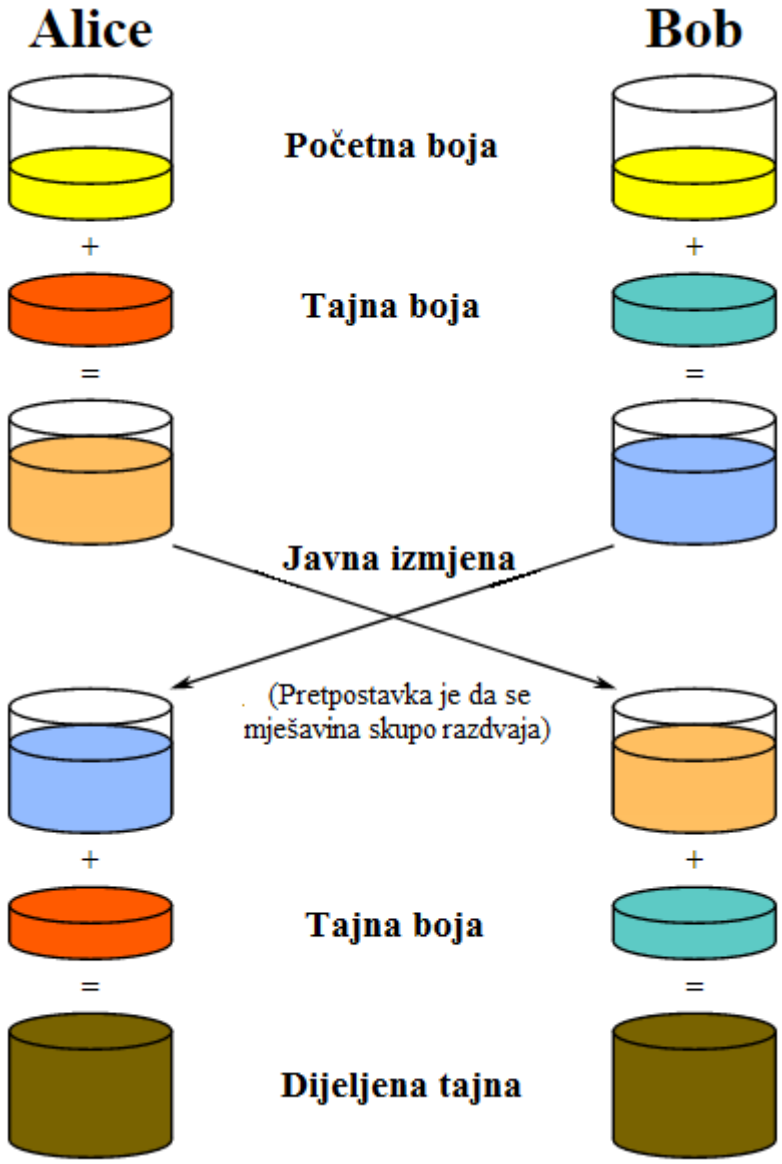
Tehnike sigurnosne razmjene ključeva postoje jer je razmjena ključeva najrizičniji proces prilikom otvaranja kanala šifrirane komunikacije. Glavni problem ne predstavlja probijanje zaštite šifriranog teksta, nego nesigurnost prilikom razmjene ključeva, poput moguće krađe od stranih promatrača ili upitne sigurnosti u istovjetbu pravog vlasnika. Zbog toga su osmišljene tehnike sigurne razmjene ključeva bilo koje vrste, da bi se nakon izmjene sigurno i nesmetano mogli koristiti postavljeni algoritmi zaštite informacija.

Diffle-Hellman razmjena ključeva (engl. *Diffie–Hellman key exchange* – DH) prvi je protokol sigurnosne razmjene ključeva, izvorno koncipiran od Ralpha Merkelea, dobio je ime po njegovim mentorima Whitfieldu Diffieu i Martinu Hellmanu. Proces počinje postojanjem dviju stranaka, u primjeru nazvanih Alice i Bob, koji razmjenjuju ključeve koristeći simboliku miješanja boja (Sl. 2.12).

Obje stranke se dogovore za početnu boju koja ne mora biti tajna, ali bi trebala biti različita prilikom svakog dogovora. U ovom primjeru to je žuta boja. Tada svatko od njih pridoda tajnu boju koju čuvaju za sebe u mješavinu boja i tu mješavinu međusobno izmjene. Pri tome u dobivenu mješavinu dodaju svoju tajnu boju i rezultat koriste kao dijeljenu tajnu. Krajnja boja simbolizira dijeljeni simetrični ključ za korištenje. Ovakva metoda ispunjava svoja očekivanja samo ako se tajni ključevi nasumično generiraju prilikom svake izmjene, što su unijele kasnije nadogradnje algoritma [10].

Tijekom vremena uočeno je da *Diffle-Hellman* razmjena ključeva ima jedan problem, potvrdu prave istovjetbe vlasnika. Tu je nakon godina pristupila metoda infrastrukture javnih ključeva (engl. *Public Key Infrastructure* - PKI). Djeluje kao skup uloga, stavki i procedura potrebnih da se stvore, upravljaju i distribuiraju javni ključevi. Infrastruktura javnih ključeva služi kao povjerljiva treća strana koja potvrđuje istovjetbu stranaka željnih uključiti se u sigurnosnu komunikaciju. Posao obavlja izdavanjem digitalnih certifikata i stvaranjem kanala šifrirane komunikacije među njima. Stranke potvrđuju svoje istovjetbe digitalnim potpisom i time se cijeli

proces, u našem slučaju zaštita licenci, potpuno osigurava. Jedini problemi ove metode su financijski tereti pretplate i moguće upletanja države u kontrolu toka certifikata [11].



Sl. 2.12. *Proces Diffie–Hellman razmjene ključeva [12].*

2.4. Poslije-kvantno doba zaštite šifriranja

Dosad navedenim klasičnim problemima sigurnosti šifriranja informacija kao što su proboj uporabom grube sile računanja, iskorištavanje determinizma algoritama, lažno predstavljanje ili prisluškivanje razmjene ključeva, stalo se na kraj raznim metodama i doradama postojećih algoritama. Tehnologija se konstantno razvija i sve većom uporabom kvantnih računala

omogućilo se znatno brže korištenje metoda proboja zaštite poput Shorovog algoritma [13]. Takvo razdoblje se nazva poslije-kvantno doba zaštite šifriranja informacija i potrebno je razvijanje boljih mjera zaštite šifriranja.

Za simetrične algoritme stvaranja ključeva poput AES-a utvrđeno je da nisu toliko skloni probojima preko kvantnih napada. No problem predstavljaju algoritmi javnih ključeva. ECC koji je prikazan kao efikasniji algoritam prilikom klasičnih napada, znatno se pokazao lošijim spram onih kvantnih i to čak lošiji od njegovog sporijeg konkurenta RSA. Zahvaljujući modernijim unapređenjima ECC metode kao odgovor dolazi poslije-kvantni, super-singularni i *isogenezni Diffle-Hellman* algoritam sigurnosne razmijene ključeva (engl. *Supersingular Isogeny Diffie–Hellman key exchange* - SIDH). Zasnovan na *Diffle-Hellman* razmjeni ključeva, ali izmijenjen za obranu od kvantnih napada preko dvije super-singularne eliptične krivulje, koristi najmanju duljinu ključa naprem ostalih post-kvantnih algoritama i pruža veliku sigurnost komunikacije [14].

2.5. Tehnologije izrade programskog modula

Pisanje programskog kôda sustava za licenciranje obavljeno je preko C programskog jezika u obliku programske biblioteke s prezentiranim modulima strukture kao funkcijama jednostavnim za korištenje. Odabrani jezik korišten je zbog predodređenog dogovora s tvrtkom partnerom u koju ulazi i njegova mogućnost korištenja na operacijskim sustavima Linux i Microsoft Windows. Uz dodatno priređene programske biblioteke tehnika šifriranja otvorenog kôda, sve je spremno za razvoj programskog sustava licenciranja i osposobljavanja programskog modula za ugradnju u ostale sustave.

C programski jezik je višenamjenski proceduralni programski jezik, razvijen od Dennisa Ritchiea, koji podržava strukturno programiranje, rekurzije i ostale operacije. Tada namijenjen za ponovnu izgradnju Unix operacijskog sustava, danas je jedan od najšire korištenih programskih jezika zbog svoje robusnosti, fleksibilnosti i pouzdanosti kod kôdiranja [15].

Za obavljanje tehnika šifriranja korištena je LibTomCrypt programska biblioteka otvorenog kôda, razvijena od Toma St Denisa [16]. Korištena je kao dodatna biblioteka koja svojim metodama omogućava jednostavno korištenje potrebnih algoritama šifriranja i uvelike olakšava ostvarivanje ovoga zadatka.

3. ANALIZA TEHNIKA ZAŠTITE LICENCE I ODABIR SUSTAVA

Završenom strukturnom raspodjelom i analizom tehnika zaštite licence i šifriranja može se krenuti u proces formiranja sustava usluge licenciranja preko međusobnog rukovanja različitim metodama. Ovdje će se sustavi razvrstati na nekoliko slijednih faza procesa, a pošto su strojna sklopovlja zatvorene strukture i specifikacijama ovog zadatka već prilagođeni programskoj strukturi, za njih će se samo spomenuti potrebne mjere osiguranja. Nakon raspodjele sustava treba se, ovisno o specifikacijama, odabrati i dizajnirati najpovoljniji modularni sustav spreman za daljnju ugradnju unutar programskog sustava licenciranja.

3.1. Analiza i formiranje struktura

Korištenjem strojnih metoda može se u potpunosti ostvariti sigurnost licence zbog fizičke odsutnosti ostalih licencnih modula. Tehnologije sklopovlja, ako nisu višenamjensko programabilne, štite se od neovlaštenih izmjena svojom nepristupačnošću i spremanjem unutar ROM-a, a daljnju sigurnost očuvanja tajne komercijalnih algoritama tvrtke mogu pružati metodama šifriranja simetričnim ključem.

Tako navedenim metodama, jedini neovlašteni pristup licencama predstavlja ilegalno nabavljanje neslužbenih komponenti uređaja i umetanje u sklopovlje. Pritom se sustav može zaštititi preko programabilne strukture digitalnog zapisa ili njene strojne alternative u smislu specifične arhitekture koju prihvaćaju samo određena sučelja. Svakom dodatnom mjerom sigurnosti javlja se rizik smanjenja efektivnog rada uređaja te raste broj utrošenih resursa i vremena pa se mora odrediti granica prihvatljive sigurnosti.

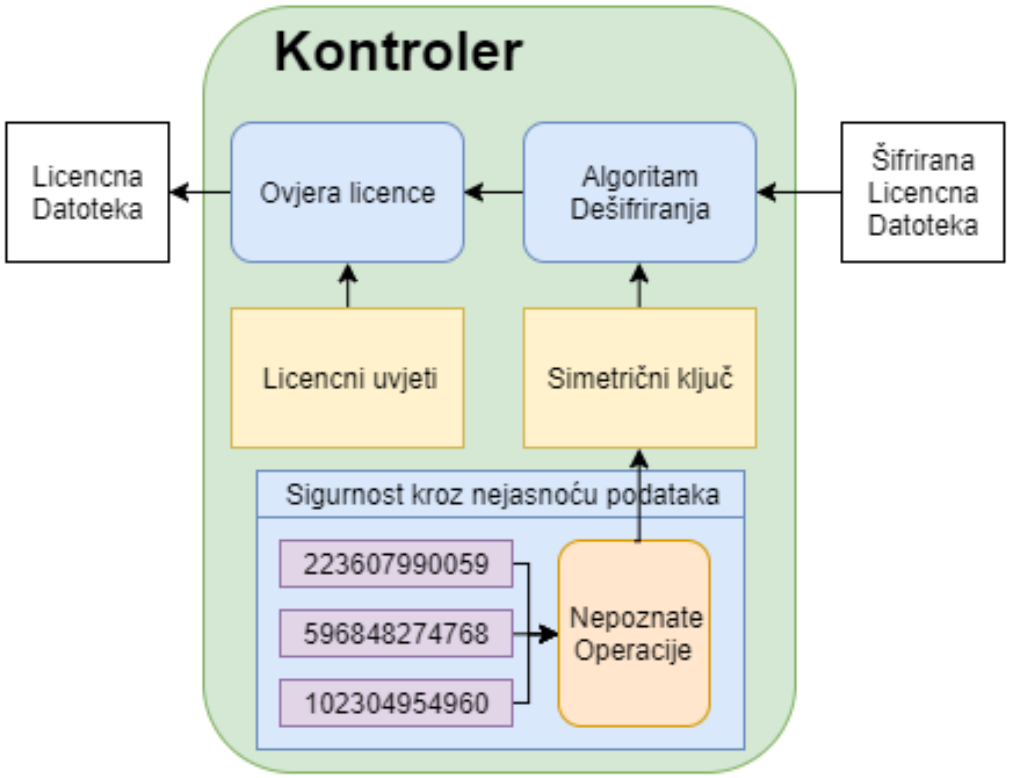
Za sklopovlja s višenamjenskom strukturom također vrijede gore navedene stavke, no ta se sklopovlja više zasnivaju na programabilnim metodama rješavanja problema sigurnosti, navedenim u sljedećem poglavlju, nego potencijalnim nesigurnostima sa strojne strane zbog prisustva ili moguće neovlaštene izmjene svih licencnih modula na njemu.

3.1.1. Metode izmjene licence

Prilikom dodjele licence ili pri komunikaciji programskom strukturom preko višenamjenskih programabilnih sklopova, prvobitno je važno osigurati sigurnost razgovora između korisničkog uređaja i proizvođača koji postavlja licence. Komunikaciju uređaja i proizvođača obavlja kontroler. Neovisno o tehnici zaštite licence ili protokola za potvrdu istovjetbe vlasništva

stranaka, najsigurnije bi bile tehnike sigurnosne razmjene ključeva, objašnjeno u potpoglavlju 2.3.4., no ako su takve metode neisplative, potrebno je osmisliti drugačije sustave dosljednih mogućnosti.

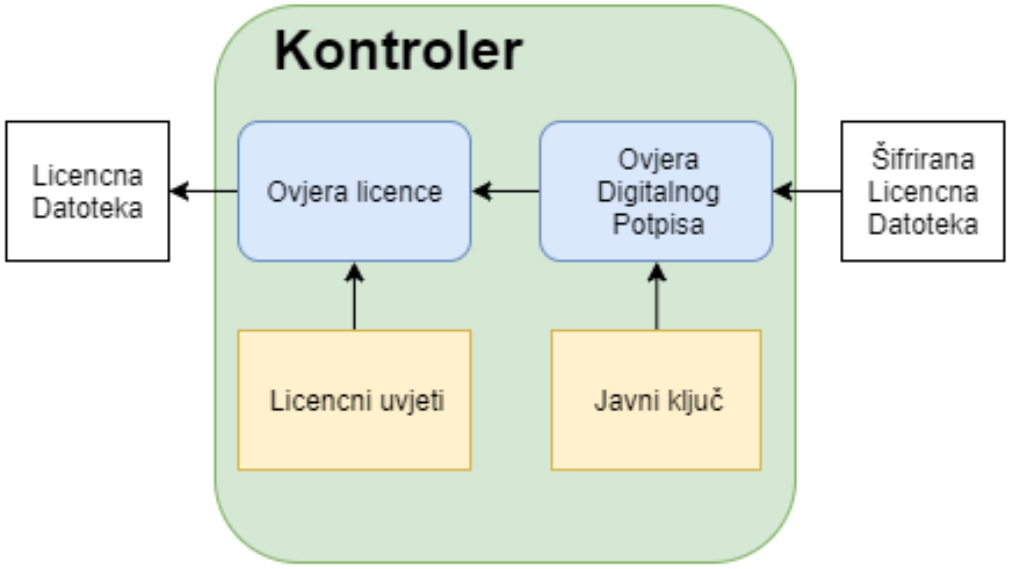
Prva formirana metoda je korištenje tehnike šifriranja simetričnim ključem, gdje se ključ pomoću sigurnosti kroz nejasnoću podataka prikriva od zlouporabe unutar uređaja. Ključ se može prikriti raznim metodama poput definiranja više manjih ključeva i vršenjem logičkih operacija nad njima da se dobije pravi ključ (Sl. 3.1.), no, kako je spomenuto u metodi, jednom otkriveni postupak ugrožava njegovu sigurnost i omogućava neovlašteno korištenje. Prilikom prihvaćanja šifrirane licence moguće ju je pročitati, potvrditi i postaviti kao zadanu. U praksi se ovakav proboj sigurnosti vjerojatno neće dogoditi zbog zatvorenosti strukture sklopovlja i neisplativosti rastavljanja, no ta mogućnost i dalje postoji.



Sl. 3.1. *Ažuriranje licence preko sigurnosti kroz nejasnoću podataka i ovjera licencnih podataka.*

Druga formirana metoda je korištenje digitalnog potpisa preko tehnike šifriranja javnim ključem. Proizvođač tajnim ključem generira digitalni potpis licence kao garanciju da ju on šalje te pritom licencu dostavlja korisniku. U uređaj korisnika postavlja se javni ključ koji može, ali ne mora biti

vezan za njega i njime se može potvrditi istovjetba vlasništva prilikom prihvaćanja licence putem provjere digitalnog potpisa (Sl. 3.2.). Ovakav sustav osigurava sigurnost ažuriranja licence, ako se dogodi neovlašteno korištenje, jer bilo kakvom promjenom ključa, licence ili digitalnog potpisa algoritam rezultira greškom. Želi li se očuvati tajnost informacija licence na sustavu, mogu se postaviti daljnje mjere zaštite poput šifriranja simetričnim ključem i sl.



Sl. 3.2. *Ažuriranje licence preko digitalnog potpisa i ovjera licencnih podataka.*

3.1.2. Metode provođenja licence

Ugovorenom licencom, njezinim ažuriranjem i odobrenim licencnim modulima dovoljno su mali rizici proboja sigurnosti te se stvar može prepustiti stroju i njegovoj sposobnosti zaštite programabilnih modula. Ovdje se može predložiti par smjernica, a potrebno je postaviti samo neke uvjete koji osiguravaju slanja obavijesti sustavu o postojećoj licenci. Osim zaštite uređaja od neovlaštenih izmjena licence, može se bolje zaštititi korištenjem dodatnih metoda poput: šifriranja simetričnim ključem, prikrivanja kroz sigurnost nejasnoće podataka ili provjere istovjetbe digitalnim potpisom prije njenog izlistanja.

Obje metode se mogu nadovezati na one objašnjene u prethodnom poglavlju i preporučuje se korištenje istog tipa metoda pri preuzimanju i korištenju licence unutar uređaja radi manjeg trošenja resursa. Metodom simetričnog ključa licenca se šifrira ključem i može se očitati samo istim prilikom legalne potražnje. Metodom digitalnog potpisa uz licencu se veže njen specifični

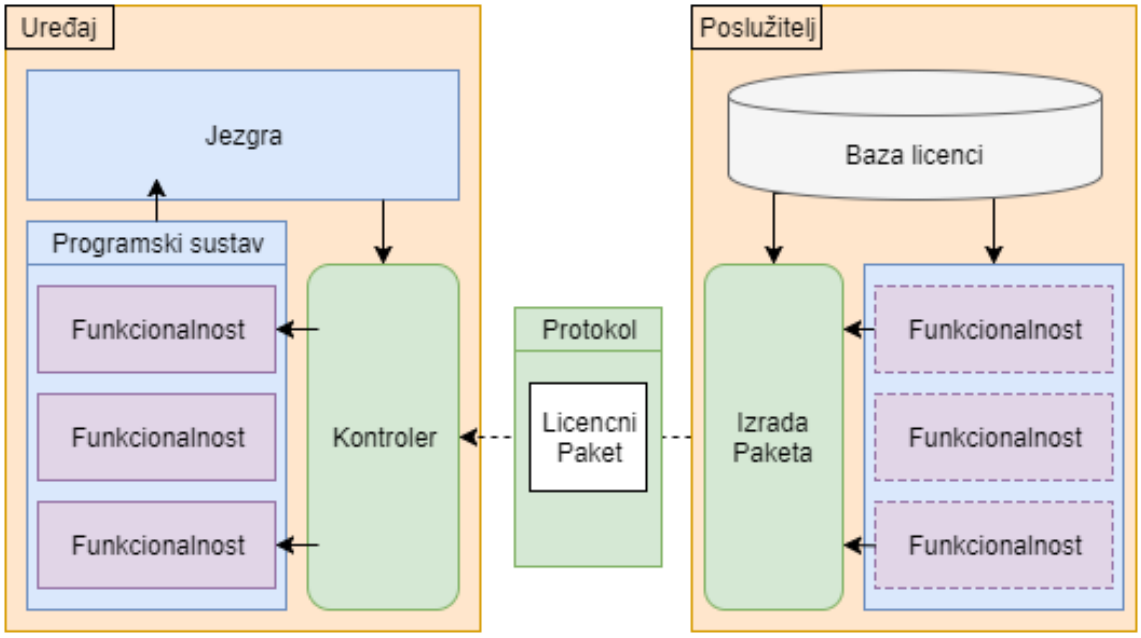
potpis i samo se ovjerom svih potrebnih elemenata može potvrditi njezina točnost. Licenca se po želji može dodatno prikriti metodom simetričnog ključa.

Za pristup licencnim modulima preko udaljenog poslužitelja nije potreban takav pristup zbog obrade podataka u sigurnosnim uvjetima koje pruža udaljeni poslužitelj. Potrebno je samo provesti sigurnost komunikacije preko navedenih metoda.

3.2. Odabir sustava ovisno o zadanim specifikacijama

Budući da je za zadani zadatak već pokrenut proces izgradnje programskog kôda i postavljene su specifikacije dizajna uređaja, daljnjim dogovaranjem s tvrtkom partnerom odabrane su najpovoljnije tehnike licenciranja, uzimajući u obzir postavljene zahtjeve i raspoložive resurse.

Zbog korištenja opširnih funkcionalnosti koje uređaj treba obavljati za strojnu strukturu koristi se univerzalno, višenamjensko sklopovlje i većinski se vrši preko programabilnih modula. Zbog velike složenosti programskog kôda, licencne module nije moguće formirati bez dodatnog trošenja vremena i resursa. Stoga se koristi model ograničenja ovlasti rada nad programskim modulima uređaja i priprema se dizajn pomoćnog programa kontrole licenci (Sl. 3.3.).



Sl. 3.3. *Odabrani sustav za licenciranje proizvoda - proizvođač radi licencni paket s digitalnim potpisom koji uređaj, preko kontrolera, ovjerava i koristi.*

Licenciranje je potrebno izvršavati preko predaje datoteke, imenovane „*lic.dat*“, koju proizvođač stvara preko istovjetbe broja ciljanog uređaja, datuma trajanja licence i ugovorenih prava korištenja licencnih modula. Datoteku treba zaštititi univerzalnim ključem šifriranja te postaviti u uređaj prilikom prodaje ili poslati korisniku da je sam ažurira preko uređaja. Svi uređaji koriste isti ključ, a metoda šifriranja prvobitno se definirala preko sigurnosti kroz nejasnoću podataka, no daljnjim dogovorima ustanovilo se da je isplativije koristiti metodu digitalnog potpisa.

Ovim se dobiva uvid u izradu plana sustava kojim se odmah može zaključiti da uzima optimalnu soluciju načina licenciranja bez velikih troškova izrade te je zasnovan na tehnikama šifriranja globalnog standarda.

3.3. Dizajn modularnog sustava

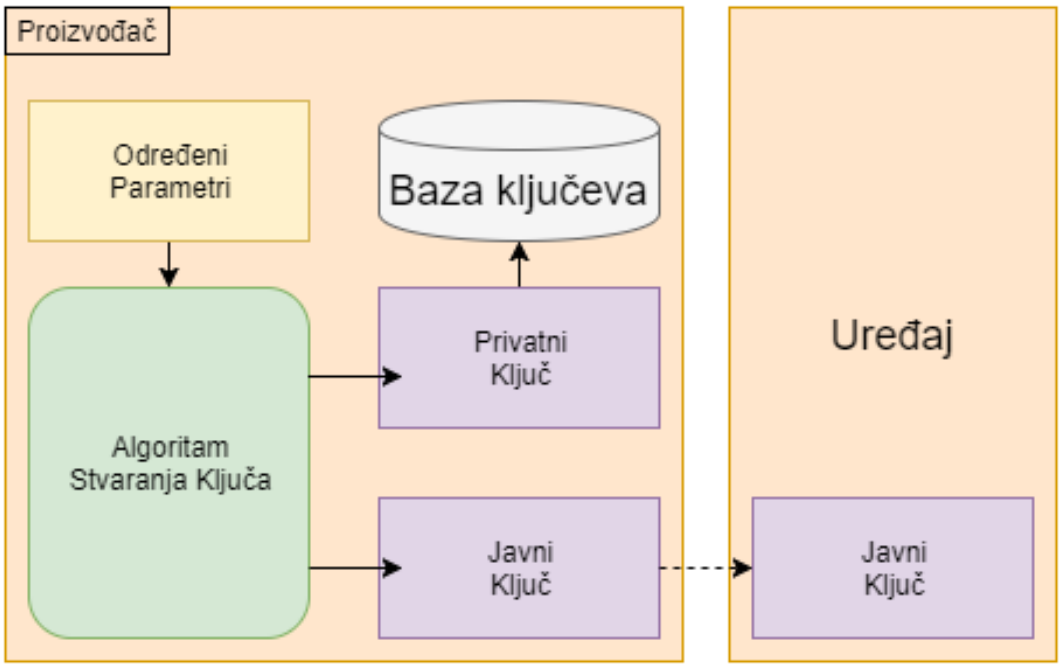
Nakon postavljenih specifikacija zadatka počinje se s planom izrade licencnog sustava koji se razvrstava na manje modularne cjeline: modul za stvaranje ključa, modul za izradu licence, modul za postavljanje licence te modul za potvrđivanje i pružanje licence. Da bi moduli mogli međusobno komunicirati i obavještavati uređaj, postavljene su univerzalne strukture označavanja vrijednosti i povratnih informacija. Dalje u tekstu se objašnjava dizajn modula.

3.3.1. Modul stvaranja ključa

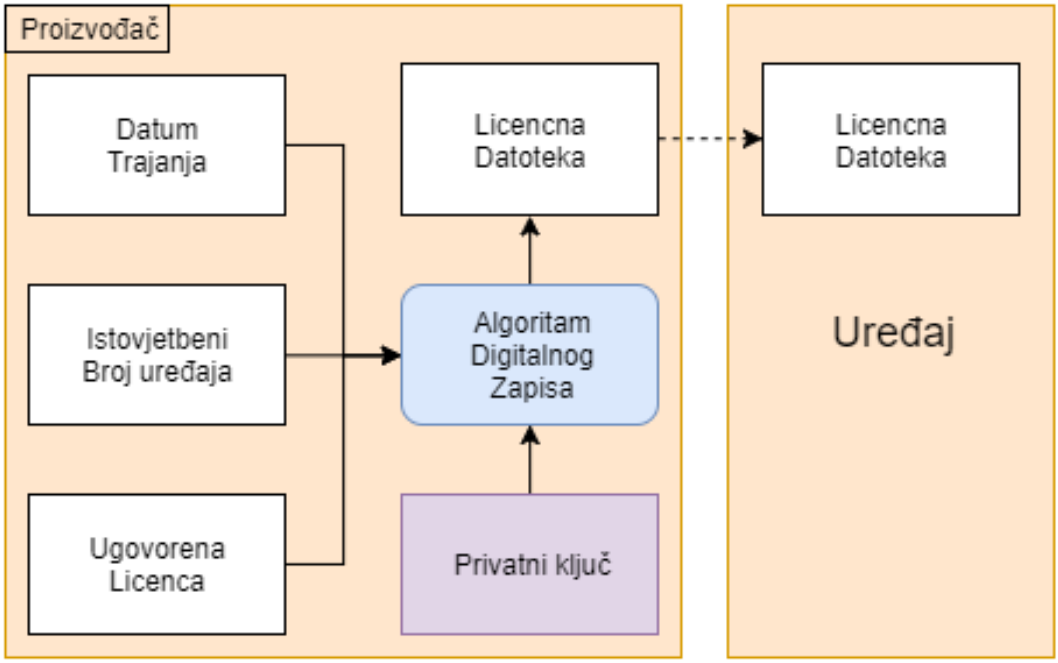
Modul za stvaranje ključa neobavezan je dio koji se može upotrebljavati za stvaranje ključeva postavljene tehnike šifriranja ili se umjesto njega mogu koristiti druga sredstva iste namjene. Ovaj modul koristi potrebne algoritme za stvaranje privatnog i javnog ključa s određenim granicama, postavljenim prema specifikacijama dizajna te ih daje na korištenje (Sl. 3.4.).

3.3.2. Modul izrade licence

Modul za izradu licence obavezan je dio koji proizvođač upotrebljava za izradu navedene licencne datoteke. Prijenos licencne datoteke nije specificiran, stoga je dizajniran kao skup osobina koje osiguravaju njenu istovjetbu prema točno određenom uređaju. Prvo se postavlja datum trajanja licence koji prikazuje do kojeg datuma vrijedi izmjena licence postavljena ovom datotekom te je definiran preko standardnog datumskog zapisa. Potom se postavlja istovjetbeni broj uređaja za kojeg je ciljana ova licenca preko određene kombinacije informacija. Na kraju se unosi ugovorena licenca prema strukturi određenoj od tvrtke i cijela se licencna datoteka šifrira, odnosno zaštićuje dodavanjem digitalnog potpisa (Sl. 3.5.). Na ovakav način nije bitno kojom metodom se prenosi licencna datoteka jer ju samo ciljani uređaj s točnim ključem može ovjeriti.



Sl. 3.4. *Modul za stvaranje ključeva - privatni ključ sprema se u bazu ključeva, a javni ključ unosi se u uređaje.*



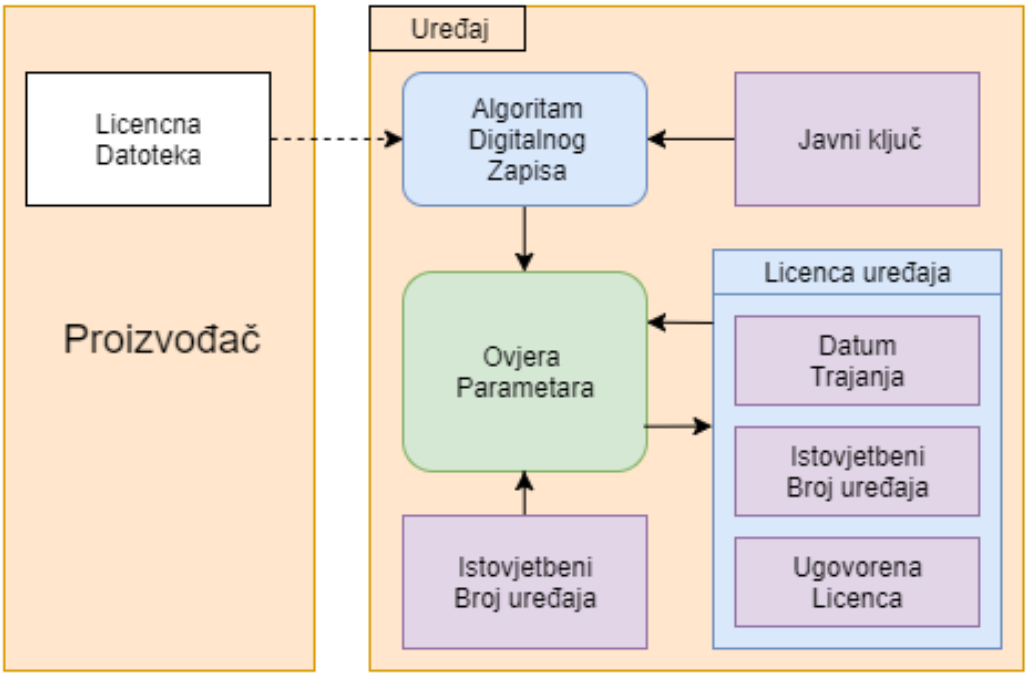
Sl. 3.5. *Modul za izradu licencne datoteke kojom korisnik može ažurirati licencu uređaja.*

3.3.3. Modul ažuriranja licence

Modul za ažuriranje licence obavezan je dio koji se nalazi unutar uređaja i služi kao proces primanja licencne datoteke, njene ovjere istovjetbe vlasnika i ostalih osobina u namjeri potvrde sigurnosti i točnosti podataka. Istovjetbom broja uređaja potvrđuje se da je licenca namijenjena istom, a datumom se potvrđuje da je u granicama mogućnosti izmjene licence (Sl. 3.6.). Nakon obavljenih svih mjera ovjere i njihovom točnosti, licenca se može postaviti na uređaj. Postavljanje licence obuhvaća spremanje cijele licencne datoteke u uređaj zbog potrebnih kasnijih ovjera objašnjenih u daljnjem odlomku.

3.3.4. Modul potvrde i pružanja licence

Modul za potvrđivanje i pružanje licence obavezan je dio koji se pokreće nakon svakog uključivanja uređaja i radi sličan proces provjere licence učitavanjem licencne datoteke, ovjere istovjetbe vlasnika i ostalih osobina namjenjenih potvrdi sigurnosti i točnosti podataka, baš kao i prethodni modul (Sl. 3.6.). Ovaj proces se odvija na ovakav način zbog zaštite od moguće neovlaštene izmjene licence unutar uređaja. Digitalni potpis unutar licencne datoteke osigurava prikaz netočne istovjetbe prilikom bilo koje izmjene podataka i pritom obavještava uređaj o problemu. Točnom istovjetbom licence, ona se prosljeđuje uređaju kao popis prava koje korisnik smije upotrebljavati.



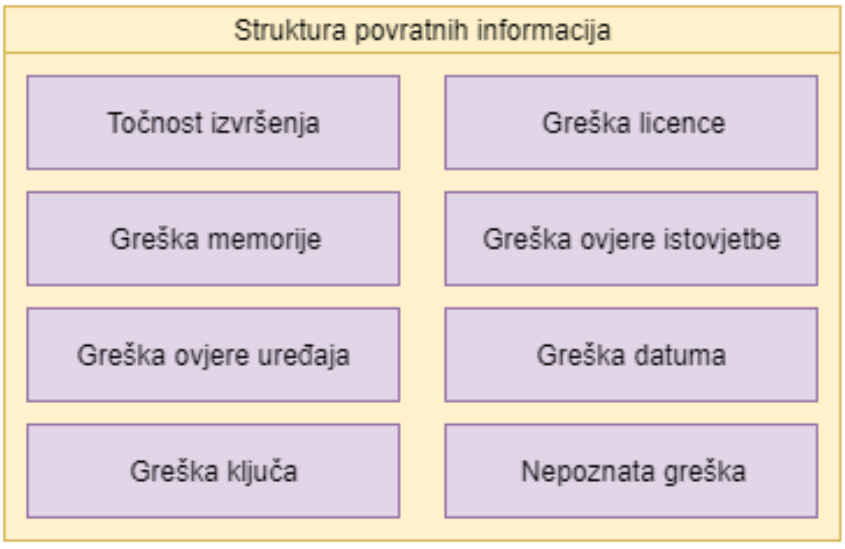
Sl. 3.6. *Metoda ovjere licence potrebne za njeno postavljanje na uređaj.*

4. IMPLEMENTACIJA I TESTIRANJE IZRAĐENOG RJEŠENJA ZA LICENCIRANJE

Navedenim modulima prireden je plan dizajna kontrolera, odnosno sustava licencnog modula gdje su obuhvaćena sva pitanja vezana za uspješno provođenje sigurnosti licenciranja uređaja. Time je moguće krenuti u proces izrade programskog sustava prema navedenim stavkama. Zbog politike tvrtke partnera detaljne informacije o sadržaju programske strukture su zatvorenog koda i moguće ih je samo ukratko objasniti.

4.1. Izrada programskog modula

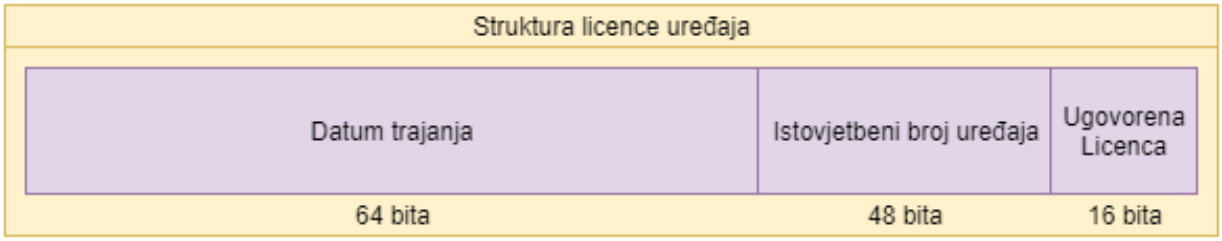
Većina problema izrade tehnika šifriranja riješena je programskim bibliotekama otvorenog kôda prema [16], tako da je metode zaštite licenciranja potrebno vlastito izraditi, a tehnike šifriranja samo integrirati unutar programskog kôda. Izrada programske strukture, praćena preko formiranih modula, razvrstana je na pet javnih i nekoliko privatnih funkcija koje služe kao pomoćne ili dijeljene funkcije. Za tehnike šifriranja odabran je ECC algoritam digitalnog zapisa koji ima dosta kraću duljinu ključeva i potpisa.



Sl. 4.1. *Izgled strukture povratnih informacija koje funkcije prosljeđuju jedna drugoj.*

Moduli koriste dvije dijeljene strukture sa svim potrebnim podacima. Jedna od njih je struktura povratnih informacija korištena za međusobnu komunikaciju funkcija i sadrži potvrdnu

vrijednost izvršenja uz niz mogućih grešaka koje se mogu dogoditi (Sl. 4.1.), dok je druga struktura licence unutar uređaja, gdje se spremanju podaci potrebni programskom modulu i opisani su prema slici 4.2. Sve funkcije rađene su na shemi slijednih logičkih upita privatnim funkcijama ili aritmetičkih operacija, te ako koji vrati rezultat greške, funkcija završava i vraća dobivenu grešku nazad. U protivnom funkcija nastavlja s radom i vraća poruku točnosti.



Sl. 4.2. *Izgled strukture licence uređaja i veličina zauzeća memorije njezinih elemenata u bitima.*

Privatne funkcije sastoje se od tri različite funkcionalnosti i nekoliko standardnih pozivača na dohvaćanje ili pohranjivanje struktura koji se koriste samo unutar strukture:

- Funkcija za ovjeru istovjetbe uređaja i datuma koristi se tako da se standardnim pozivanjem struktura dobiju vrijednosti iz uređaja i onda usporede s upitnima;
- Funkcija za izradu digitalnog potpisa učitava postavljenu licencu i stvara licencnu datoteku preko postavljenog privatnog ključa;
- Funkcija za provjeru digitalnog potpisa vrši ovjeru nad dobivenom licencnom datotekom preko javnog ključa i vraća stanje točnosti;
- Ostale funkcije namijenjene su za standardno pozivanje struktura i koriste se za dohvaćanje ili pohranjivanje: licencne datoteke, ključeva, istovjetbenog broja uređaja ili trenutnog datuma u uređaju.

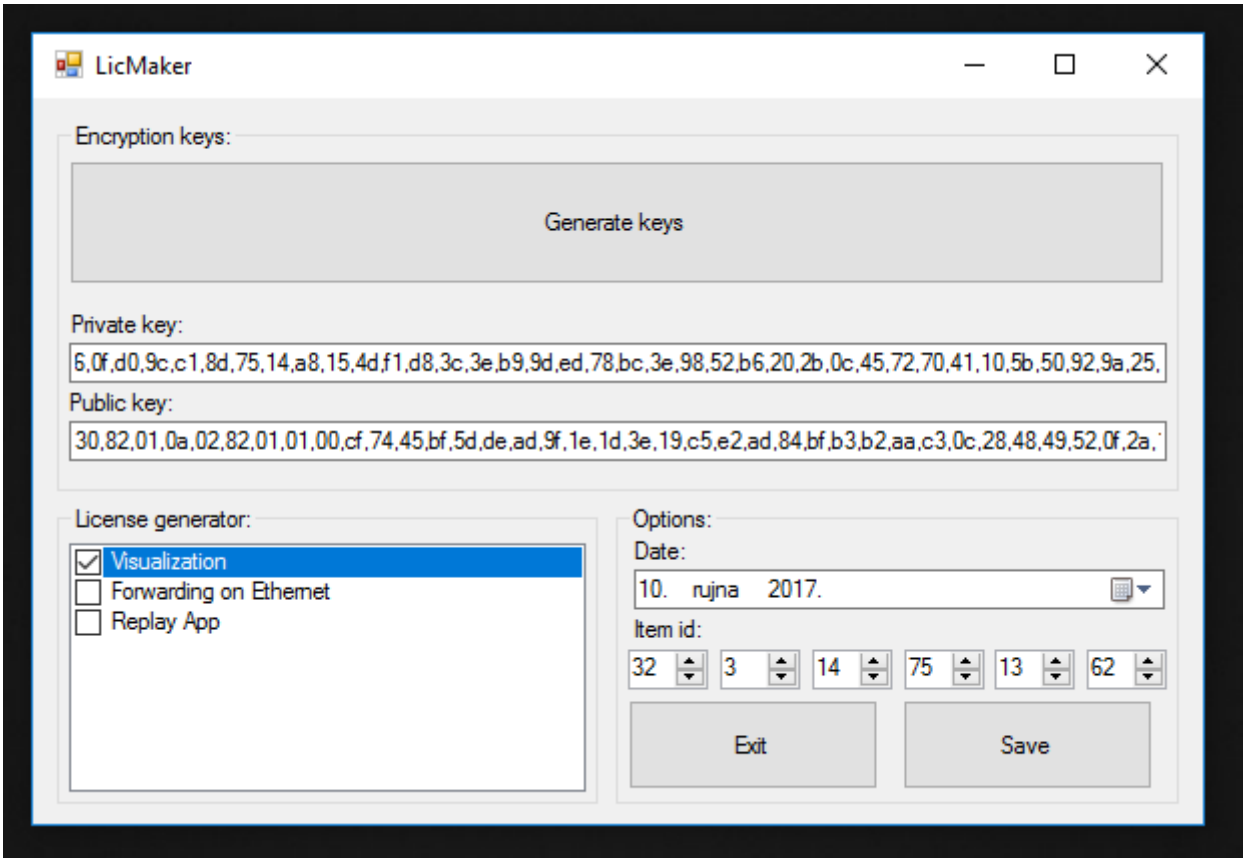
Glavne funkcije namijenjene su za pozivanje izvan sustava i dijele se na: stvaranje ključeva i stvaranje licencne datoteke od strane proizvođača i provedba istovjetbe prilikom pokretanja, ažuriranje licencne i čitanje licencne unutar uređaja. Prema modulima iz potpoglavlju 3.3. izrađene funkcije su:

- Funkcija stvaranja ključeva koja koristi osnovni slijed programskih biblioteka za stvaranje javnog i privatnog ključa te ih nakon uspješnog stvaranja sprema na postavljena mjesta;

- Funkcija stvaranja licencne datoteke koja preko ulaznih parametara željene licence i postavljenog ključa stvara digitalni potpis, pridodan licenci i zapakiran kao licencna datoteka;
- Funkcija ažuriranja licence koja primljenu licencu provodi kroz provjeru digitalnog zapisa i, ako sve odgovara, poziva se funkcija za spremanje licence;
- Funkcija istovjetbe prilikom pokretanja koja radi na isti način kao i prethodna funkcija, samo što se svaki put licencna datoteka unutar uređaja ovjerava i postavlja u strukturu ili vraća prazna prilikom greške;
- Funkcija čitanja licencne koja učitanu licencu iz uređaja prosljeđuje dalje na korištenje.

4.2. Izrada programskog sučelja

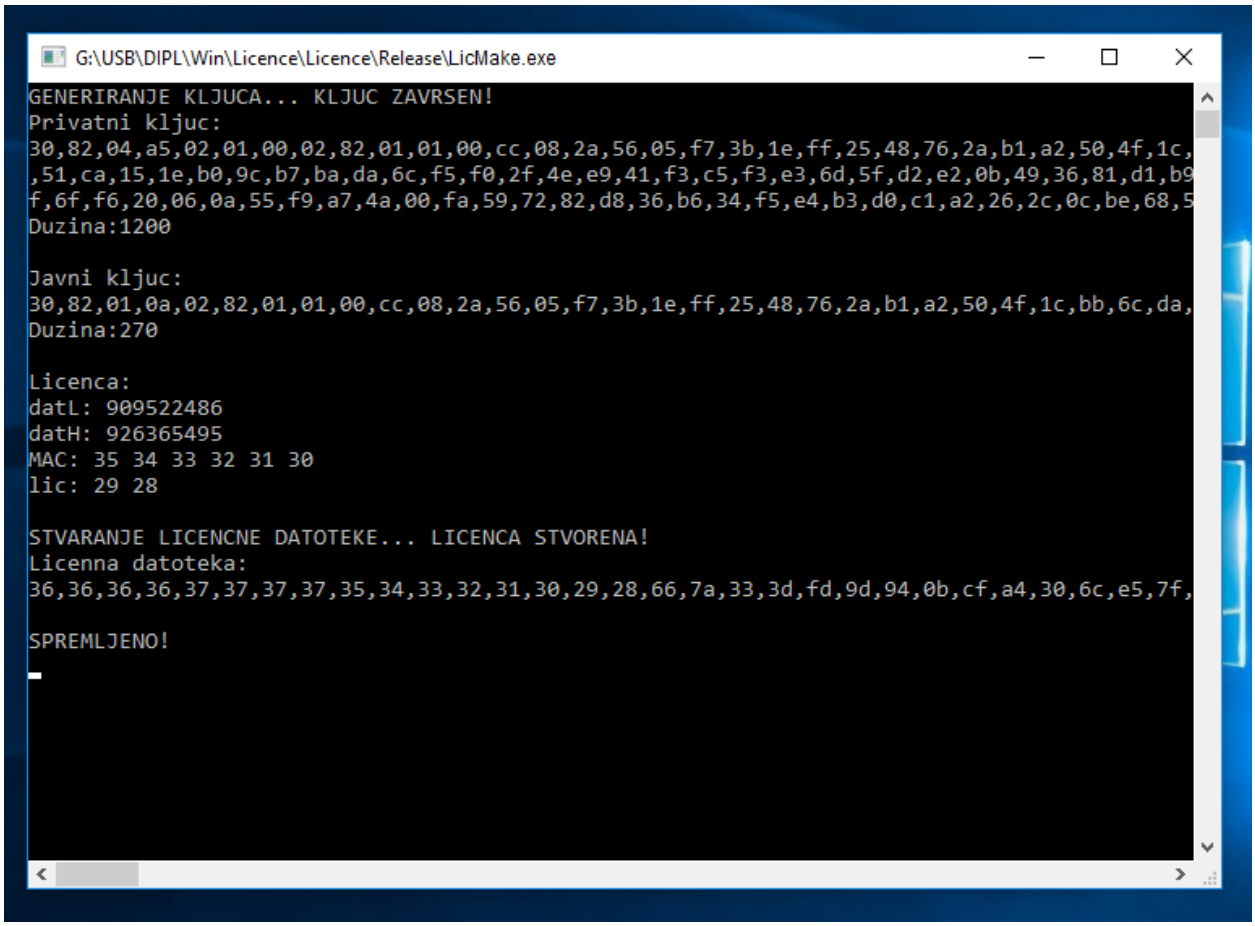
Za stvaranje ključeva zadane metode šifriranja i izrade licencne datoteke odlučilo se dizajnirati i izraditi programsko sučelje koje će koristiti stvorene programske biblioteke unutar Windows operacijskog sustava. Program sadrži jednostavan raspored potrebnih parametara za rad i kratki izbornik koji stvorenu licencnu datoteku sprema na poželjno mjesto (Sl. 4.3.).



Sl. 4.3. *Programsko sučelje za izradu ključa i licencne datoteke.*

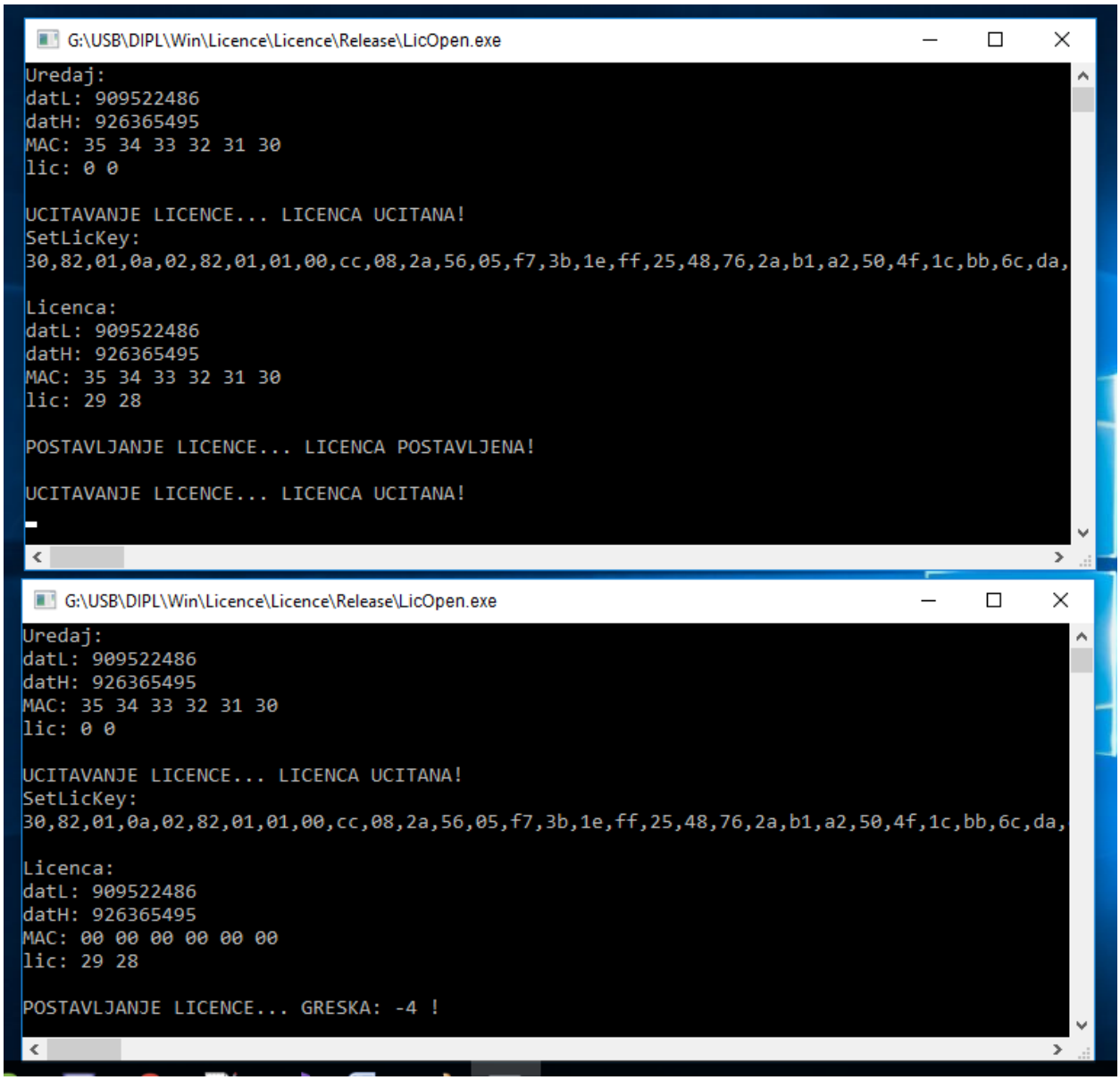
4.3. Testiranje rješenja

Testiranje je izvršeno pomoću dva stvorena simulacijska programa, zvanih proizvođač i uređaj. Simulacijski program proizvođača sadrži sve potrebne funkcije proizvođača te prilikom svakog pokretanja stvara novu kombinaciju ključeva za šifriranje i preko njih, ovisno o postavljenim parametrima licence, stvara licencnu datoteku koju sprema u direktorij. Sve faze procesa ispisuju se prema slici 4.4.



Sl. 4.4. *Testiranje generiranja ključa, unosa licence i stvaranja licencne datoteke.*

Simulacijski program uređaja sadrži sve potrebne funkcije uređaja. Počinje učitavanjem dobivene licencne datoteke koju pritom pokušava ažurirati i učitati u strukturu ako ista odgovara. Sve faze procesa se ispisuju prema slici 4.5. Ovim testovima su se korigirale manje uočene greške i pokazalo se da ovakav sustav dobro uočava izmjenu licencne datoteke, neistovjetnosti uređaja ili istek datumskog roka.



Sl. 4.5. *Testiranje učitavanja licence u uređaj. Gornja polovica slike pokazuje točnu ovjeru licencne datoteke, a donja polovica slike, uz promijenu broja uređaja, javlja grešku.*

Daljnjim se testiranjem provjeravala zlouporaba licencnih prava korištenjem javnog ključa unutar uređaja u digitalnom potpisivanju lažne licencne datoteke, koju bi uređaj prihvatio, i ustanovilo se da ECC algoritam digitalnog zapisa ima tu manu ovjeravanja bez prisustva privatnog ključa. Na sreću, promjenom metode digitalnog zapisa na RSA algoritam, pokazalo se da on ne omogućuje ovakav propust i zahtjeva da se samo privatnim ključem mogu stvoriti i ovjeriti digitalni zapisi.

Programskom modulu nije omogućeno da se testira na konkretnom uređaju zbog nedovršenosti samog proizvoda, no nesmetan rad je uvelike osiguran pošto zadatak ne pati od vremenskog rizika izvršavanja te operacijski sustav uređaja omogućava isto ponašanje stvorenih programskih biblioteka kao i na testnim primjerima.

5. ZAKLJUČAK

U skladu s postavljenim zadatkom od u vezi licenciranja proizvoda u automobilskoj industriji, ovaj diplomski rad se pozabavio temeljnim pitanjima i razlozima uvođenja licenciranja proizvoda. Dotakao se kompleksne raspodjele problema, implementacije i sigurnosti procesa te izrade i troškova programskih modulacija koje tvrtke mogu iskoristiti u svojem poslovanju.

Usporedbom različitih tehnika, metode su se razvrstale na dvije osnovne strukturne grupe: strojne i programabilne strukture. Djelomično zavisne, svaka struktura ima svoje načine zaštite licenciranja, no specifično ovom zadatku fokusiralo se više na one programabilne. Formiranjem i razvrstavanjem metoda zaštite, šifriranja i protokola proveo se zadnji korak analize zadatka i time su se zaokružili svi aspekti licenciranja za daljnje dizajniranje sustava.

Rukovanjem spomenutim metodama te stvarajući formirane sustave s mogućnošću uspješnijeg pružanja usluge licenciranja unutar zadanog zadatka, prikazalo se nekoliko načina moguće implementacije, od kojih se treba odabrati jedan za implementaciju unutar modularnog sustava. U obzir su uzete sve dane specifikacije tvrtke koje su obuhvaćale sklopovlje i programsku strukturu, a odabirom onog optimalnog, krenulo se na izradu i testiranje.

U izradi modula korištene su standardne programske biblioteke šifriranja i prema specifikacijama tvrtke dizajnirao se, njima prihvatljiv, sustav licenciranja i programski modul koji se može koristiti. Testiranjem se utvrdilo da nisu svi načini jedne kategorije sigurni za korištenje i daljnjom analizom se pronašlo optimalno rješenje problema i time u potpunosti završilo s ovim zadatkom.

Tijekom rada na zadatku i analizom svih metoda licenciranja došlo se do zaključka da je izabrana solucija u prihvatljivim granicama sigurnosti. Premda postoje sigurnije metode, ponekad to nije moguće zbog ograničenja resursa i vremena te je potrebno pronaći neku ravnotežu i što više težiti kvaliteti. U sklopu ovog diplomskog rada provela se analiza metoda licenciranja i izradila gotova programska struktura, ali nije izvršeno krajnje testiranje i korištenje na konkretnim uređajima pa je obavezno da ih tvrtka naknadno provede.

LITERATURA

[1] R. Raysman, E. A. Pisacreta i K. A. Adler, „*Intellectual Property Licensing: Forms and Analysis*“, Law Journal Press, New York, USA. 1999.

[2] A. Ross, „*Security Engineering: A Guide to Building Dependable Distributed Systems*“, str. 240, New York, USA, 2001.

[3] A. Shamir, „*How to share a secret*“, Communications of the ACM, New York, USA, 1979.

[4] W. Tuchman, „A *brief history of the data encryption standard*“, Addison-Wesley Publishing Co., New York, USA, str. 275–280, 1997.

[5] B. Schneier, „*Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)*“, Springer-Verlag, Njemačka, 1993.

[6] National Institute of Standards and Technology, „*Announcing the Advanced Encryption Standard (AES)*“, Federal Information Processing Standards Publication, USA, 2001.

[7] R. L. Rivest, A. Shamir i L. Adleman, „*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*“, Communications of the ACM, New York, USA, 1978.

[8] National Security Agency„„*The Case for Elliptic Curve Cryptography*", USA, 2009.

[9] A. Lysyanskaya, „*Signature Schemes and Applications to Cryptographic Protocol Design*“, Massachusetts Institute of Technology, USA, 2002.

[10] D. W. Hellman, „*New directions in cryptography*", IEEE Transactions on Information Theory, 1976.

[11] J. R. Vacca, „*Public key infrastructure: building trusted applications and Web services*“, Aurbach Publications, New York, USA, 2004.

[12] https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange (15. rujna 2017.)

[13] L. M. K. Vandersypen, S. Matthias, B. Gregory i dr. „*Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*“, Stanford University, California , USA, 2001.

[14] D. J. Bernstein, „*Introduction to post-quantum cryptography*“, Department of Computer Science, Chicago, USA, 2009.

[15] B. Kernighan, D. M. Ritchie, „*The* C *Programming Language*“, New Jersey, USA, 1978.

[16] T. St Denis, „LibTomCrypt“, Developer manual, 2002.

SAŽETAK

Analiza različitih mehanizama za licenciranje softverskih modula u automobilskoj industriji

U automobilskoj industriji upravljačke jedinice često sadrže više različitih funkcionalnosti i proizvođači imaju potrebu kontrolirati distribuciju i cijenu različitih varijanti istog proizvoda. Ovim se diplomskim radom provela detaljna analiza metoda licenciranja proizvoda u automobilskoj industriji. Razvrstavanjem različitih modela zaštite i šifriranja licence formirani su gotovi sustavi dobrih funkcionalnosti i odabran je najpovoljniji. Gotovim dizajnom i naknadnim testiranjem, stvoreno je programsko rješenje, u obliku biblioteke, spremno za unošenje u namijenjene uređaje i nesmetano korištenje.

Ključne riječi: automobilska industrija, licenca, šifriranje, programski modul

ANALYSIS OF DIFFERENT MECHANISMS FOR LICENCING OF SOFTWARE MODULES IN AUTO INDUSTRY

ABSTRACT

In the automotive industry the control units often have many different functionalities and manufacturers need to control the distribution and prices of different variants of the same product. Through this graduate thesis, a detailed analysis of product licensing in the automotive industry has been carried out. By classifying different models of license protection and encryption, a systems with good functionality have been created and the most beneficial for the usage was chosen. With a finished design and subsequent testing, a program-based library was created that is ready to be put into the intended devices and be used indefinitely.

Keawords: automobile industry, license, encryption, module

ŽIVOTOPIS

Filip Kraus rođen je 20. lipnja 1991. godine u Osijeku, Hrvatska. Osnovnu školu završava 2006. godine u Osijeku te iste godine upisuje Prirodoslovno-matematičku gimnaziju u Osijeku. Srednju školu završava 2010. godine i upisuje stručni studij Informatike na Elektrotehničkom fakultetu, Osijek i završava ga 2013. godine. Iste godine upisuje razlikovnu godinu smjer Računarstvo na istom fakultetu i završava ju 2015. godine, uz usporedno odrađeno stručno usavršavanje preko Zavoda za zapošljavanje u Domu zdravlja Osijek kao informacijski tehničar. Time stječe zvanje prvostupnik inženjera računalstva, smjer informatika i dobiva pravo upisa na sveučilišni diplomski studij gdje upisuje smjer Procesno računarstvo na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija, Osijek.

_____

Filip Kraus