ISSN 1864-6168
UDK 62

O IZVEDBI POSTUPKA FISKALIZACIJE RAČUNA NA ANDROID PLATFORMI

ABOUT IMPLEMENTATION OF RECEIPT FISCALIZATION ON ANDROID PLATFORM

Dražen Hižak, Matija Mikac

Stručni rad

Sažetak: *Od prvog pojavljivanja na tržištu 2008. do danas Android platforma je preuzela vodeće mjesto među platformama za mobilne uređaje. Otvorenost koda operacijskog sustava, dostupnost dokumentacije te besplatna razvojna okolina omogućili su programerima brzi razvoj korisnih aplikacija za tu platformu. Danas se Android mobilni uređaji koriste u mnoge svrhe - s jedne strane omogućuju korisnicima jednostavne radnje kao što su pristupanje internetu, organiziranje kućnih financija, pregledavanje zemljopisnih karti, dok s druge postoje i mnogo složenije primjene – kako za osobnu tako i za poslovnu primjenu. Ovim radom opisani su ključni koraci primjenjivi u razvoju aplikacije za fiskalizaciju, koja je 2013. postala zakonska obaveza većine poslovnih subjekata u Republici Hrvatskoj. Opisana je ukratko sama fiskalizacija, protokol za komunikaciju s poslužiteljem Porezne, korištenje digitalnih sigurnosnih certifikata koje je izdala Financijska agencija (FINA) te princip digitalnog potpisivanja XML dokumenata, neophodan za realizaciju propisanog postupka fiskalizacije.*

Ključne riječi: *Android, porezna uprava, FINA, fiskalizacija, fiskalna blagajna, XML, sigurnosni certifikat*

Professional paper

Abstract: *Since its first appearance on the market in 2008., Android has become one the leading platform for mobile devices. The open-source operations system, the accessibility of its documentation and the free development environment has provided the programmers with all the prerequisites to rapidly develop useful apps for the platform. Today the Android mobile devices are used for numerous purposes. On one hand, they enable simple actions such as internet access, household bill control, browsing through geographical maps, as well as the usage of more complex applications for personal and business/enterprise usage. This paper describes necessary steps that can be used for development of fiscalization app, which (will) become mandatory for most enterprises in Croatia during 2013. In short lines, it describes the fiscalization itself, the protocol used for communication with Tax Administration server, usage of digital security certificate that can be obtained from Croatian Financial Agency (FINA), as well as the procedure of digital signing XML files, which is obligatory for implementing the procedure.*

Key words: *Android, Tax Administration, FINA, fiscalization, fiscal point of sale, XML, security certificate*

1. UVOD

Odlukom Sabora Republike Hrvatske, u studenom 2012. donesen je Zakon o fiskalizaciji u prometu gotovinom, objavljen u Narodnim novinama, broj 133/12 [1]. Zakon je počeo važiti od 1. siječnja 2013., a primjenjuje se prema specificiranim grupama korisnika u nekoliko faza. Jedan od ciljeva Zakona je uvođenje reda i bolja kontrola poslovanja poduzetnika koji dio naplate izvode gotovinski. Primjena Zakona sama po sebi donosi nove troškove poduzetnicima, ali isto tako osigurava informatičkim i telekomunikacijskim tvrtkama mogućnost dodatne zarade kroz razvoj i nadogradnju postojećih poslovnih rješenja. Ne ulazeći u detalje i bez prosuđivanja o pozitivnim i negativnim stranama Zakona, činjenica je da za ostvarenje propisanih uvjeta treba osigurati određene tehničke pretpostavke te treba nadograditi postojeća softverska rješenja. Također, s obzirom na to da Zakon obuhvaća i dio malih poduzetnika uz koje su vezane specifičnosti mobilne prodaje, može se zaključiti da je doneseni Zakon direktno utjecao i na neke promjene u izvedbi poslovnih rješenja, potaknuvši razvoj programskih rješenja za mobilne platforme.

Sukladno Zakonu, fiskalne blagajne (blagajne koje osim standardnih funkcionalnosti izrade računa osiguravaju i tzv. fiskalizaciju, odnosno automatsku prijavu računa Poreznoj upravi) postale su obavezne za korištenje kod određenih grupa poslovnih subjekata, a tehničke specifikacije su objavljene u [2]. Da bi fiskalna blagajna mogla funkcionirati, tvrtke korisnici moraju ispuniti neke preduvjete: osigurati (internet) vezu blagajne i poslužitelja Porezne uprave te osigurati digitalni sigurnosni certifikat koji izdaje Financijska agencija (FINA). FINA je trenutačno jedini ovlašteni izdavač digitalnih certifikata za provođenje fiskalizacije (CA – eng. *Certificate Authority*, [3]) u Republici Hrvatskoj.

Uobičajeni način rada u tvrtkama uključuje korištenje blagajni na stolnim računalima. Međutim, zbog fiskalizacije i kod mobilnih korisnika nastala je potreba za razvojem prijenosnih fiskalnih blagajni. Jedno od

primjenjivih rješenja za implementaciju mobilne fiskalne blagajne je izvedba blagajne na mobilnim uređajima baziranim na operacijskom sustavu Android. Zbog raširenosti Android sustava aplikaciju s modulom za fiskalizaciju moguće je pokretati na mnogim mobilnim uređajima kao i na tabletima, naravno uz zadovoljene preduvjeta kao što su internet te osiguranje sigurnosnih pretpostavki. Ovim radom daje se pregled tehničkih aspekata izvedbe fiskalizacije, uključujući opis komunikacijskog protokola za ostvarenje veze s poslužiteljem Porezne uprave, kao i opis postupka zaštite i digitalnog potpisivanja XML dokumenata koji se prosljeđuju na poslužitelj. Opisuje se i moguća izvedba fiskalizacijske komponente prijenosne blagajne bazirane na Android platformi.

2. FISKALIZACIJA

Radi efikasnijeg nadzora Porezne uprave nad ostvarenim prometom poduzetnika, uvedena je fiskalizacija koja zakonski definira poslovne subjekte-obveznike fiskalizacije i sva pravila vezana uz vođenje fiskalnih blagajni i prijavljivanje izdanih računa. Sam proces fiskalizacije na naplatnom uređaju svodi se na slanje informacija o izdanom računu i obvezniku, te se obavlja prema točno definiranom postupku koji se detaljnije opisuje u odjeljku 2.1. Fiskalizacija obavezuje korisnika da osim prijave računa prijavi i prostor u kojem će izdavati račune putem naplatnog uređaja.

2.1. Proces prijave računa poreznoj upravi

Slika 1. prikazuje službeni [2] dijagram postupka fiskalizacije – prikazuje proces prijave računa prema poslužitelju Porezne uprave. Sve počinje u trenutku kada operater na blagajni treba izdati račun. Naplatni uređaj priprema podatke za račun te izračunava zaštitni kod izdavatelja (ZKI) sukladno algoritmu opisanom u tehničkoj dokumentaciji Porezne uprave [2] namijenjenoj onima koji su razvili programska rješenja za fiskalne blagajne. Nakon toga priprema XML poruku zahtjeva te ju elektronički potpisuje privatnim ključem sigurnosnog aplikativnog certifikata koji je izdan obvezniku fiskalizacije (kao što je opisano u uvodnom poglavlju, obveznik je dužan osigurati sigurnosni certifikat – izdaje ga FINA). Kada je XML poruka zahtjeva potpisana (do ove točke postupak se odvija lokalno, na računalu/uređaju obveznika fiskalizacije), potrebno je uspostaviti sigurnu vezu prema poslužitelju, prema tzv. središnjem informacijskom sustavu Ministarstva financija, odnosno Porezne uprave (u nastavku CIS), te proslijediti zahtjev na obradu.

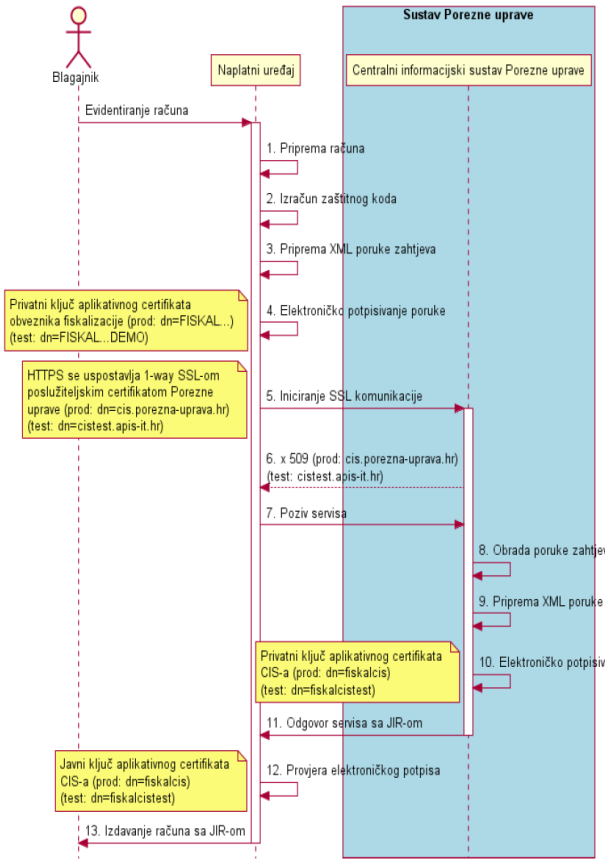
Sigurna komunikacija s CIS-om izvodi se korištenjem standardnih protokola. Koristi se sigurna verzija aplikacijskog HTTP(S) protokola uz korištenje SSLv3 (eng. *Secure Socket Level, version 3*) protokola za realizaciju sigurne veze.

Nakon uspostave sigurne veze zahtjev se prosljeđuje CIS-u pa započinje obrada poslanog zahtjeva. U slučaju uspješne obrade (standardni slučaj) CIS vraća poruku-odgovor koji sadrži i jedinstveni identifikator računa (JIR). Odgovor je potpisan privatnim ključem aplikativnog certifikata CIS-a.

Ako je kojim slučajem u obradi zahtjeva došlo do greške, CIS će odgovoriti sa šifrom greške te opisom greške. Do greške npr. može doći ako se proslijede neispravni podaci (provodi se osnovna kontrola poslanog zahtjeva).

Naplatni uređaj (fiskalna blagajna) zaprima poruku s odgovorom, obavlja sigurnosnu provjeru podataka korištenjem javnog ključa aplikativnog certifikata CIS-a, te dovršava postupak izdavanja računa. U slučaju greške ili nemogućnosti obrade zahtjeva (preopterećenost CIS-a, nemogućnost korištenja internetske veze), JIR nije dodijeljen te obveznik mora naknadno provesti (ručno ili automatski, ovisno o izvedbi fiskalne blagajne) prijavu i dobiti JIR za prijavljeni račun!

Zakonom su propisani obavezni elementi računa, od informacija direktno vezanih uz opisani postupak, na račun se obavezno mora ispisati JIR i ZKI.



Slika 1. Dijagram postupka prijave računa [2]

S obzirom na prirodu informacija koje se razmjenjuju, jasno je da su sigurnost komunikacije i zaštita prenosivih podataka vrlo bitne stavke kompletnog fiskalnog sustava. Prema dosad iznesenom može se zaključiti da se podaci zaštićuju na dvije razine. Prva razina bila bi razina mrežne komunikacije koja osigurava enkripciju i zaštitu podataka od neovlaštenog čitanja. Druga razina je integritet podataka - ako se netko i uplete u razmjenu informacija i napravi promjene, digitalni potpis dokumenta će osigurati dovoljno informacija za kontrolu i donošenje zaključka da su podaci u postupku prijenosa bili mijenjani.

3. INFRASTRUKTURA JAVNIH KLJUČEVA

Da bi se zaštitile informacije koje se izmjenjuju između klijenta i davatelja usluga, u ovom slučaju obveznika fiskalizacija i CIS-a, te da bi se oni mogli međusobno identificirati, koristi se infrastruktura javnih ključeva (eng. *Public Key Infrastructure*, PKI). Glavni element te infrastrukture su digitalni certifikati. Digitalni certifikati su danas jedan od temelja sigurnosti na internetu te svoju primjenu nalaze u mnogim područjima. Za potrebe fiskalizacije digitalni se certifikati koriste kako bi zaštitili podatke (u prijenosu) na transportnom sloju (TLS ili SSL protokoli između aplikacijskog i transportnog sloja) i kako bi osigurali da dođu u nepromijenjenom obliku na odredište. Isto tako, za fiskalizaciju se koristi i postupak digitalnog potpisivanja poruka.

Digitalno potpisivanje ili enkripcija poruke provodi se privatnim ključem pošiljatelja, a primatelj provjeru potpisa ili dekripciju poruke radi korištenjem javnog ključa (pošiljatelja). Time može provjeriti autentičnost pošiljatelja i nepromijenjenost poruke u postupku komunikacije. Digitalnim potpisom poruke smatra se sažetak poruke, odnosno njegova *hash* vrijednost. Digitalni certifikati se temelje na tehnologiji javnog i privatnog ključa te su standardizirani pomoću X.509 standarda. Ovi ključevi se uvijek generiraju u paru. Podaci koji se kriptiraju javnim ključem dekriptiraju se privatnim ključem i obratno.

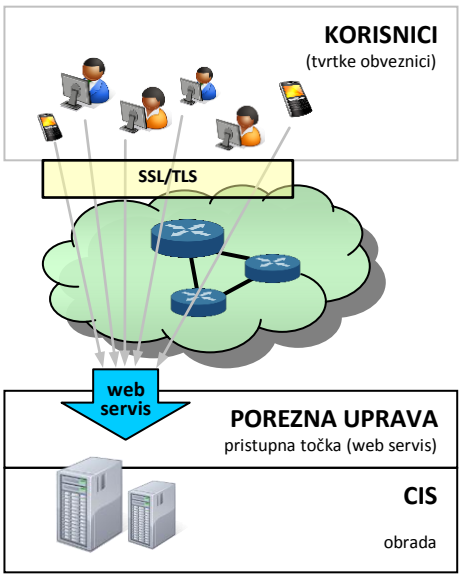
Bitno je naglasiti da digitalne certifikate izdaju tvrtke ili ovlaštene agencije. Kada treba, takav centralizirani pristup osigurava dodatnu kontrolu, jedinstvenost ključeva i sigurnu identifikaciju korisnika. Svaki obveznik fiskalizacije dužan je pribaviti digitalni certifikat da bi se mogao koristiti sustavom fiskalizacije, a taj certifikat izdaje FINA RDC (Centar za registre digitalnih certifikata, [4]), s obzirom na to da je FINA jedini ovlašteni izdavač certifikata u RH).

Digitalni certifikat potvrđuje povezanost javnog i privatnog ključa koji posjeduje neki entitet. Identitet entiteta, koji može biti osoba ili aplikacija, sadržan je u certifikatu zajedno s javnim ključem. Da bi ovakva struktura bila valjana, nju mora potpisati treća strana, certifikacijski autoritet CA (eng. *Certificate Authority*), koji predstavlja autoritet od povjerenja – u slučaju fiskalizacije to je FINA.

Sama primjena digitalnih certifikata u fiskalizaciji bit će objašnjena u nastavku.

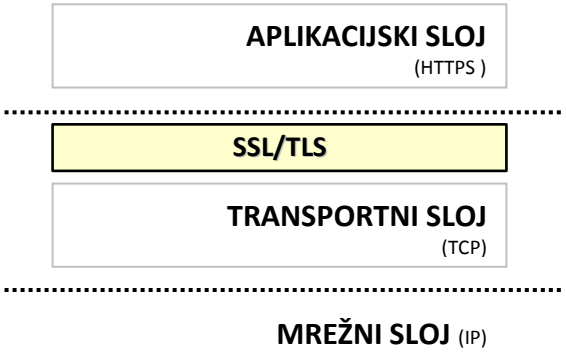
4. KOMUNIKACIJA

Da bi se osigurala sigurna komunikacija s obveznikom fiskalizacije, komunicira se korištenjem SSL protokola, verzija 3. Koristeći SSL nadogradnju standardnog transportnog TCP protokola privatnim ključem kriptiramo (šifriramo) podatke koji se šalju na CIS. Ako je certifikat koji koristi klijent izdala FINA, CIS će moći pročitati pristiglu poruku te će početi s obradom i pripremom odgovora. Aplikacijski protokol koji se koristi u komunikaciji s CIS-om je HTTPS (sigurna verzija standardnog HTTP-a, ostvaruje se primjenom SSLv3 međusloja između HTTP i TCP protokola). Prema tome, usluga CIS-a za obradu prijava u sklopu fiskalizacije smatra se tzv. web servisom. Ideju sustava prikazuje slika 2.



Slika 2. Koncept sustava fiskalizacije

Na slici 3. Prikazani su bitni slojevi komunikacijskog modela koji se koristi za ostvarenje sigurne komunikacije u sustavu fiskalizacije. Kao što je već spomenuto, sigurnost na razini aplikacijskog sloja postiže se primjenom SSL podsloja.



Slika 3. Slojevi komunikacijskog modela

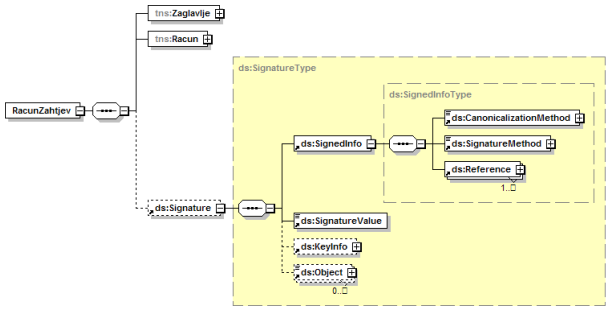
Komunikacija između uređaja obveznika i serverske strane započinje slanjem *Client Hello* poruke poslužitelju na adresi ***cis.porezna-uprava.hr*** u produkcijskoj fazi, odnosno ***cistest.apis-it.hr*** za potrebe testiranja (kao transportni protokol koristi se TCP i vrata 8449). Tom porukom klijent se predstavlja svojim certifikatom (dobivenim od FINE). S obzirom na korištenje sigurnih protokola, poruka sadrži i informacije o verziji sigurnosnih protokola i popis algoritama za kriptiranje podataka koje klijentov uređaj podržava (eng. *cipher suite*), te ostale informacije potrebne za komunikaciju. Nakon toga server odgovara *Server Hello* porukom u kojoj navodi algoritam koji želi koristiti te šalje podatke o svom certifikatu. Ako oba uređaja međusobno prihvate ponuđene postavke i ako se ispostavi da su uređaji ti kojima se predstavljaju da jesu pomoću certifikata, razmjena podataka može početi. Upravo opisana

inicijalna komunikacija naziva se rukovanje (eng. *Handshake*), a ovdje su spomenute samo neke osnovne smjernice rukovanja. Samo rukovanje sadrži još neke korake koji nisu bitni za ovaj članak. Važno je napomenuti da su u izvedbi programskog rješenja za realizaciju rukovanja zadužene standardne klase za komunikaciju.

5. ZAHJTEV ZA PRIJAVU RAČUNA

Obveznik fiskalizacije prilikom prijave računa šalje XML dokument u kojem se unutar njegovog korijenskog elementa *RacunZahtjev* nalaze elementi *Zaglavlje*, *Racun* i *Signature*. U zaglavlju računa se navode datum i vrijeme slanja poruke kao i jedinstveni identifikator poruke (eng. *UUID*), dok se u elementu *Racun* nalazi OIB obveznika fiskalizacije, OIB prodavača, redni broj računa, informacija o tome je li račun naknadno poslan, informacije o naplatnom uređaju i ostale informacije potrebne poreznoj upravi da bi jednoznačno identificirala obveznika, račun i fiskalni promet. Nakon što je stvoren XML dokument kreće potpisivanje digitalnim certifikatom obveznika. Potpisivanje je nužno kako bi se osigurala neporecivost i cjelovitost podataka.

Shematski prikaz strukture poruke zahtjeva za prijavu računa prikazan je na slici 4.



Slika 4. Shematski prikaz zahtjeva prijave računa [2]

Svaka poruka poslana CIS-u mora biti potpuno usklađena sa specifikacijama definiranim službenim dokumentom koji je izdala Porezna uprava Republike Hrvatske [2]. Pošto su same stavke vezane uz elemente *Zaglavlje* i *Racun* nebitne za ovaj članak, shema detaljno prikazuje *Signature* element koji treba generirati za svaki zapis primjenom propisanih sigurnosnih postupaka. S obzirom na to da se za definiranje računa koristi XML dokument koji se kasnije šalje prema CIS-u korištenjem HTTPS protokola, za slanje podataka se koristi standardni SOAP (eng. *Simple Object Access Protocol*) protokol koji osigurava interoperabilnost između različitih platformi. Kako je SOAP standardom propisan, dokumentu (*RacunZahtjev*) koji se šalje dodaje se SOAP omotnica (eng. *SOAP Envelope*).

5.1. SOAP omotnica

SOAP protokol je komunikacijski protokol koji se koristi za razmjenu podataka između obveznika fiskalizacije i CIS-a. SOAP protokol je neovisan od platforme pa mu to daje veliku fleksibilnost i standardno je rješenje koje se koristi u komunikacijskim sustavima, posebno kod pristupanja tzv. *web servisima*. Lako se primjenjuje na XML dokumente. Dovoljno je poruci zahtjeva računa dodati SOAP omotnicu, što je opet čisti XML zapis (primjer zapisa je na slici 5.).

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
   <tns:RacunZahtjev

      ...

   </tns:RacunZahtjev>
</soapenv:Body>
</soapenv:Envelope>
```

Slika 5. *RacunZahtjev* omotan SOAP omotnicom

U primjeru je vidljivo da elementi imaju svoje tzv. XML prefikse (*soapenv* i *tns*). Prefiksi se koriste u *XML* dokumentima da bi se izbjegli konflikti u nazivima elemenata - npr. dva elementa istog naziva, a različitih značenja, prisutna u dokumentu. Da bi u dokumentu mogli koristiti prefikse, potrebno im je definirati tzv. *namespace* i *URI* (eng. *Uniform Resource Identifier*) – jedinstveni identifikator resursa. Da ne bi bilo zabune, *URL* i *URI* se ne odnose na iste stvari. Dok nam *URL* govori lokaciju i na neki način identificira, *URI* samo identificira objekt, u ovom slučaj elemente s određenim prefiksom. URL se smatra posebnim slučajem URI-ja.

5.4. Potpis dokumenta

Osim poslovnih podataka, poruka zahtjeva računa mora sadržavati i digitalni potpis. Prema položaju potpis se može pozicionirati na dva mjesta naspram XML dokumenta. Dok u jednom slučaju može biti odvojen (eng. *detached*) od *XML* elementa kojeg potpisuje, u drugom slučaju može biti dio elementa koji se potpisuje te ga se u tom slučaju naziva omotavajući potpis (eng. *enveloped signature*). U sustavu fiskalizacije koristi se omotavajući potpis. Shematski prikaz na slici 3., kao što je već naznačeno, "raspisuje" element potpisa. Za lakši uvid u *Signature* element koristimo opis strukture na slici 6. Prvi element, odnosno *SignedInfo* element daje informaciju o tome koji su podaci digitalno potpisani i sadrži informacije o protokolima koji se koriste prilikom potpisivanja.

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
       <Transforms>
       <DigestMethod>
       <DigestValue>
    </Reference>
    <Reference />
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
</Signature>
```

Slika 6. Struktura *Signature* elementa

Sljedeći element je *SignatureValue* koji sadrži *base64* (vrsta kodiranja) kodiranu vrijednost potpisa. Ovaj digitalni potpis je potpis generiran prema parametrima

koji su uneseni u *SignedInfo* elementu nakon što je nad dokumentom (XML dokument koji sadrži *RacunZahtjev* element) izvršena kanonikalizacija. Na kraju se nalazi *KeyInfo* element koji sadrži informacije o certifikatu koji se koristi kod potpisivanja poruke.

5.4.1. Element *SignedInfo*

Da bi digitalni potpis bio standardiziran i da bi se koristio uvijek isti protokol potpisivanja, treba u *SignedInfo* elementu navesti koji će se sve protokoli koristiti. Ovdje se navodi vrsta kanonikalizacije (u našem slučaju *Exlusive XML Canonicalization*), algoritam digitalnog potpisa, referenca na element koji će biti digitalno potpisan te metoda kojom će se izračunati sažetak (eng. *hash*) poruke. Kao metoda potpisivanja u postupku fiskalizacije koristi se RSA-SHA1 algoritam. Referenca kod prijave računa pokazuje na korijenski element zahtjeva za račun, *RacunZahtjev*.

5.4.2. Kanonikalizacija

Kanonikalizacija ili popularno označavana *c14n (*eng. *canonicalization,* prvo i zadnje slovo i 14 slova između) je postupak normalizacije dokumenta, odnosno standardizacije koja se radi zbog mogućih solucija prikaza dokumenata. Kanonikalizacija se rješava praznih prostora, koristi određeno kodiranje znakova, briše deklaraciju *XML* dokumenta te ima još mnoge druge zadaće. Dokument bi zapravo trebao biti normaliziran i čitljiv, odnosno interpretiran na isti način na svim platformama.

Npr., element *DigestValue* sadrži *hash* (funkcija koja radi sažetak, eng. *hash*, informacija) vrijednost poruke i koncipirana je tako da ako se poruka i najmanje promijeni tijekom prijenosa, *hash* vrijednost više neće biti ista. Kada poruka dođe do serverske strane, server također izračunava *hash* vrijednost poruke. Ako se vrijednosti koje su stvorili pošiljatelj i primalac ne podudaraju, može se zaključiti da je došlo do promjene podataka tijekom slanja. Da bi se isključila mogućnost nekih običnih nepravilnosti koje mogu prouzročiti neispravnu *hash* vrijednost, koristi se kanonikalizacija da bi standardizirala tu poruku i onemućila da neke manje pogreške (npr. razlike u zapisu na različitim platformama) dovedu do nepravilnosti u čitanju. Izračun i slanje sažetka je standardni postupak koji se primjenjuje za zaštitu cjelovitosti informacija u kontekstu sigurne komunikacije i sustava za kriptografiju. Dok se u elementu *CanonicalizationMethod* precizira postupak kanonikalizacije koji će se primijeniti na sam *SignedInfo* element, u elementu *Transforms* dobivamo informacije o transformacijama koje će izvršiti nad porukom prije izračuna *hash* vrijednosti.

5.4.3. Element *KeyInfo*

KeyInfo element sadrži informacije o certifikatu/ključu i pošiljatelju. Da bi se primatelju poruke omogućilo identificiranje pošiljatelja, dodaje se *KeyInfo* element koji sadrži informacije o pošiljatelju, njegov *base64* kodiran certifikat, serijski broj certifikata i informacije o izdavatelju certifikata.

5.5. *XMLSec* sigurnosna knjižnica

Posebnost pri Android implementaciji opisanog postupka fiskalizacije je upotreba *XMLSec* (skraćeno od *XML Security*, `org.apache.xml.security` paketi [5]) knjižnice u Android aplikaciji. Zbog nedostatka knjižnice za digitalno potpisivanje XML dokumenta u osnovnom Android SDK, autori ovog članka koristili su standardnu knjižnicu za digitalno potpisivanje programskog jezika *Java*. Unatoč tome da se programiranje aplikacija za Android sustav bazira na *Java* programskom jeziku, mnoge knjižnice standardnog sustava se zbog limitiranih resursa samih uređaja ne uključuju u Android sustav. Uz određene preinake na samoj knjižnici moguće ih je prevesti i koristiti na sustavu Android. Važno je napomenuti da se u praksi ovakva upotreba nestandardnih knjižnica ne preporuča, osim ako se ne obrati posebna pozornost prilikom prilagođavanja istih Android sustavu. Da bi se koristila ova knjižnica potrebno je preuzeti izvorni kod s interneta te ga prekompajlirati tako da se iz knjižnice izbaci *javax* paket klasa. Time ostaju samo knjižnice *Apache Santuario* projekta [5]. *Javax* treba izbaciti zbog međudjelovanja s ostalim paketima, odnosno klase objekata koje se nalaze u ovom paketu ovise o drugim klasama koje se ne nalaze u Android sustavu. Za digitalno potpisivanje dokumenta dovoljne su klase koje se nalaze u *Apache Santuario* dijelu knjižnice. Također, ova knjižnica podliježe *w3c* standardu koji zahtijeva CIS.

5.6. Poruka odgovora na prijavu

Poruka odgovora na prijavu računa pokriva dvije mogućnosti: mogućnost pogreške i mogućnost ispravne prijave računa. U slučajevima u kojima CIS u zahtjevu detektira neke neispravnosti, na prijavu se odgovara opisom pogreške. Ako je zahtjev korektno formiran, CIS odgovara obvezniku fiskalizacije s JIR-om koji je obveznik fiskalizacije dužan ispisati na račun. Poruka odgovora je također potpisana digitalnim certifikatom. Uređaj obveznika fiskalizacije provjerava potpis i utvrđuje da je uređaj s kojega je poslana poruka odgovora taj kojim se predstavlja da jest.

Nakon uspješne prijave računa, JIR, kao kontrolni broj kojeg generira sustav porezne uprave, postaje sastavni dio računa i porezni obveznik ga je dužan ispisati na računu zajedno sa ZKI i ostalim propisanim elementima računa.

6. IMPLEMENTACIJA NA ANDROID UREĐAJU

Do sada je opisivan princip rada modula za fiskalizaciju na Android uređaju. Konceptualno, nema razlika u izvedbi rješenja fiskalizacije i za druge platforme. No, osim tog modula aplikacija obveznika fiskalizacije dužna je osigurati i niz drugih funkcionalnosti kao npr. spremanje računa, spremanje zaštitnog koda koji je izračunao (ZKI) uređaj obveznika

fiskalizacije, te spremanje JIR-a dobivenog od CIS-a u internu bazu podataka. Funkcionalna aplikacija može (ili mora) uključiti i bazu podataka s uslugama i artiklima koje obveznik nudi svojim kupcima. Zapravo aplikacija sadrži sve bitne dijelove dosad uobičajenih blagajni, uz dodatak fiskalizacijskog modula za ispunjenje novih, Zakonom o fiskalizaciji definiranih propisa. Komunikacija s CIS-om se odvija u odvojenoj dretvi zbog mogućnosti odvijanja drugih radnji na uređaju i zbog toga jer sam Android sustav zahtijeva da se komunikacija s internetom odvija u odvojenim dretvama da bi aplikacija mogla nesmetano komunicirati s korisnikom. Da se izbjegne blokada sučelja aplikacije koristi se preporučeni *AsyncTask* razred [6]. Osim toga, izvedeno je i ispisivanje na *Bluetooth* mobilni POS pisač koje se također odvija u odvojenoj dretvi.

Aplikacija mora omogućiti kontrolu toka te mora ponuditi mogućnost odluke korisnika u slučaju nedostupnosti interneta, onda kada pisač ne reagira, račun sadrži grešku i sl. U slučaju nedostupnosti mreže ili CIS-a račun se ispisuje bez JIR-a, ali postoji obaveza (samim time i nužnost za implementaciju te funkcionalnosti) naknadne prijave računa i evidentiranje dodijeljenog JIR-a (iako je kupac dobio račun bez JIR-a, provjerom u Poreznoj upravi pomoću ZKI je moguće utvrditi je li račun fiskaliziran). Radi kasnije kontrole računa poželjno je omogućiti i naknadni pregled računa, ispisivanje istih te uvesti i dodatne funkcije za kalkulacije dnevnog, tjednog i mjesečnog prometa, ovisno o želji i potrebama obveznika fiskalizacije. Ovisno o složenosti cjelokupnog poslovnog sustava, može se pojaviti i potreba za sinkronizacijom između mobilnog uređaja i uredskog sustava i sl.

Iako je ovim člankom primarno opisivan postupak prijave računa, postupak fiskalizacije uključuje i neke druge funkcionalnosti poput prijave poslovnog prostora. S obzirom na to da se radi o jednokratnoj aktivnosti, ista se može provesti i korištenjem drugih pomoćnih alata: npr. u standardnom računovodstvenom softveru korištenom u uredu opisano rješenje prije svega se orijentira na mobilnu prodaju, odnosno na korištenje mobilne Android platforme. Sama prijava prostora ne razlikuje se mnogo od prijave računa. Tehničkom specifikacijom definirani su elementi XML prijave, a daljnji postupak je vrlo sličan prijavi računa. XML prijava se potpisuje i šalje u CIS, očita dobiveni odgovor i reagira ovisno o njemu.

7. ZAKLJUČAK

Ovim člankom opisuju se određeni koraci u razvoju aplikacijskog modula za fiskalizaciju računa izvedenom za Android mobilnu platformu. Naglasak je stavljen na opis koncepta fiskalizacije i na opis realizacije pojedinih ključnih faza u razvoju modula za provođenje prijave računa Poreznoj upravi. Iako je izneseni pristup orijentiran na Android platformu, temelj razvoja sličnih rješenja za druge platforme je identičan.

Detalji o korištenim strukturama zapisa nisu u cijelosti spomenuti s obzirom na to da je riječ o elementima koji su definirani u tehničkoj specifikaciji [2] koju je izdalo Ministarstvo financija, pa se čitatelji zainteresirani za izvedbu implementacije prije svega upućuju na proučavanje tog dokumenta.

Aplikacija unutar koje je implementiran opisani modul uključuje i druge funkcionalnosti koje osiguravaju korisniku jednostavnu mobilnu prodaju proizvoda ili usluga. Sam fiskalni modul može se uz neznatne preinake iskoristiti i u drugim tipovima specijaliziranih aplikacija za naplatu, npr. naplata naknade za taxi usluge i sl.

8. LITERATURA

[1] Zakon o fiskalizaciji u prometu gotovinom, Narodne novine 133/12, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2822.html

[2] Fiskalizacija – Tehnička specifikacija za korisnike, v1.2, Ministarstvo financija; APIS IT, 2012.

[3] http://en.wikipedia.org/wiki/Certificate_authority

[4] FINA Centar za registre digitalnih certifikata - RDC, http://rdc.fina.hr/

[5] http://santuario.apache.org/

[6] http://developer.android.com/reference/android/os/AsyncTask.html

Kontakt autora:

mr.sc. Matija Mikac, dipl.ing.el.
VELV - Veleučilište u Varaždinu
e-mail: *matija.mikac@velv.hr*

Dražen Hižak, bacc.ing.el.
VELV – bivši student (2012.)
e-mail: *drazen.hizak@gmail.com*