Fiskalizacija - Tehnička specifikacija za korisnike

Verzija 1.1

Povijest promjena na dokumentu

Broj verzije	Datum verzije	Kratki opis promjena	Autor
1.0	5.10.2012.	Inicijalna verzija dokumenta.	APIS IT
1.1	29.10.2012.	Izmjene i dopune u poglavljima 2.1.2, 2.1.3, 2.1.4, 2.2.1, 2.2.3, 2.2.4, 2.3, 2.3.1, 2.3.2, 3.3, 4.2, 8.8, 9, 10, 12, 12.1, 12.2, 12.3, 13.	APIS IT

Sadržaj

Fiskalizacija - Tehnička specifikacija za korisnike

1. Uvod

Ovim dokumentom opisuje se način informatičkog povezivanja centralnog informacijskog sustava za Fiskalizaciju kod Porezne uprave i obveznika fiskalizacije. Dokument je namijenjen svim zainteresiranim stranama koje će sudjelovati u implementaciji rješenja na strani obveznika fiskalizacije.

Dokumentom se opisuju sve poruke koje sustavi razmjenjuju, procesi razmjene poruka, definiraju se podatkovni skupovi i pravila koja je nužno poštivati u komunikaciji.

Razmjena podataka odvijat će se putem Web servisa korištenjem XML poruka. Upravo takav način razmjene podataka nije ovisan ni o tehnologiji koju koriste obveznici fiskalizacije ni o tehnologiji koju koristi Porezna uprava i omogućuje uniformnu komunikaciju između bilo kojeg obveznika fiskalizacije i Porezne uprave.

U ovoj verziji dokumenta navedene su sve potrebne informacije i opisan je proces povezivanja na testni sustav.

U konačnoj verziji dokumenta, koji će biti objavljen naknadno, biti će navedene i informacije za povezivanje na produkcijski sustav.

1.1 Definicije i skraćenice

Pojam	Opis
CIS	Centralni informacijski sustav Ministarstva financija, Porezne uprave
Korisnik sustava	Obveznik fiskalizacije
JIR	Jedinstveni identifikator računa

2. Poslovna interakcija korisnika sustava

Postoje dva tipa poslovnih poruka koje su obveznici fiskalizacije dužni dostavljati Poreznoj upravi:

1. Račun
2. Podaci o poslovnom prostoru

Osim razmjene poslovnih poruka servisom je predviđena mogućnost provjere dostupnosti servisa tehničkom porukom *echo*.

Za svaki tip poruke se u nastavku opisuje proces slanja poruke, podatkovni skup, poslovna pravila povezana s porukom i ostale bitne informacije. Također, opisuju se i poruke odgovora koje vraća CIS kao i šifarnik mogućih grešaka koje se mogu pojaviti prilikom razmjene poruka.

2.1 Račun

Obveznik fiskalizacije dostavlja podatke o računu pojedinačno za svaki izdani račun u trenutku izdavanja računa. Iznimno, podaci o računu se mogu dostaviti i naknadno ali samo u izuzetnim situacijama predviđenim Zakonom. U oba slučaja je proces dostave podataka identičan što se tiče komunikacije s CIS-om.

Proces razmjene podataka započinje u trenutku kad operater na naplatnom uređaju (blagajnik) treba izdati kupcu račun. Naplatni uređaj (ili informacijski sustav) obveznika fiskalizacije priprema podatke za račun i temeljem istih izračunava zaštitni kod izdavatelja sukladno algoritmu opisanom u poglavlju 12. Nakon toga priprema XML poruku zahtjeva i elektronički ju potpisuje s privatnim ključem DEMO aplikativnog certifikata koji je izdan obvezniku u svrhu fiskalizacije. Nakon toga inicira 1-way SSL komunikaciju pri čemu se poslužitelj Porezne uprave predstavlja s DEMO poslužiteljskim certifikatom *cistest.apis-it.hr*. Nakon uspješno uspostavljene SSL komunikacije vrši poziv servisa.

CIS zaprima i obrađuje poruku zahtjeva. Ako je zahtjev uspješno obrađen CIS priprema XML poruku odgovora koja sadrži JIR, elektronički ju potpisuje s privatnim ključem DEMO aplikativnog certifikata *fiskalcistest* i šalje naplatnom uređaju (ili informacijskom sustavu) obveznika.

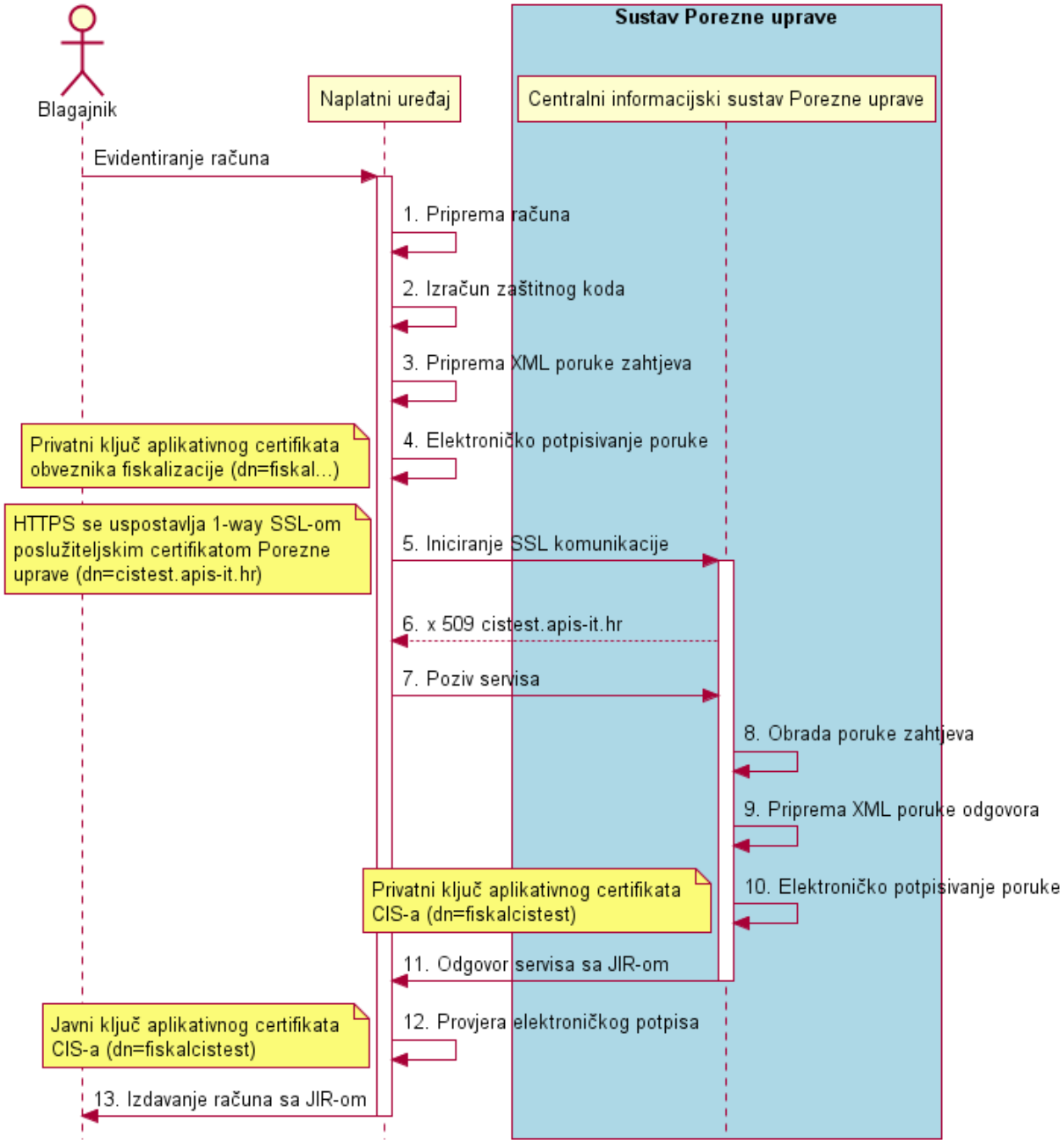
Naplatni uređaj (ili informacijski sustav) obveznika zaprima poruku odgovora i provjerava elektronički potpis s javnim ključem DEMO aplikativnog certifikata *fiskalcistest*. Nakon toga operater na naplatnom uređaju (blagajnik) izdaje kupcu račun s ispisanim JIR-om. Prije opisani proces prikazan je slijednim dijagramom na slici 1.

U slučaju da se prilikom obrade poruke zahtjeva dogodi greška (poruka neispravna po XML shemi, neispravan elektronički potpis i sl.) CIS vraća XML poruku odgovora koja sadrži opis greške. U tom slučaju odgovor ne sadrži JIR i operater na naplatnom uređaju (blagajnik) izdaje kupcu račun bez JIR-a. Poslovni proces izdavanja računa kupcu ne smije biti onemogućen zbog nastale greške ali obveznik fiskalizacije je dužan ispraviti nepravilnosti u slanju poruke i poruku naknadno dostaviti. Proces u slučaju greške je prikazan slijednim dijagramom na slici 2.

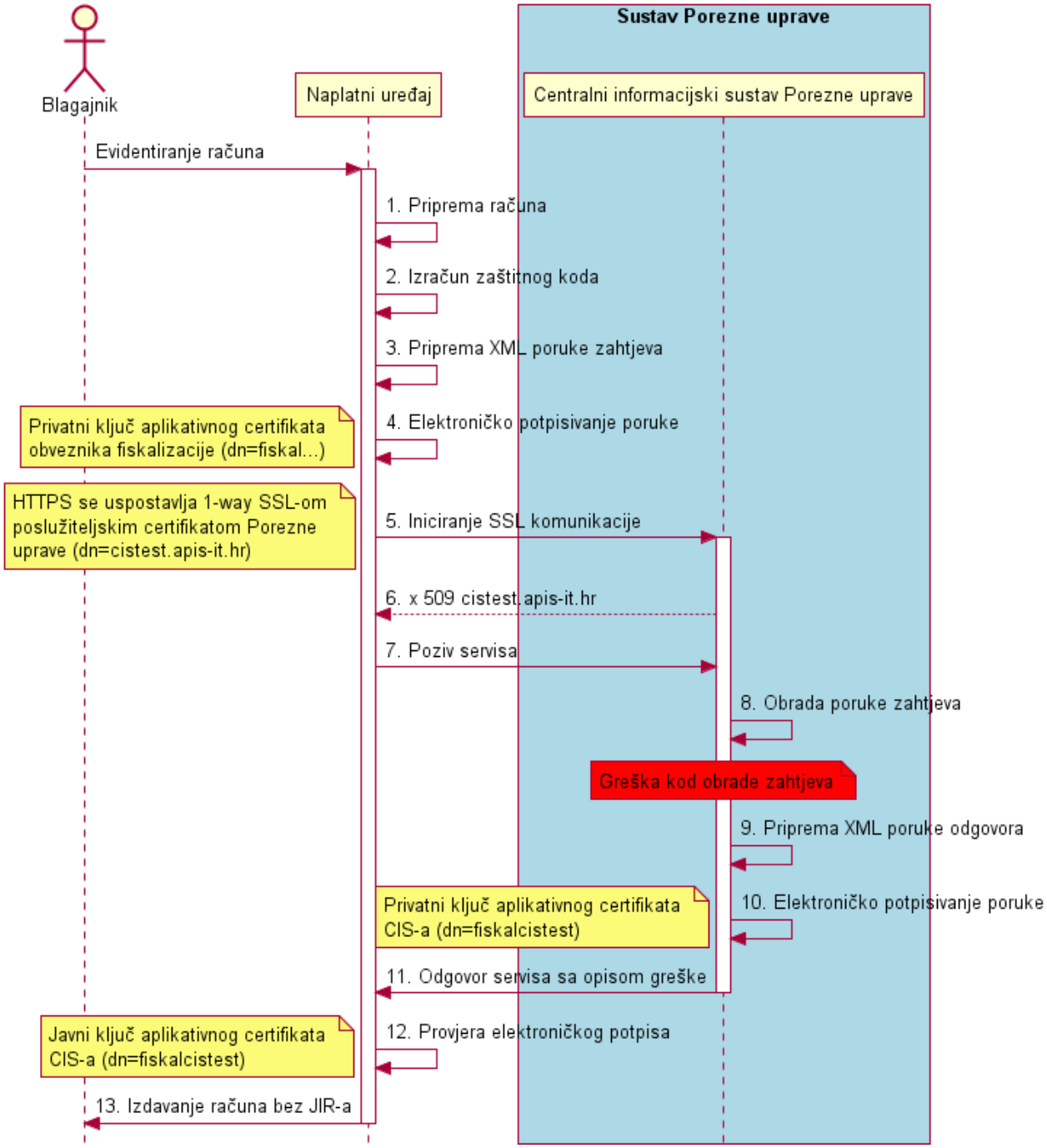
U svim slučajevima kad obveznik iz nekog razloga nije dobio JIR za izdani račun (prekid Internet veze, potpuni prestanka rada naplatnog uređaja, greška u poruci odgovora, privremena nedostupnost CIS-a) obveznik je dužan naknadno ponoviti slanje poruke. Tek kad obveznik dobije ispravnu poruku odgovora od CIS-a koja sadrži JIR može smatrati da je račun prijavljen Poreznoj upravi.

U slučajevima kad obveznik ne može dobiti JIR, npr. prekid Internet veze, i veza se ponovo uspostavi prioritet imaju poruke kojima se prijavljuju tekući računi koji se izdaju kako bi oni dobili JIR. Poruke koje nisu dobile JIR treba dostaviti naknadno u periodu manjeg opterećenja. U budućim verzijama dokumenta tehničke specifikacije mogu se propisati protokoli i preporuke za slanje veće količine poruka koje nisu dostavljene Poreznoj upravi.

Maksimalno vrijeme (*time-out*) koje naplatni uređaj (ili informacijski sustav) obveznika treba čekati poruku odgovora s JIR-om od CIS-a određuje obveznik. Obveznik treba napraviti procjenu vremena uzimajući u obzir vrstu i dostupnost Internet veze koju koristi i poslovno prihvatljivo vrijeme za dobivanje odgovora. Kod procjene u obzir treba uzeti i maksimalno vrijeme od 2 sekunde u kojem CIS treba obraditi poruku zahtjeva i vratiti poruku odgovora (vrijeme od trenutka ulaska poruke zahtjeva u CIS do trenutka izlaska poruke odgovora iz CIS-a).



Slika 1. Slijedni dijagram procesa za slanje računa



Slika 2. Slijedni dijagram procesa za slanje računa u slučaju greške

2.1.1 Podatkovni skup zahtjeva za račun

U tablici u nastavku opisan je podatkovni skup poruke zahtjeva za račun.

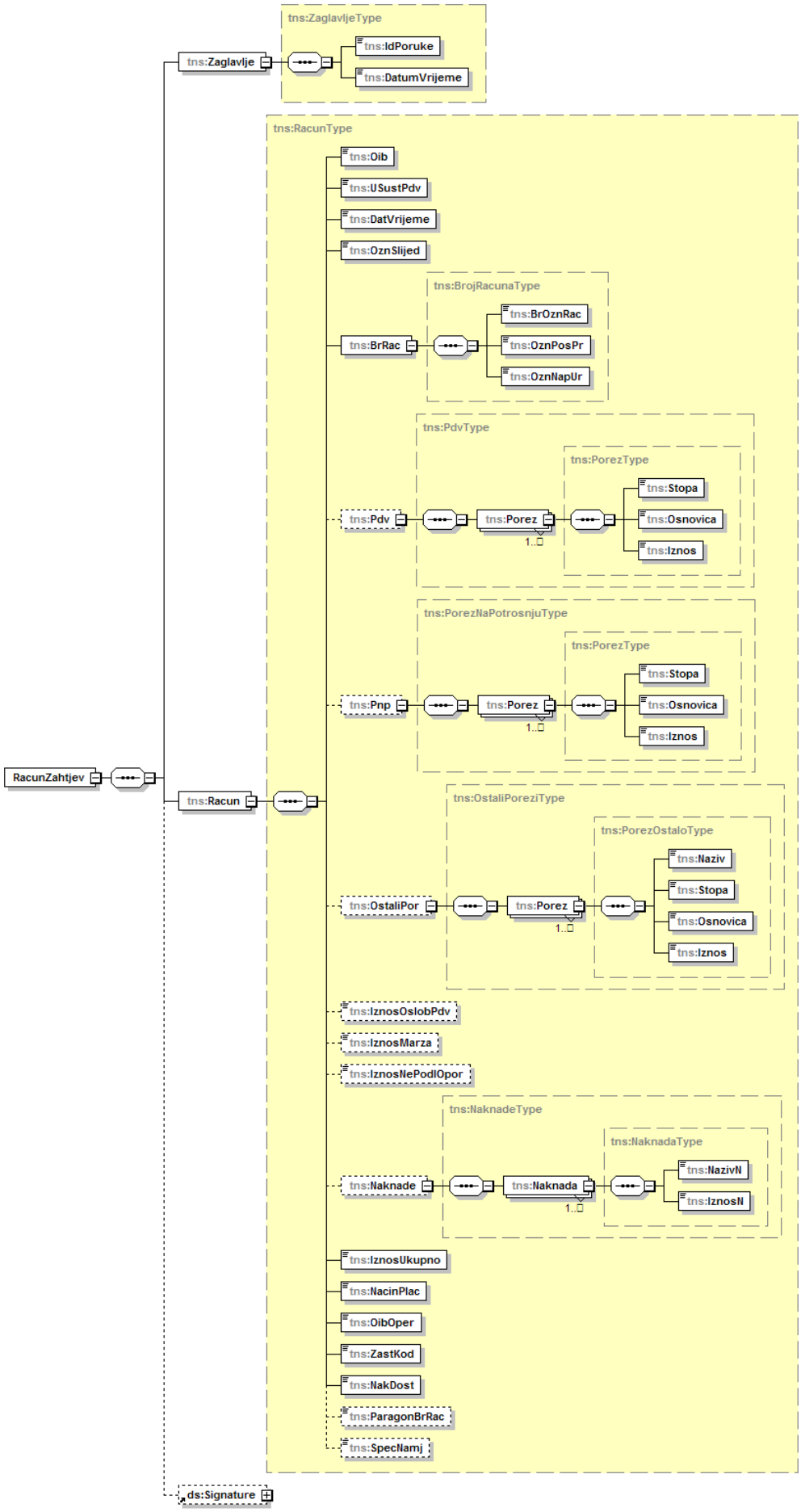
Podatak	Opis/Napomena	Obavezan DA/NE	Tip/Duljina
Zaglavlje			
Identifikator poruke	ID poruke (UUID). Svaka poruka koja se šalje prema CIS-u mora sadržavati različiti ID poruke. Isto vrijedi i u slučaju kad se ponavlja slanje poruke zbog greške u razmjeni poruka.	DA	Char(36)
Datum i vrijeme slanja	Datum i vrijeme slanja poruke zahtjeva. dd.mm.ggggThh:mm:ss	DA	Date & Time
Račun			
OIB	OIB obveznika fiskalizacije.	DA	Char(11)
U sustavu PDV	Oznaka je li obveznik u sustavu PDV-a ili nije. *True* ako je obveznik u sustavu PDV-a, u suprotnom *false*. Boolean (1-true/0-false)	DA	Boolean
Datum i vrijeme izdavanja	Datum i vrijeme izdavanja koji se ispisuju na računu. dd.mm.ggggThh:mm:ss	DA	Date & Time
Oznaka slijednosti	Oznaka slijednosti brojeva računa. Oznaka koja govori gdje se određuje dodjela broja računa tj. dodjeljuje li se broj računa centralno na razini poslovnog prostora ili pojedinačno na svakom naplatnom uređaju. Dodjela brojeva računa može biti na razini poslovnog prostora ili naplatnog uređaja: P - na nivou poslovnog prostora N - na nivou naplatnog uređaja	DA	Char(1)
Broj računa	Propisati će se izgled broja računa kako se treba ispisivati na fizičkom računu u sljedećem obliku: brojčana oznaka računa/oznaka poslovnog prostora/oznaka naplatnog uređaja Primjer: 1234567890/POSL1/12 Podaci će se Poreznoj upravi dostavljati odvojeni u XML-u radi kasnije lakše manipulacije u izvještajima i analizama.	DA	
Brojčana oznaka računa	Može sadržavati samo znamenke 0-9. Nisu dozvoljene vodeće nule.	DA	Varchar(20)
Oznaka poslovnog prostora	Može sadržavati samo znamenke i slova 0-9, a-z, A-Z. Mora biti jedinstvena na razini OIB-a obveznika.	DA	Varchar(20)
Oznaka naplatnog uređaja	Može sadržavati samo znamenke 0-9. Nisu dozvoljene vodeće nule. Mora biti jedinstvena na razini jednog poslovnog prostora obveznika.	DA	Varchar(20)
PDV	Porez na dodanu vrijednost.	NE	

	Podatak se dostavlja Poreznoj upravi samo ako na računu postoji PDV. Podatak se sastoji od porezne stope, osnovice i iznosa poreza. Može postojati lista poreznih stopa.		
Porezna stopa	Iznos porezne stope. Npr. stopa od 25,00% se dostavlja kao 25.00.	DA, ako postoji porez	Decimal(3,2)
Osnovica	Iznos osnovice.	DA, ako postoji porez	Decimal(15,2)
Iznos poreza		DA, ako postoji porez	Decimal(15,2)
PNP	Porez na potrošnju. Podatak se dostavlja Poreznoj upravi samo ako na računu postoji porez na potrošnju. Podatak se sastoji od porezne stope, osnovice i iznosa poreza. Može postojati lista poreznih stopa.	NE	
Porezna stopa	Iznos porezne stope. Npr. stopa od 3,00% se dostavlja kao 3.00.	DA, ako postoji porez	Decimal(3,2)
Osnovica	Iznos osnovice.	DA, ako postoji porez	Decimal(15,2)
Iznos poreza		DA, ako postoji porez	Decimal(15,2)
Ostali porezi	Ostali porezi koji se mogu pojaviti na računu osim PDV-a i poreza na potrošnju. Podatak se dostavlja Poreznoj upravi samo ako na računu postoje ostali porezi. Podatak se sastoji od naziva poreza, porezne stope, osnovice i iznosa poreza. Može postojati lista poreza.	NE	
Naziv poreza	Naziv poreza za koji se šalju podaci. Npr. Porez na luksuz.	DA, ako postoji porez	Varchar(100)
Porezna stopa	Iznos porezne stope. Npr. stopa od 15,00% se dostavlja kao 15.00.	DA, ako postoji porez	Decimal(3,2)
Osnovica	Iznos osnovice.	DA, ako postoji porez	Decimal(15,2)
Iznos poreza		DA, ako postoji porez	Decimal(15,2)
Iznos oslobođenja	Ukupni iznos oslobođenja na računu. Oslobođenja u slučajevima kada se isporučuju dobra ili obavljaju usluge koje su oslobođene od plaćanja PDV-a. Podatak se dostavlja Poreznoj upravi samo ako na računu postoji oslobođenje.	NE	Decimal(15,2)
Iznos na koji se odnosi poseban postupak oporezivanja marže	Ukupni iznos na koji se odnosi poseban postupak oporezivanja marže na računu. Marža za rabljena dobra, umjetnička djela, kolekcionarske ili antikne predmete (članak	NE	Decimal(15,2)

	22.a Zakona o PDV-u). Podatak se dostavlja Poreznoj upravi samo ako na računu postoji poseban postupak oporezivanja marže.		
Iznos koji ne podliježe oporezivanju	Ukupni iznos koji ne podliježe oporezivanju na računu. Podatak se dostavlja Poreznoj upravi samo ako na računu postoji iznos koji ne podliježe oporezivanju.	NE	Decimal(15,2)
Naknade	Naknade koje se mogu pojaviti na računu tipa povratne naknade za ambalažu i sl. Podatak se dostavlja Poreznoj upravi samo ako na računu postoje naknade. Podatak se sastoji od naziva naknade i iznosa naknade. Može postojati lista naknada.	NE	
Naziv naknade	Opisno naziv naknade.	DA, ako postoji naknada	Varchar(100)
Iznos naknade		DA, ako postoji naknada	Decimal(15,2)
Ukupan iznos	Ukupan iznos iskazan na računu.	DA	Decimal(15,2)
Način plaćanja	G – gotovina K – kartice C – ček T – transakcijski račun O – ostalo U slučaju više načina plaćanja po jednom računu, isto je potrebno prijaviti pod 'Ostalo'. Za sve načine plaćanja koji nisu prije navedeni koristiti će se oznaka 'Ostalo'.	DA	Char(1)
OIB operatera na naplatnom uređaju	OIB operatera na naplatnom uređaju koji izdaje račun. U slučaju samouslužnih naplatnih uređaja i automata potrebno je dostaviti OIB izdavatelja (OIB s računa).	DA	Char(11)
Zaštitni kod izdavatelja	Zaštitni kod izdavatelja obveznika fiskalizacije je alfanumerički zapis kojim se potvrđuje veza između obveznika fiskalizacije i izdanog računa. Zaštitni kod generira obveznik fiskalizacije sukladno algoritmu opisanom u poglavlju 12 ovog dokumenta i ispisuje na računu. 32-znamenkasti broj zapisan u heksadecimalnom formatu. Može sadržavati znamenke 0-9 i mala slova a-f. Primjer: e4d909c290d0fb1ca068ffaddf22cbd0	DA	Char(32)
Oznaka naknadne dostave računa	Pod naknadnom dostavom računa Poreznoj upravi smatra se situacija kad je isti prethodno izdan kupcu bez JIR-a (npr. prekid Internet veze ili potpuni prestanak rada naplatnog uređaja). *True* ako je riječ o naknadnoj dostavi računa, u suprotnom *false*. Boolean (1-true/0-false)	DA	Boolean

Oznaka paragon računa	Dostavlja se samo u slučaju potpunog prestanka rada naplatnog uređaja kada obveznik fiskalizacije mora prepisati izdane paragon račune i prijaviti ih putem poruke Poreznoj upravi.	NE	Varchar(100)
Specifična namjena	Predviđeno za slučaj da se naknadno pojavi potreba za dostavom podataka koji nisu prepoznati tokom analize.	NE	Varchar(1000)

Na slici 3 u nastavku pregledno je prikazana shema poruke zahtjeva za račun.



Slika 3. Shema poruke zahtjeva za račun

2.1.2 Primjer poruke zahtjeva za račun

U nastavku je naveden primjer poruke zahtjeva za račun. Napomena: Podaci navedeni u primjeru su testni i ne moraju biti poslovno ispravni ili logični.

```
<tns:RacunZahtjev
 xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <tns:Zaglavlje>
  <tns:IdPoruke>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</tns:IdPoruke>
  <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
 </tns:Zaglavlje>
 <tns:Racun>
  <tns:Oib>98765432198</tns:Oib>
  <tns:USustPdv>true</tns:USustPdv>
  <tns:DatVrijeme>01.09.2012T21:10:34</tns:DatVrijeme>
  <tns:OznSlijed>P</tns:OznSlijed>
  <tns:BrRac>
   <tns:BrOznRac>123456789</tns:BrOznRac>
   <tns:OznPosPr>POSL1</tns:OznPosPr>
   <tns:OznNapUr>12</tns:OznNapUr>
  </tns:BrRac>
  <tns:Pdv>
   <tns:Porez>
    <tns:Stopa>25.00</tns:Stopa>
    <tns:Osnovica>10.00</tns:Osnovica>
    <tns:Iznos>2.50</tns:Iznos>
   </tns:Porez>
   <tns:Porez>
    <tns:Stopa>10.00</tns:Stopa>
    <tns:Osnovica>10.00</tns:Osnovica>
    <tns:Iznos>1.00</tns:Iznos>
   </tns:Porez>
   <tns:Porez>
    <tns:Stopa>0.00</tns:Stopa>
    <tns:Osnovica>10.00</tns:Osnovica>
    <tns:Iznos>0.00</tns:Iznos>
   </tns:Porez>
  </tns:Pdv>
  <tns:Pnp>
   <tns:Porez>
    <tns:Stopa>3.00</tns:Stopa>
    <tns:Osnovica>10.00</tns:Osnovica>
    <tns:Iznos>0.30</tns:Iznos>
   </tns:Porez>
  </tns:Pnp>
  <tns:OstaliPor>
   <tns:Porez>
    <tns:Naziv>Porez na luksuz</tns:Naziv>
    <tns:Stopa>15.00</tns:Stopa>
    <tns:Osnovica>10.00</tns:Osnovica>
    <tns:Iznos>1.50</tns:Iznos>
   </tns:Porez>
  </tns:OstaliPor>
  <tns:IznosOslobPdv>12.00</tns:IznosOslobPdv>
  <tns:IznosMarza>13.00</tns:IznosMarza>
  <tns:Naknade>
   <tns:Naknada>
    <tns:NazivN>Povratna naknada</tns:NazivN>
    <tns:IznosN>1.00</tns:IznosN>
   </tns:Naknada>
  </tns:Naknade>
  <tns:IznosUkupno>30.00</tns:IznosUkupno>
```

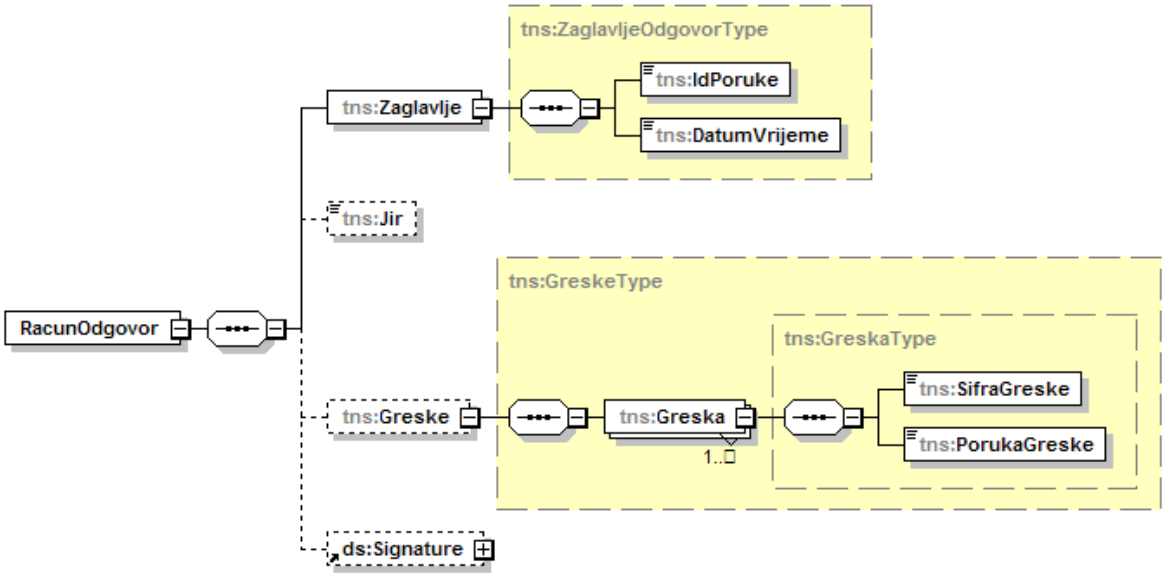
```
    <tns:NacinPlac>K</tns:NacinPlac>
    <tns:OibOper>01234567890</tns:OibOper>
    <tns:ZastKod>e4d909c290d0fb1ca068ffaddf22cbd0</tns:ZastKod>
    <tns:NakDost>false</tns:NakDost>
    <tns:ParagonBrRac>123/458/5</tns:ParagonBrRac>
    <tns:SpecNamj>Navedeno kao primjer</tns:SpecNamj>
  </tns:Racun>
</tns:RacunZahtjev>
```

2.1.3 Podatkovni skup odgovora za račun

U tablici u nastavku opisan je podatkovni skup poruke odgovora za račun.

Podatak	Opis/Napomena	Obvezan DA/NE	Tip/Duljina
Zaglavlje			
Identifikator poruke	ID poruke (UUID). Kao identifikator poruke odgovora uzima se ID iz poruke zahtjeva.	DA	Varchar(0-36)
Datum i vrijeme obrade	Datum i vrijeme obrade poruke zahtjeva. dd.mm.ggggThh:mm:ss	DA	Date & Time
Jedinstveni identifikator računa			
JIR	Jedinstveni identifikator računa. U slučaju greške, JIR se ne šalje u odgovoru.	NE	Char(36)
Greške			
Šifra greške	Šifra greške je u formatu sXXX gdje je XXX troznamenkasti prirodni broj. Šifre grešaka sukladno šifarniku grešaka.	DA, ako ima grešaka	Varchar(4)
Poruka	Poruka greške je tekstualni opis greške sukladno šifarniku grešaka.	DA, ako ima grešaka	Varchar(500)

Na slici 4 u nastavku pregledno je prikazana shema poruke odgovora za račun.



Slika 4. Shema poruke odgovora za račun

2.1.4 Primjer poruke odgovora za račun

A. Primjer odgovora (bez greške)

```
<tns:RacunOdgovor xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <tns:Zaglavlje>
    <tns:IdPoruke>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</tns:IdPoruke>
    <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
  </tns:Zaglavlje>
  <tns:Jir>2cf55235-9470-4b5c-a539-463f52b109d2</tns:Jir>
</tns:RacunOdgovor>
```

B. Primjer odgovora (s greškom: Certifikat nije izdan od strane FINA-e)

```
<tns:RacunOdgovor xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <tns:Zaglavlje>
    <tns:IdPoruke>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</tns:IdPoruke>
    <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
  </tns:Zaglavlje>
  <tns:Greske>
    <tns:Greska>
      <tns:SifraGreske>s002</tns:SifraGreske>
      <tns:PorukaGreske>Certifikat nije izdan od strane FINA-e.</tns:PorukaGreske>
    </tns:Greska>
  </tns:Greske>
</tns:RacunOdgovor>
```

2.2 Podaci o poslovnom prostoru

Obveznik fiskalizacije inicijalno dostavlja podatke o poslovnim prostorima prilikom uključivanja u sustav fiskalizacije za sve poslovne prostore u kojima izdaje račune, a koji podliježu fiskalizaciji.

Nakon toga obveznik dostavlja podatke za svaki novootvoreni poslovni prostor kao i promjene za postojeći. Tipovi promjena koje je potrebno dostaviti:

- promjena adrese,
- promjena radnog vremena,
- poslovni prostor se zatvara tj. prestaje s radom.

Obveznik fiskalizacije dostavlja pojedinačno podatke za svaki poslovni prostor. Podatke o poslovnom prostoru je potrebno dostaviti prije slanja prvog računa koji se odnosi na taj poslovni prostor.

Proces razmjene podataka započinje u trenutku kad obveznik treba dostaviti podatke o poslovnom prostoru. Naplatni uređaj (ili informacijski sustav) obveznika priprema podatke o poslovnom prostoru. Nakon toga priprema XML poruku zahtjeva i elektronički ju potpisuje s privatnim ključem DEMO aplikativnog certifikata koji je izdan obvezniku u svrhu fiskalizacije. Nakon toga inicira 1-way SSL komunikaciju pri čemu se poslužitelj Porezne uprave predstavlja s DEMO poslužiteljskim certifikatom *cistest.apis-it.hr*. Nakon uspješno uspostavljene SSL komunikacije vrši poziv servisa.

CIS zaprima i obrađuje poruku zahtjeva. Ako je zahtjev uspješno obrađen CIS priprema XML poruku odgovora, elektronički ju potpisuje s privatnim ključem DEMO aplikativnog certifikata *fiskalcistest* i šalje naplatnom uređaju (ili informacijskom sustavu) obveznika.

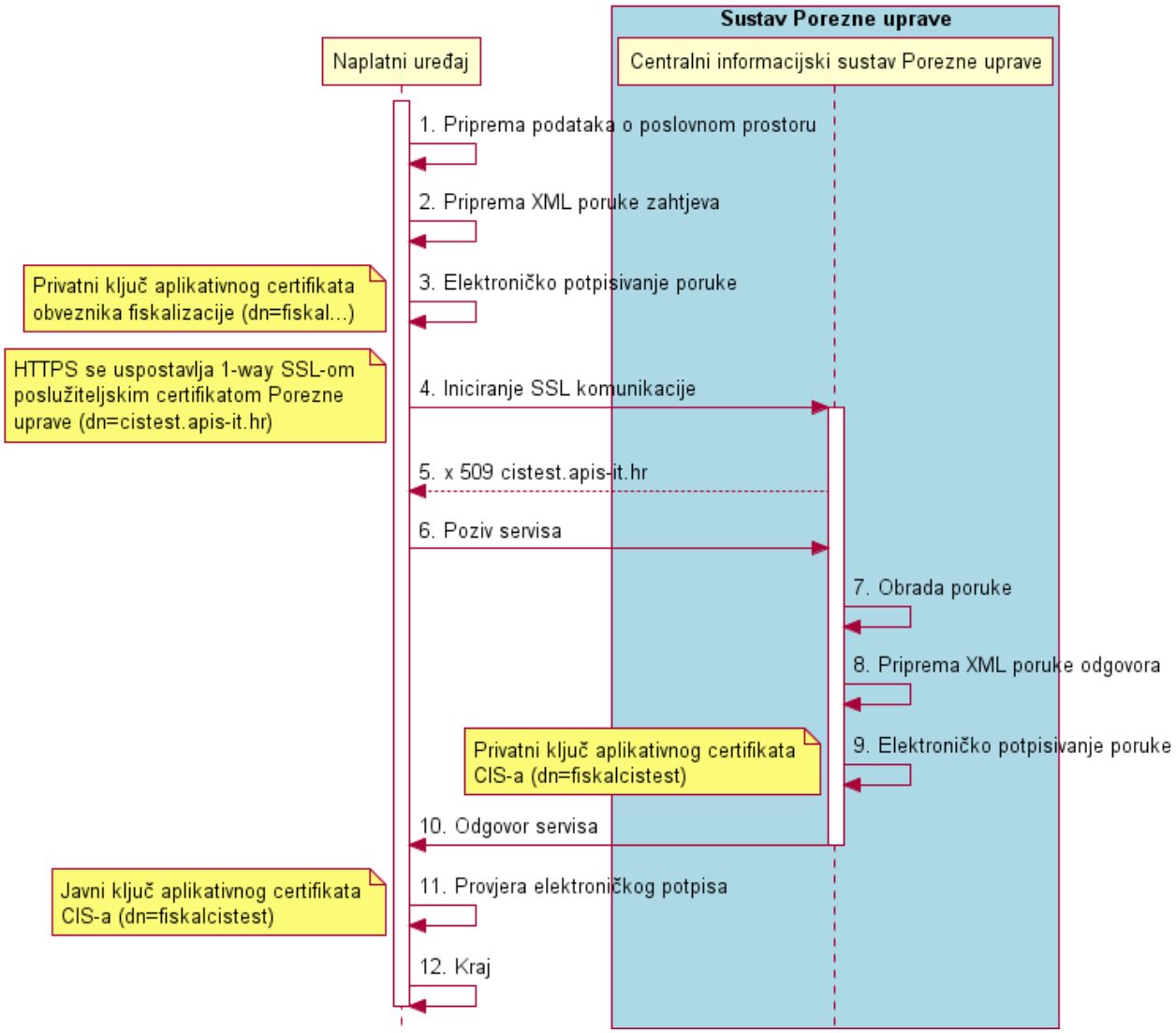
Naplatni uređaj (ili informacijski sustav) obveznika zaprima poruku odgovora i provjerava elektronički potpis s javnim ključem DEMO aplikativnog certifikata *fiskalcistest*. U slučaju da odgovor ne sadrži grešku proces završava. Prije opisani proces prikazan je slijednim dijagramom na slici 5.

U slučaju da se prilikom obrade poruke zahtjeva dogodi greška (poruka neispravna po XML shemi, neispravan elektronički potpis i sl.) CIS vraća XML poruku odgovora koja sadrži opis greške. Obveznik je dužan ispraviti nepravilnosti u slanju poruke i poruku naknadno dostaviti. Proces u slučaju greške je prikazan slijednim dijagramom na slici 6.

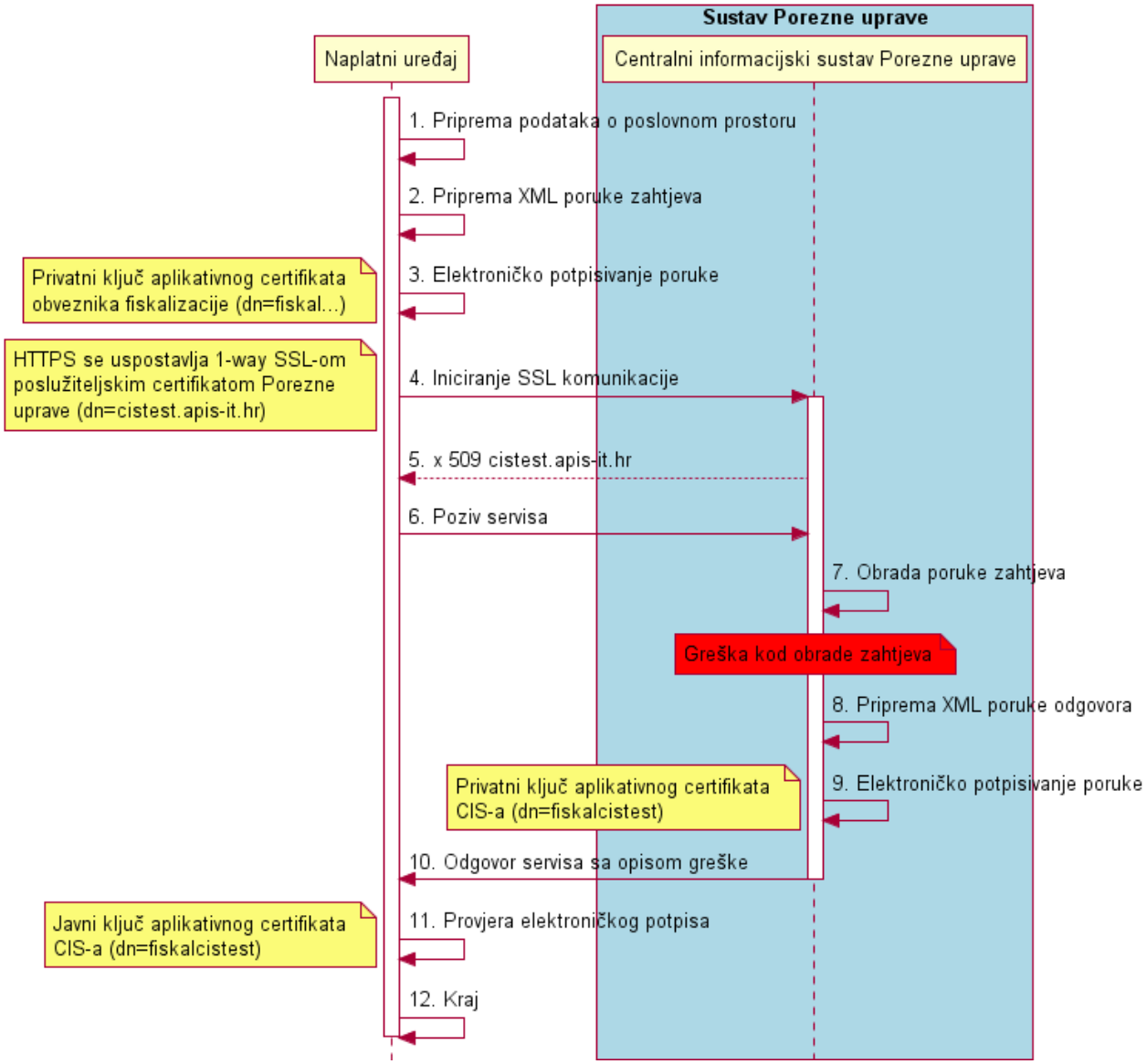
U svim slučajevima kad obveznik iz nekog razloga nije dobio poruku odgovora ili je dobio poruku odgovora koja sadrži grešku (prekid Internet veze, potpuni prestanka rada naplatnog uređaja, greška u poruci odgovora, privremena nedostupnost CIS-a) obveznik je dužan naknadno ponoviti slanje poruke. Tek kad obveznik dobije ispravnu poruku odgovora od CIS-a može smatrati da su podaci o poslovnom prostoru prijavljeni Poreznoj upravi.

Poruke koje nisu dostavljene Poreznoj upravi treba dostaviti naknadno u periodu manjeg opterećenja. U budućim verzijama dokumenta tehničke specifikacije mogu se propisati protokoli i preporuke za slanje veće količine poruka koje nisu dostavljene Poreznoj upravi.

Maksimalno vrijeme (*time-out*) koje naplatni uređaj (ili informacijski sustav) obveznika treba čekati poruku odgovora od CIS-a određuje obveznik. Prilikom procjene treba uzeti u obzir sve što je navedeno i u poglavlju gdje se opisuje proces dostave podataka za račun.



Slika 5. Slijedni dijagram procesa za slanje podataka o poslovnom prostoru



Slika 6. Slijedni dijagram procesa za slanje podataka o poslovnom prostoru u slučaju greške

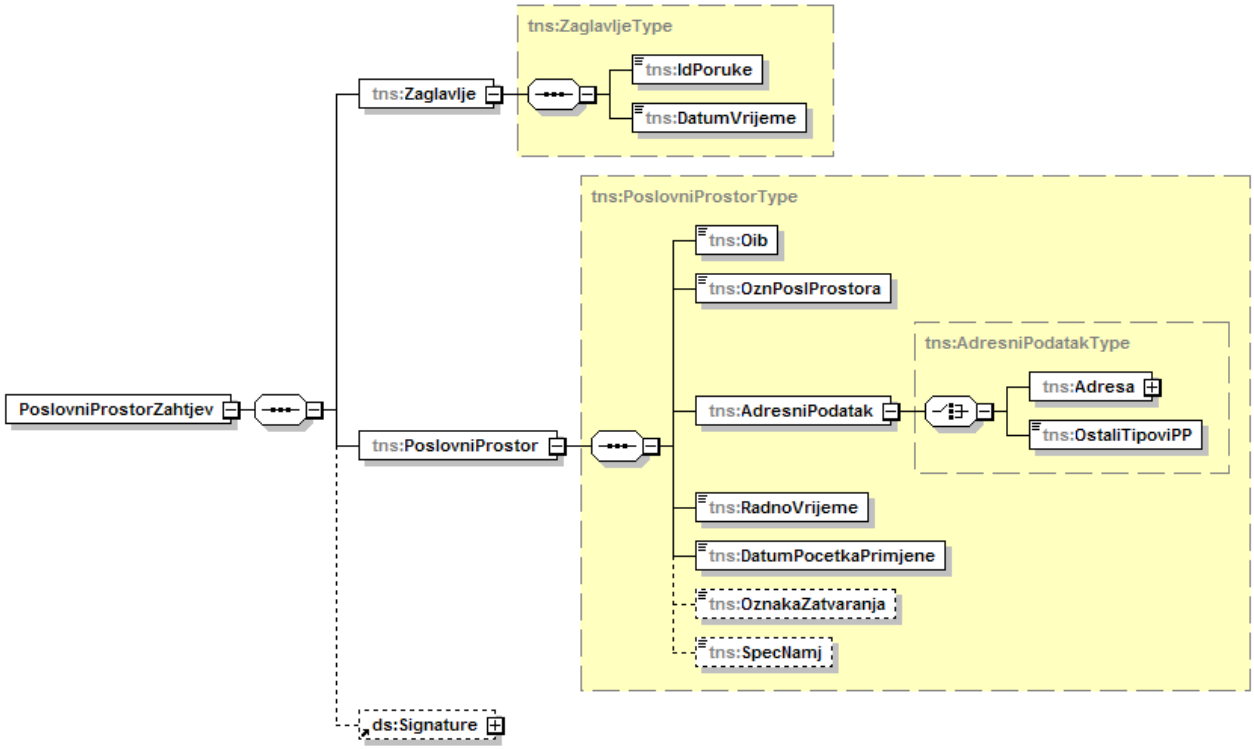
2.2.1 Podatkovni skup zahtjeva za podatke o poslovnom prostoru

U tablici u nastavku opisan je podatkovni skup poruke zahtjeva za podatke o poslovnom prostoru.

Podatak	Opis/Napomena	Obvezan DA/NE	Tip/Duljina
Zaglavlje			
Identifikator poruke	ID poruke (UUID). Svaka poruka koja se šalje prema CIS-u mora sadržavati različiti ID poruke. Isto vrijedi i u slučaju kad se ponavlja slanje poruke zbog greške u razmjeni poruka.	DA	Char(36)
Datum i vrijeme slanja	Datum i vrijeme slanja poruke zahtjeva. dd.mm.ggggThh:mm:ss	DA	Date & Time
Poslovni prostor			
OIB	OIB obveznika fiskalizacije.	DA	Char(11)

Oznaka poslovnog prostora	Može sadržavati samo znamenke i slova 0-9, a-z, A-Z. Oznaka mora biti ista kao ona koja se navodi na računima. Mora biti jedinstvena na razini OIB-a obveznika.	DA	Varchar(20)
Adresni podatak	Adresa ili opis tipa poslovnog prostora (npr. Internet trgovina) kada poslovni prostor nema adresu. Mora se dostaviti jedan od ta dva podatka.	DA	
Adresa	Adresa poslovnog prostora. Podatak se sastoji od ulice, kućnog broja, dodatka kućnom broju, broja pošte, naselja i općine.	NE	
Ulica		NE	Varchar(100)
Kućni broj		NE	Varchar(4)
Dodatak kućnom broju		NE	Varchar(4)
Broj pošte		NE	Varchar(12)
Naselje		NE	Varchar(35)
Općina		NE	Varchar(35)
Ostali tipovi poslovnog prostora	Predviđen je slobodan unos za specifične slučajeve kada ne postoji adresa poslovnog prostora (Internet trgovina, pokretna trgovina i sl).	NE	Varchar(100)
Radno vrijeme	Radno vrijeme poslovnog prostora. Predviđen je slobodan unos.	DA	Varchar(1000)
Datum početka primjene	Datum otkad vrijedi promjena. dd.mm.gggg	DA	Date
Oznaka zatvaranja	Podatak se dostavlja Poreznoj upravi samo ako se trajno zatvara poslovni prostor. U tom se slučaju dostavlja zadnje radno vrijeme i adresa ili opis tipa poslovnog prostora (jer su obavezni podaci u poruci). Moguća vrijednost je „Z". Nakon zatvaranja poslovnog prostora ne smiju se više dostavljati računi s oznakom tog poslovnog prostora.	NE	Char(1)
Specifična namjena	Potrebno je dostaviti jedan od podataka u nastavku: • OIB pravne ili fizičke osobe koja je proizvela programsko rješenje ili • OIB pravne ili fizičke osobe koja održava programsko rješenje ili • OIB pravne ili fizičke osobe prodavatelja u slučaju da se koristi rješenje od stranog proizvođača – bez lokalnog partnera	NE	Varchar(1000)

Na slici 7 u nastavku pregledno je prikazana shema poruke zahtjeva za podatke o poslovnom prostoru.



Slika 7. Shema poruke zahtjeva za podatke o poslovnom prostoru

2.2.2 *Primjer poruke zahtjeva za podatke o poslovnom prostoru*

U nastavku je naveden primjer poruke zahtjeva za podatke o poslovnom prostoru. Napomena: Podaci navedeni u primjeru su testni i ne moraju biti poslovno ispravni ili logični.

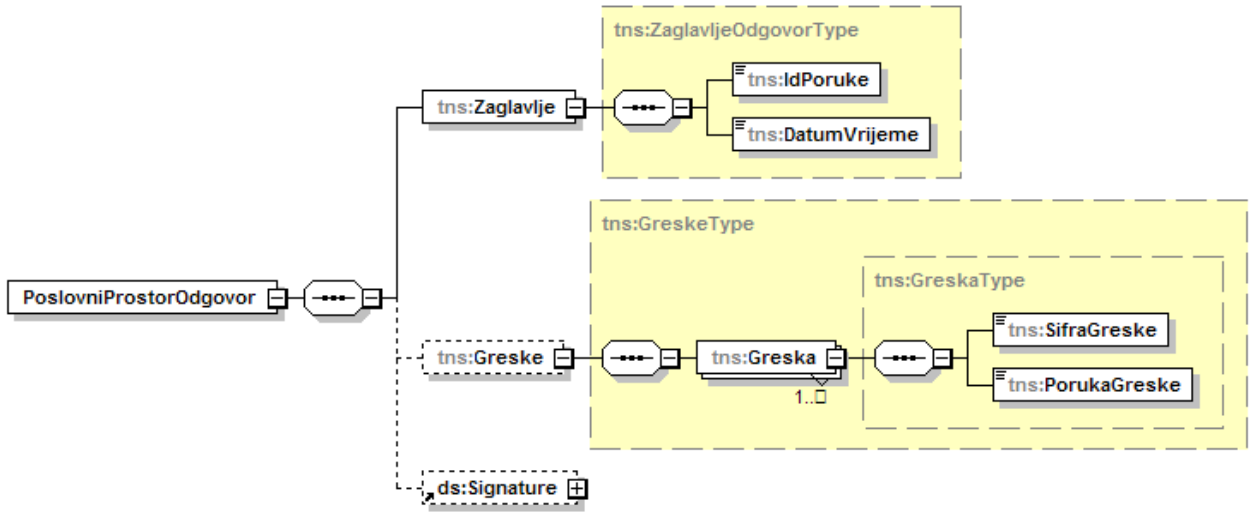
```
<tns:PoslovniProstorZahtjev xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
  <tns:Zaglavlje>
    <tns:IdPoruke>ca996cc7-fcc3-4c50-961b-40c8b875a5e8</tns:IdPoruke>
    <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
  </tns:Zaglavlje>
  <tns:PoslovniProstor>
    <tns:Oib>98765432198</tns:Oib>
    <tns:OznPoslProstora>Poslovnica1</tns:OznPoslProstora>
    <tns:AdresniPodatak>
      <tns:Adresa>
        <tns:Ulica>Avenija Marina Držića</tns:Ulica>
        <tns:KucniBroj>0014</tns:KucniBroj>
        <tns:KucniBrojDodatak>B</tns:KucniBrojDodatak>
        <tns:BrojPoste>10000</tns:BrojPoste>
        <tns:Naselje>Zagreb</tns:Naselje>
        <tns:Opcina>12345</tns:Opcina>
      </tns:Adresa>
    </tns:AdresniPodatak>
    <tns:RadnoVrijeme>Pon-Sub: 08:00-21:00, Ned: 09:00-14:00</tns:RadnoVrijeme>
    <tns:DatumPocetkaPrimjene>01.09.2012</tns:DatumPocetkaPrimjene>
    <tns:SpecNamj>08765432498</tns:SpecNamj>
  </tns:PoslovniProstor>
</tns:PoslovniProstorZahtjev>
```

2.2.3 Podatkovni skup odgovora za podatke o poslovnom prostoru

U tablici u nastavku opisan je podatkovni skup poruke odgovora za podatke o poslovnom prostoru.

Podatak	Opis/Napomena	Obvezan DA/NE	Tip/Duljina
Zaglavlje			
Identifikator poruke	ID poruke (UUID). Kao identifikator poruke odgovora uzima se ID iz poruke zahtjeva.	DA	Varchar(0-36)
Datum i vrijeme obrade	Datum i vrijeme obrade poruke zahtjeva. dd.mm.ggggThh:mm:ss	DA	Date & Time
Greške			
Šifra greške	Šifra greške je u formatu sXXX gdje je XXX troznamenkasti prirodni broj. Šifre grešaka sukladno šifarniku grešaka.	DA, ako ima grešaka	Varchar(4)
Poruka	Poruka greške je tekstualni opis greške sukladno šifarniku grešaka.	DA, ako ima grešaka	Varchar(500)

Na slici 8 u nastavku pregledno je prikazana shema poruke odgovora za podatke o poslovnom prostoru.



Slika 8. Shema poruke odgovora za podatke o poslovnom prostoru

2.2.4 Primjer poruke odgovora za podatke o poslovnom prostoru

A. Primjer odgovora (bez greške)

```
<tns:PoslovniProstorOdgovor xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
   <tns:Zaglavlje>
      <tns:IdPoruke>ca996cc7-fcc3-4c50-961b-40c8b875a5e8</tns:IdPoruke>
      <tns:DatumVrijeme>01.09.2012T21:10:35</tns:DatumVrijeme>
   </tns:Zaglavlje>
</tns:PoslovniProstorOdgovor>
```

B. Primjer odgovora (s greškom: Poruka nije u skladu s XML shemom...)

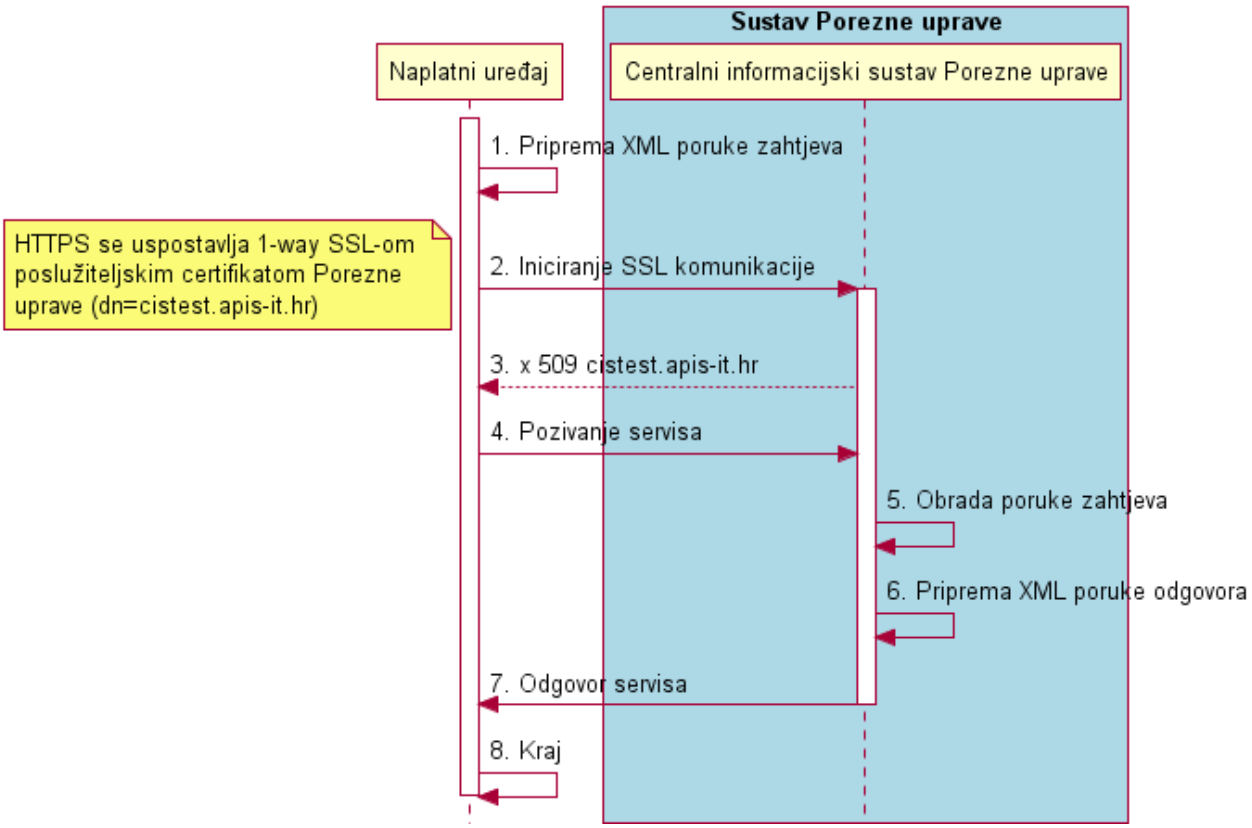
```
<tns:PoslovniProstorOdgovor xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
    <tns:Zaglavlje>
       <tns:IdPoruke>9766e3f0-0710-11e2-892e-0800200c9a66</tns:IdPoruke>
       <tns:DatumVrijeme>25.10.2012T14:44:03</tns:DatumVrijeme>
     </tns:Zaglavlje>
     <tns:Greske>
        <tns:Greska>
            <tns:SifraGreske>s001</tns:SifraGreske>
              <tns:PorukaGreske>
               Poruka nije u skladu s XML shemom :  cvc-simple-type 1: element {http://www.apis-
it.hr/fin/2012/types/f73}BrojPoste value '10000000000000000000000000' is not a valid instance
of type {http://www.apis-it.hr/fin/2012/types/f73}String12BrojType</tns:PorukaGreske>
        </tns:Greska>
     </tns:Greske>
  </tns:PoslovniProstorOdgovor>
```

2.3 Echo metoda

Echo metoda je implementirana u svrhu testiranja ispravnog povezivanja s Web servisom što indirektno uključuje uspješnu uspostavu SSL komunikacije i potvrdu dostupnosti servisa fiskalizacije Porezne uprave. Ako je poziv echo metode uspješan, metoda će u poruci odgovora vratiti tekst prepisan iz poruke zahtjeva.

Poziv echo metode ne uključuje provjeru certifikata i elektroničkog potpisa i samim time uspješan poziv te metode ne znači i da će poziv ostalih metoda servisa (račun i poslovni prostor) biti uspješan.

Proces je prikazan slijednim dijagramom na slici 9.



Slika 9. Slijedni dijagram procesa slanja *echo* poruke

2.3.1 Primjer poruke zahtjeva za echo metodu

```
<tns:EchoRequest xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
 xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 FiskalizacijaSchema.xsd ">proizvoljan
tekst</tns:EchoRequest>
```

2.3.2 Primjer poruke odgovora za echo metodu

```
<tns:EchoResponse xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
 xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 FiskalizacijaSchema.xsd ">proizvoljan
tekst</tns:EchoResponse>
```

2.4 Šifarnik grešaka

U nastavku je šifarnik grešaka koji je jedinstven za sve tipove poruka.

Šifra greške	Poruka greške
s001	'Poruka nije u skladu s XML shemom : #element ili lista elemenata koji nisu ispravni po shemi#'
s002	'Certifikat nije izdan od strane FINA-e.'
s003	'Certifikat ne sadrži naziv 'Fiskal' .'
s004	'Neispravan digitalni potpis.'
s005	'OIB iz poruke zahtjeva nije jednak OIB-u iz certifikata.'
s006	'Sistemska pogreška prilikom obrade zahtjeva.'

3. Pregled preduvjeta za spajanje na CIS Porezne uprave

Centralni informacijski sustav Porezne uprave biti će dostupan u dvije okoline:

1. Testna
2. Produkcijska

Uvjeti spajanja su slični, a razlikuju se u različitim adresama pristupnih točaka i certifikatima. Funkcionalno se okoline neće razlikovati (osim kod razvoja novih funkcionalnosti) ali u testnoj okolini koristit će se testni podaci.

Pretpostavlja se da u klijentskom informacijskom sustavu također postoje dvije okoline koje će se koristiti za testiranje i produkcijski rad.

3.1 Mrežni preduvjeti i preporuke

Za spajanje na CIS Porezne uprave klijentski sustav mora zadovoljiti sljedeće mrežne preduvjete:

Vrsta mreže	Internet
Potrebni otvoreni TCP portovi prema CIS sustavu	8449

Mrežne preporuke za klijentski sustav za spajanje na CIS Porezne uprave su:

Karakteristike linka	Stalni link
Propusnost	min. 2 Mb/s (do 40 poruka/sec vršnog opterećenja)

Potrebna propusnost se procjenjuje na temelju broja poruka/sec vršnog opterećenja.

3.2 Sigurnosni preduvjeti

Sva komunikacija sa CIS-om Porezne uprave u testnoj okolini zaštićena je 1-way SSL enkripcijom na transportnom sloju. CIS Porezne uprave predstavlja se klijentu SSL certifikatom izdanim od FINA DEMO PKI (https://demo-pki.fina.hr).

Zaštita na transportnom sloju	HTTPS (SSL v3, min AES_256 enkripcija)
Certifikat(i) za elektroničko potpisivanje izdan od FINA DEMO PKI	Tip certifikata: aplikativni digitalni certifikat za fiskalizaciju

3.3 Aplikacijski preduvjeti

Funkcionalnost CIS-a je dostupna klijentima koristeći tehnologiju Web servisa. Iz tog razloga klijentska aplikacija (ili infrastruktura, ovisno o realizaciji) mora zadovoljiti sljedeće preduvjete:

Standardi kreiranja klijenta	WS-I
Tip servisa	document-literal
Aplikacijski protokol	SOAP/HTTPS (SOAP 1.1)

4. Topologija pristupa CIS-u Porezne uprave

Korisnici pristupaju CIS-u Porezne uprave iniciranjem 1-way SSL veze. Koristeći SSL kanal klijenti prema opisanoj proceduri razmjenjuju poruke s pristupnom točkom Porezne uprave. Razmjena podataka je sinkrona što znači da pristupna točka odmah odgovara na zahtjev korisnika. Formati poruka zahtjeva i odgovora specificirani su kroz XML shemu.

CIS pristupna točka

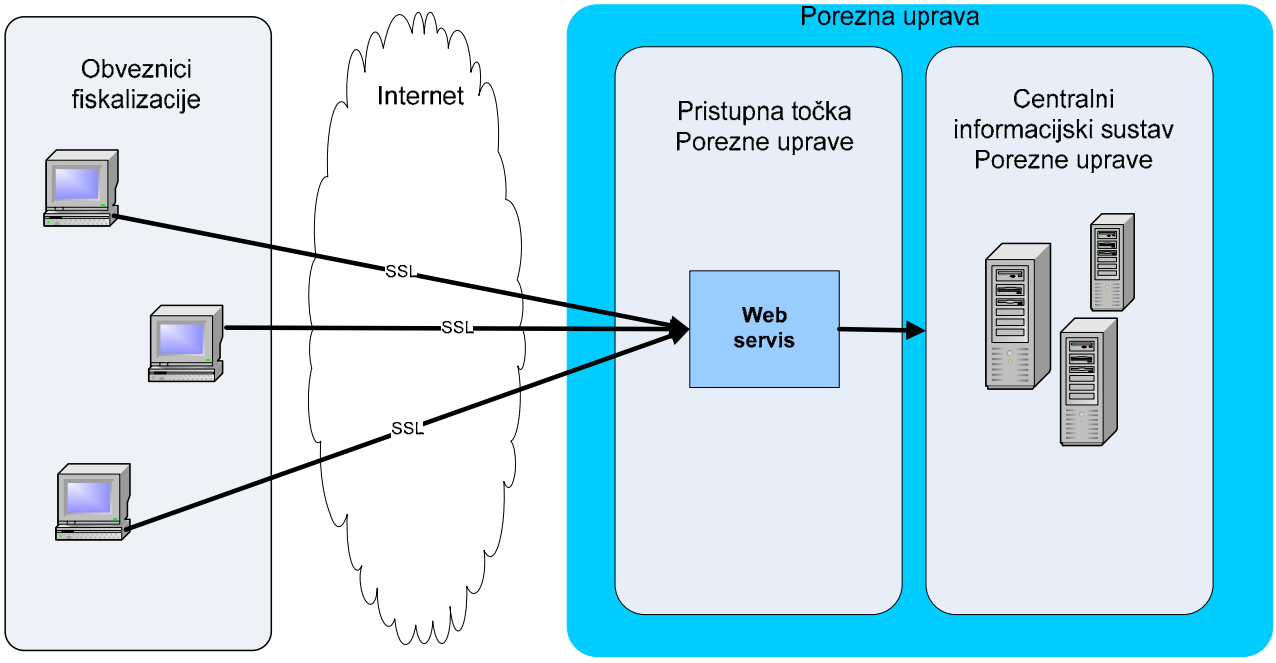
Implementacija i održavanje pristupne točke je zadaća APIS IT-a. APIS IT će klijentima omogućiti spajanje na pristupnu točku i to u dvije okoline, testnoj i produkcijskoj.

Internet veza

Pristupna točka će biti dostupna preko Internet mreže HTTPS protokolom.

Informacijski sustav obveznika fiskalizacije (klijenta)

Klijenti su zaduženi osigurati hardversku i softversku podršku za razmjenu poruka s pristupnom točkom. Kao što se vidi na slici 10, nije predviđen razvoj „posredničke komponente". Razvoj hardversko-softverskog rješenja je u domeni klijenta. Klijent je također dužan osigurati Internet vezu prema CIS pristupnoj točci s potrebnom propusnošću. Odabir platforme i implementacija softverskog rješenja je u domeni klijenta i takve informacije nije potrebno dojaviti APIS IT-u.



Slika 10. Topologija pristupa CIS-u Porezne uprave

4.1 Sigurnost (zaštita od uplitanja treće strane)

Komunikacija s partnerima sustava mora biti onemogućena od uplitanja treće strane. To znači da XML poruke poslane između strana moraju biti zaštićene od gledanja ili mijenjanja od treće strane. Ovi zahtjevi se realiziraju kroz zaštitu na transportnom sloju (HTTPS).

Konkretno, koristi se 1-way SSL s poslužiteljskim certifikatom Porezne uprave za terminaciju SSL-a u kojem se poslužitelj Porezne uprave predstavlja klijentima.

Kao Certificate Authority koristiti će se usluge FINA DEMO CA.

4.2 Kontrola pristupa

U CIS će biti zaprimljene samo poruke potpisane aplikativnim certifikatom izdanim u svrhu fiskalizacije. Na taj način pristup je omogućen samo klijentima koji posjeduju važeće X.509 certifikate prema FINA DEMO PKI-u.

Za povezivanje koristi se SOAP/HTTPS protokol. Treba napomenuti da je primijenjena verzija SOAP protokola 1.1.

5. Public Key Infrastructure (PKI)

Kao davatelj usluge PKI odabrana je FINA registar digitalnih certifikata. Klijentski sustavi za testnu okolinu moraju imati izdan certifikat od FINA DEMO PKI (https://demo-pki.fina.hr/).

Uporaba certifikata na strani CIS pristupne točke Porezne uprave je:
- uspostava SSL veze prema CIS-u Porezne uprave
- elektroničko potpisivanje poruka

Certifikati koje koristi CIS pristupna točka Porezne uprave u testnoj okolini imaju sljedeće nazive:
- Poslužiteljski: **cistest.apis-it.hr**
- Aplikacijski: **fiskalcistest**

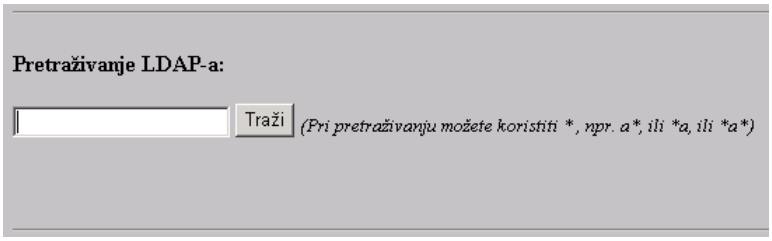
Postupak preuzimanja CIS certifikata/javnih ključeva s FINA DEMO PKI

Preuzimanje certifikata potrebnih za pristup CIS-u Porezne uprave, može se napraviti preko FINA DEMO PKI Web stranica (https://demo-pki.fina.hr/) korištenjem funkcionalnosti pretraživanja javnog imenika. Navedena funkcija omogućava spremanje certifikata preko Microsoft Address Book aplikacije u datoteku na disk radne stanice, odnosno poslužitelja.

Alternativa je pretraživanje direktorija direktno kroz Address Book aplikaciju (Start->Run->wab.exe).

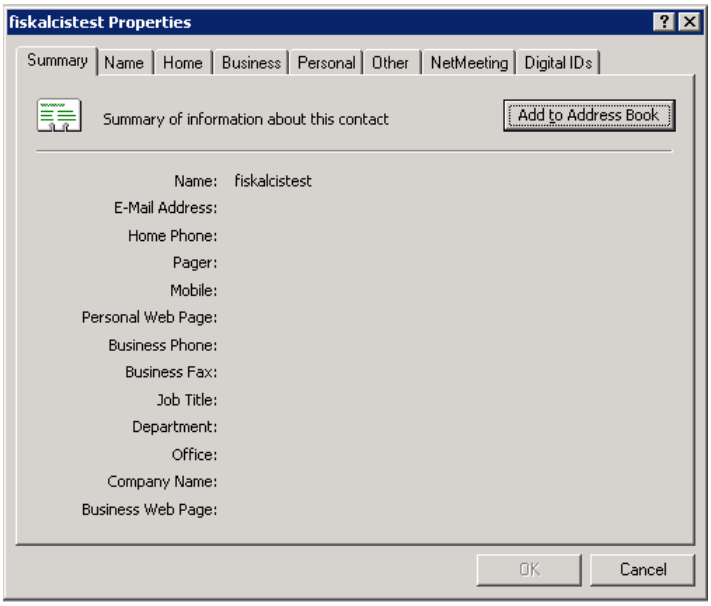
Kratke upute za preuzimanje certifikata/javnih ključeva

Za preuzimanje certifikata/javnih ključeva u Internet pregledniku je potrebno:
- pozvati Web stranicu FINA DEMO PKI https://demo-pki.fina.hr/
- na Web stranici potražiti "Pretraživanje LDAP-a:" prikazano na slici 11



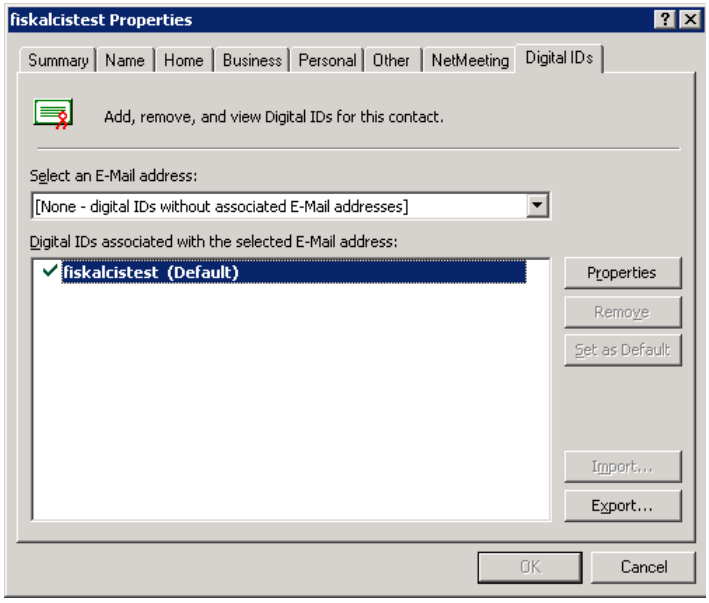
Slika 11. Pretraživanje LDAP-a

- u polje za pretraživanje unijeti naziv certifikata te odabrati "Traži".
- otvara se Microsoft Address Book aplikacija (na slici 12 je dan primjer za *fiskalcistest* certifikat)



Slika 12. Microsoft Address Book (primjer za *fiskalcistest* certifikat)

- preuzimanje javnog ključa za željeni certifikat se može napraviti odabirom kartice "Digital IDs" i klikom na "Export", prikazano na slici 13



Slika 13. Preuzimanje javnog ključa

6. Postupak spajanja obveznika fiskalizacije na CIS Porezne uprave

1. Nabaviti minimalno jedan aplikativni digitalni certifikat za fiskalizaciju od FINA DEMO PKI za testnu okolinu. Broj ukupno izdanih aplikativnih digitalnih certifikata za fiskalizaciju ovisi o obvezniku fiskalizacije i potrebi. Postupak opisan u poglavlju 11.

2. Nakon što FINA izda potrebne certifikate, obveznik fiskalizacije ih implementira u svoju okolinu.

3. Preuzeti CIS certifikate/javne ključeve s FINA DEMO PKI. Postupak opisan u poglavlju 5.

4. Obveznici fiskalizacije prvo se spajaju na testni sustav. Minimalno dva dana neprekidnog i stabilnog rada preduvjet je za prijelaz u produkcijski sustav.

6.1 Url adrese za spajanje na CIS Porezne uprave

1. TEST

Okolina:	TEST
Servis:	Prihvat podataka o računima i poslovnim prostorima (FiskalizacijaServiceTest)
URL:	https://cistest.apis-it.hr:8449/FiskalizacijaServiceTest

Nakon objave servisa isti će stalno biti dostupan za testiranje u <u>testnoj okolini</u> osim u servisnim intervalima navedenim u nastavku:

- **radnim danom od 16:00 do 17:00**
- **nedjeljom od 08:00 do 12:00**

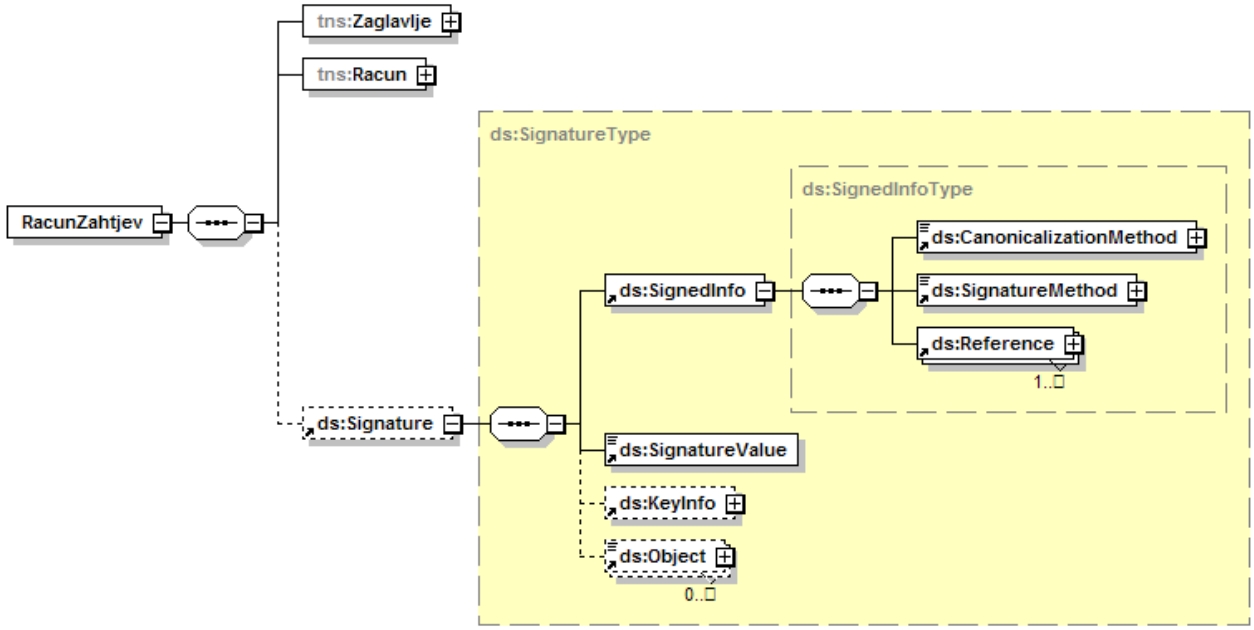
7. Elektronički potpis poruke zahtjeva

Poruka zahtjeva osim poslovnih podataka sadrži i elektronički potpis. Struktura poruke definirana je XML shemom. Za elektronički potpis poruke obveznik fiskalizacije koristi aplikativni certifikat izdan u svrhu fiskalizacije.

Elektronički potpis poruke realiziran je kao "XML enveloped signature" tj. elektronički potpis sadržan je unutar XML elementa koji se potpisuje. U svim porukama potpisuje se *root* element zahtjeva.

Sve informacije vezane na elektroničko potpisivanje sadržane su u elementu <Signature> čija struktura je propisana

http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd shemom i definirani su unutar http://www.w3.org/2000/09/xmldsig# namespacea definiranog kroz W3C preporuku XML Signature Syntax and Processing (xmldsig-core), prikazano na slici 14.



Slika 14. Shema <Signature> elementa

U nastavku je primjer elektronički potpisane poruke zahtjeva:

```
<tns:RacunZahtjev Id="RacunZahtjev" xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
    <tns:Zaglavlje>
      <tns:IdPoruke>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</tns:IdPoruke>
      <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
    </tns:Zaglavlje>
    <tns:Racun>
     ...
    </tns:Racun>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <Reference URI="#RacunZahtjev">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </Transforms>
```

```
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>VItfxY/A1BITZ/BuWpsGd9gKix4=</DigestValue>
          </Reference>
        </SignedInfo>
              <SignatureValue>0+5UDLzJuGy56HojH510+d.....</SignatureValue>
        <KeyInfo>
          <X509Data>
            <X509Certificate>MIIEyDCCA7CgAwIBAgIEPssQ2TANBgkqh...</X509Certificate>
            <X509IssuerSerial>
              <X509IssuerName>OU=DEMO,O=FINA,C=HR</X509IssuerName>
              <X509SerialNumber>1053495513</X509SerialNumber>
            </X509IssuerSerial>
          </X509Data>
        </KeyInfo>
      </Signature>
    </tns:RacunZahtjev>
```

<Signature> elementa ima sljedeću strukturu:

<SignedInfo> – XML-DSIG blok s informacijama koje se potpisuju

<SignatureValue> – vrijednost potpisa

<KeyInfo> – certifikat korišten pri potpisivanju

Unutar SignedInfo elementa definirani su podaci o kanonizaciji i metodi potpisivanja. Potpisi su kanonizirani i metoda potpisivanja je uvijek RSA-SHA1 što se vidi kroz elemente <CanonicalizationMethod> i <SignatureMethod> koji imaju fiksan sadržaj:

Kanonikalizacijska metoda koja se koristi prilikom potpisa obvezno mora biti **Exclusive XML Canonicalization (*xml-exc-c14n*)**

```
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

Nakon tih elemenata nalazi se <Reference> element. Element ima pripadajući atribut URI koji se odnosi na podatke koji se potpisuju.

```
<Reference URI="#RacunZahtjev">
```

Podaci koji se potpisuju tj. *root* element zahtjeva ima atribut Id (definiran je u XML shemi zahtjeva) kojeg se onda referencira unutar samog potpisa iz elementa Reference. Preporuka je da vrijednost Id-a bude sam naziv *root* elementa zahtjeva (u ovom primjeru RacunZahtjev).

U primjeru je potpisan element tns:RacunZahtjev i ima Id="RacunZahtjev".

```
<tns:RacunZahtjev Id="RacunZahtjev" xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
```

Unutar elementa <Reference> nalaze se elementi <Transforms>, <DigestMethod> i <DigestValue>.

Element <Transforms> sadrži:

```
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

Element <DigestMethod> ima vrijednost:

```
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

Element <DigestValue> sadržava vrijednost izračunatu digest algoritmom za referencirani element.

Element <SignatureValue> sadrži base64 enkodiranu vrijednost koja predstavlja elektronički potpis unutar <SignedInfo> elementa.

Element <KeyInfo> sadržava podatke o certifikatu pomoću kojeg je potpisan zahtjev. Sam certifikat je Base64 kodiran u PEM formatu.

<X509Data>/<X509Certificate> sadržava Base64 enkodiran certifikat.

8. Pregled tehnologija korištenih u komunikaciji s pristupnom točkom CIS-a

8.1 XML

XML je kratica za EXtensible Markup Language - odnosno jezik za označavanje podataka. Ideja je bila stvoriti jedan jezik koji će biti jednostavno čitljiv i ljudima i računalnim programima. Princip realizacije je vrlo jednostavan: odgovarajući sadržaj treba se uokviriti odgovarajućim oznakama koje ga opisuju i imaju poznato ili lako shvatljivo značenje. Format oznaka u XML-u vrlo je sličan formatu oznaka u npr. HTML jeziku. Danas je XML jezik vrlo raširen i koristi se za različite namjene: odvajanje podataka od prezentacije, razmjenu podataka, pohranu podataka, povećavanje dostupnosti podataka i izradu novih specijaliziranih jezika za označavanje. XML je standardizirani jezik i za njegovu standardizaciju brine se World Wide Web Consortium.

8.2 SOAP

Simple Object Access Protocol (SOAP) je komunikacijski protokol, neovisan o platformi, baziran na XML–u koji se koristi za razmjenu informacija između aplikacija preko nekog transportnog kanala (HTTP, JMS, SMTP i dr.) Razvijen je kako bi se omogućila jednostavna komunikacija tekstualnim sadržajem, neovisan je o programskom jeziku, platformi i jednostavno proširiv.

SOAP protokol omogućuje komunikaciju između aplikacija koje rade na različitim operacijskim sustavima i različitim tehnologijama. Aplikacije razmjenjuju poruke dogovorenog formata. Poruke su formatirane kao XML dokumenti pa je njihova obrada i provjera jednostavna i može ih provoditi bilo koji program namijenjen radu s XML dokumentima. SOAP klijent kreira XML dokument koji sadrži odgovarajući zahtjev. Taj dokument formatiran je u skladu sa SOAP specifikacijom (http://www.w3.org/TR/soap/). Dokument dolazi do SOAP poslužitelja koji obrađuje pristigle zahtjeve i na osnovu pristiglih zahtjeva pokreće odgovarajuću aplikaciju. Po završenoj obradi SOAP poslužitelj, korištenjem SOAP protokola vraća poruku odgovora SOAP klijentu.

8.3 WS-x

W3C organizacija definira web servis kao softverski sistem dizajniran tako da podrži komunikaciju između dva računala (odnosno računalna sistema) preko mreže. Web servis ima sučelje opisano u formatu čitljivom računalima (WSDL). Vanjski sistemi komuniciraju s web servisom koristeći SOAP poruke.

Pojednostavljeno, web servisi otvaraju prema vanjskom svijetu (aplikacijama unutar i van kuće) poslovne servise koji implementiraju poslovna pravila. Specifikacija web servisa je namjerno razdvojena u tri dijela: SOAP, WSDL i UDDI. Svaki pojedinačni dio specifikacije je neovisan o platformi i programskom jeziku. Upravo zato su web servisi postali standard koji omogućava interoperabilnost između različitih razvojnih okruženja. Danas je na tržištu dostupan cijeli niz biblioteka, u gotovo svakom programskom jeziku i za svaki operacijski sustav, koje omogućavaju kreiranje i korištenje web servisa na jedinstven način.

8.4 WSDL

Web Services Description Language (WSDL) je format XML dokumenta kojim se opisuju web servisi, odnosno lokacija (u mreži) i operacije koje web servis nudi. Prethodna verzija 1.1 nije bila službena preporuka World Wide Web Consortiuma (W3C), dok je aktualna verzija 2.0 to postala.

Apstraktna definicija lokacije i operacija je odvojena od konkretne instance, odnosno implementacije servisa. Time se omogućava ponovna iskoristivost tih definicija.

8.5 HTTP

Hypertext Transfer Protocol (HTTP) je komunikacijski protokol koji se koristi za prenošenje informacija na Internetu te na intranet mrežama. Razvoj protokola koordiniraju W3C (World Wide Web Consortium) i IETF (Internet Engineering Task Force) organizacije a verzija protokola koja je danas u širokoj upotrebi je HTTP/1.1 i definirana je 1999. godine.

HTTP protokol radi na principu zahtjeva i odgovora (*request/response*) koje razmjenjuju klijent i poslužitelj. Klijent kreira HTTP zahtjev (najčešće je to Web preglednik, no u slučaju Web servisa to je klijentska aplikacija) dok poslužitelj na osnovu tog zahtjeva kreira HTTP odgovor.

8.6 HTTPS

Hypertext Transfer Protocol Secure (HTTPS) je kombinacija HTTP-a i protokola koji ostvaruje mrežnu sigurnost. U stvari, HTTPS i nije novi protokol već je spoj normalne HTTP interakcije putem Secure Sockets Layer (SSL) ili Transport Layer Security (TLS) konekcije. To osigurava da poruke koje razmjenjuju klijent i poslužitelj ne može pročitati ili izmijeniti treća strana koja se nalazi između njih.

8.7 XMLDsig

XML signature (XMLDsig) definira XML sintaksu za elektroničko potpisivanje i definirano je W3C preporukom XML Signature Syntax and Processing. Funkcionalno je vrlo sličan PKCS#7 specifikaciji no više je prilagođen potpisivanju XML dokumenata.

Primjenjuje se u Web tehnologijama kao što su SOAP, SAML i slični. Potpisi mogu biti korišteni za potpisivanje podataka bilo kakvog tipa, tipično XML dokumenata, no potpisati se može bilo što dohvatljivo putem URL adrese. Ako se potpisuje sadržaj izvan nosivog XML-a tada je to **detached** vrsta potpisa, ako potpisujemo dio nosivog XML-a tada se radi o **enveloped** vrsti potpisa i ako potpis sam sadržava potpisani sadržaj tada se radi o **enveloping** vrsti potpisa.

8.7.1 XML Canonicalization

Kreiranje XML elektroničkog potpisa je značajno kompleksnije od kreiranja običnog elektroničkog potpisa jer XML dokument može imati više od jedne ispravne serijalizirane reprezentacije. Na primjer, razmaknica unutar XML elementa nema nikakvog značenja tako da je <Elem> i <Elem > sa sadržajnog gledišta XML-a isto.

Budući da se elektronički potpis kreira pomoću algoritma asimteričnog ključa (obično RSA) za enkripciju rezultata ili računanjem rezultata putem kriptografske funkcije (obično SHA1), razlika u samo jednom bitu izazvat će razliku u potpisu. Štoviše, ako se XML dokument prenosi s računala na računalo može se promijeniti i linijski terminator, što kasnije može rezultirati različitim renderiranjem dokumenta i izračunom digesta. Da bi se izbjegle ovakve situacije i osiguralo da logički i sadržajno istovjetni XML dokumenti rezultiraju identičnim elektroničkim potpisima koristimo kanonikalizacijske transformacije (obično skraćeno u c14n). Ti algoritmi garantiraju da će logički i sadržajno istovjetni dokumenti rezultirati identičnom reprezentacijom.

Sljedeća komplikacija nastaje zbog načina na koji defaultni kanonikalizacijski algoritam obrađuje namespace deklaracije. Često se potpisani XML dokument nalazi unutar nekog drugog XML dokumenta, što je i naš slučaj. U tom slučaju defaultna kanonikalizacijska metoda neće dati identične rezultate. Iz tog razloga moramo koristiti takozvanu Ekskluzivnu metodu (**Exclusive Canonicalization**) koja serijalizira XML neovisno o okružujućem XML-u.

8.8 UUID

UUID (Universally unique identifier), po definiciji, je standardni jedinstveni indentifikator korišten pri razvoju softvera, standardiziran od strane Open Software Fundacije kao dio DCE (Distributed Computing Environment) specifikacije. Namjena UUID-a je omogućiti distribuiranim sustavima jedinstven način identifikacije bez značajnije centralizirane koordinacije. Svatko može generirati UUID i koristiti ga s razumnnom dozom sigurnosti da nitko nenamjerno neće kreirati isti identifikator. Shodno tome podaci označeni UUID-om mogu bez bojazni biti insertirani u jedinstvenu bazu podataka bez bojazni da će nastati ikakvi ID konflikti.

Po definiciji UUID je 16-oktetni (128-bitni) broj. U svom kanoničkom obliku UUID čine 32 heksadecimalne znamenke grupirane u 5 grupa odvojenih crticama u obliku 8-4-4-4-12 što u totalu čini 36 znakova (32 broja i 4 crtice). Na primjer:

550e8400-e29b-41d4-a716-446655440000

UUID specifikacija propisuje 5 verzija UUID-a:

1. verzija - generiranje je bazirano na MAC adresi

2. verzija - generiranje je bazirano na vremenskoj komponenti i domeni

3. verzija - generiranje je bazirano na izračunu MD5 hash-a iz URL-a, domene i sl.

4. verzija - random generirani broj

5. verzija - generiran izračunom SHA-1 hasha iz podataka istih kao u verziji 3.

9. Primjeri poruka

9.1 Poruka zahtjeva za račun u izvornom obliku

Primjer poruke zahtjeva za račun sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Body>
      <tns:RacunZahtjev xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 ../schema/FiskalizacijaSchema.xsd">
         <tns:Zaglavlje>
            <tns:IdPoruke>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</tns:IdPoruke>
            <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <tns:Racun>
            <tns:Oib>98765432198</tns:Oib>
            <tns:USustPdv>true</tns:USustPdv>
            <tns:DatVrijeme>01.09.2012T21:10:34</tns:DatVrijeme>
            <tns:OznSlijed>P</tns:OznSlijed>
            <tns:BrRac>
               <tns:BrOznRac>123456789</tns:BrOznRac>
               <tns:OznPosPr>POSL1</tns:OznPosPr>
               <tns:OznNapUr>12</tns:OznNapUr>
            </tns:BrRac>
            <tns:Pdv>
               <tns:Porez>
                  <tns:Stopa>25.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>2.50</tns:Iznos>
               </tns:Porez>
               <tns:Porez>
                  <tns:Stopa>10.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>1.00</tns:Iznos>
               </tns:Porez>
               <tns:Porez>
                  <tns:Stopa>0.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>0.00</tns:Iznos>
               </tns:Porez>
            </tns:Pdv>
            <tns:Pnp>
               <tns:Porez>
                  <tns:Stopa>3.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>0.30</tns:Iznos>
               </tns:Porez>
            </tns:Pnp>
            <tns:OstaliPor>
               <tns:Porez>
                  <tns:Naziv>Porez na luksuz</tns:Naziv>
                  <tns:Stopa>15.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>1.50</tns:Iznos>
               </tns:Porez>
            </tns:OstaliPor>
            <tns:IznosOslobPdv>12.00</tns:IznosOslobPdv>
            <tns:IznosMarza>13.00</tns:IznosMarza>
            <tns:IznosNePodlOpor>100.00</tns:IznosNePodlOpor>
            <tns:Naknade>
```

```
            <tns:Naknada>
               <tns:NazivN>Povratna naknada</tns:NazivN>
               <tns:IznosN>1.00</tns:IznosN>
            </tns:Naknada>
         </tns:Naknade>
         <tns:IznosUkupno>145.68</tns:IznosUkupno>
         <tns:NacinPlac>K</tns:NacinPlac>
         <tns:OibOper>01234567890</tns:OibOper>
         <tns:ZastKod>e4d909c290d0fb1ca068ffaddf22cbd0</tns:ZastKod>
         <tns:NakDost>false</tns:NakDost>
         <tns:ParagonBrRac>123/458/5</tns:ParagonBrRac>
         <tns:SpecNamj>Navedeno kao primjer</tns:SpecNamj>
      </tns:Racun>
   </tns:RacunZahtjev>
</soapenv:Body>
</soapenv:Envelope>
```

9.2 Poruka zahtjeva za račun s elektroničkim potpisom

Primjer poruke zahtjeva za račun s elektroničkim potpisom i SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Body>
      <tns:RacunZahtjev xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Id="racunId"
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 ../schema/FiskalizacijaSchema.xsd">
         <tns:Zaglavlje>
            <tns:IdPoruke>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</tns:IdPoruke>
            <tns:DatumVrijeme>01.09.2012T21:10:34</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <tns:Racun>
            <tns:Oib>98765432198</tns:Oib>
            <tns:USustPdv>true</tns:USustPdv>
            <tns:DatVrijeme>01.09.2012T21:10:34</tns:DatVrijeme>
            <tns:OznSlijed>P</tns:OznSlijed>
            <tns:BrRac>
               <tns:BrOznRac>123456789</tns:BrOznRac>
               <tns:OznPosPr>POSL1</tns:OznPosPr>
               <tns:OznNapUr>12</tns:OznNapUr>
            </tns:BrRac>
            <tns:Pdv>
               <tns:Porez>
                  <tns:Stopa>25.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>2.50</tns:Iznos>
               </tns:Porez>
               <tns:Porez>
                  <tns:Stopa>10.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>1.00</tns:Iznos>
               </tns:Porez>
               <tns:Porez>
                  <tns:Stopa>0.00</tns:Stopa>
                  <tns:Osnovica>10.00</tns:Osnovica>
                  <tns:Iznos>0.00</tns:Iznos>
               </tns:Porez>
            </tns:Pdv>
            <tns:Pnp>
               <tns:Porez>
                  <tns:Stopa>3.00</tns:Stopa>
```

<tns:Osnovica>**10.00**</tns:Osnovica>
<tns:Iznos>**0.30**</tns:Iznos>
</tns:Porez>
</tns:Pnp>
<tns:OstaliPor>
<tns:Porez>
<tns:Naziv>**Porez na luksuz**</tns:Naziv>
<tns:Stopa>**15.00**</tns:Stopa>
<tns:Osnovica>**10.00**</tns:Osnovica>
<tns:Iznos>**1.50**</tns:Iznos>
</tns:Porez>
</tns:OstaliPor>
<tns:IznosOslobPdv>**12.00**</tns:IznosOslobPdv>
<tns:IznosMarza>**13.00**</tns:IznosMarza>
<tns:IznosNePodlOpor>**100.00**</tns:IznosNePodlOpor>
<tns:Naknade>
<tns:Naknada>
<tns:NazivN>**Povratna naknada**</tns:NazivN>
<tns:IznosN>**1.00**</tns:IznosN>
</tns:Naknada>
</tns:Naknade>
<tns:IznosUkupno>**145.68**</tns:IznosUkupno>
<tns:NacinPlac>**K**</tns:NacinPlac>
<tns:OibOper>**01234567890**</tns:OibOper>
<tns:ZastKod>**e4d909c290d0fb1ca068ffaddf22cbd0**</tns:ZastKod>
<tns:NakDost>**false**</tns:NakDost>
<tns:ParagonBrRac>**123/458/5**</tns:ParagonBrRac>
<tns:SpecNamj>**Navedeno kao primjer**</tns:SpecNamj>
</tns:Racun>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#racunId">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>**VltfxY/A1BITZ/BuWpsGd9gKix4=**</DigestValue>
</Reference>
</SignedInfo>

<SignatureValue>0+5UDLzJuGy56HojH510+dX6VurJmL52Ob7FDNNH8U3NltxIo7fUvU1ra6HPSyCd4H3O
QEvZIb3xv1yqvLGYr0M5yzVGbu9o4IXG3qlTTVtEWu1MCC7OYeyltnKwr9/QRAbFrA3QWZu/F8qnc4dKg6o
hl8X8hZLLh2wIzNxtOrzbtJO6IZciCyfptR6u1vvwmUxIlo7ISCTLXw/UC9LqC86C5HBbQU+QT1i9rTsUdYZZ0
kTeI4Z/ZPkYO+OqZmpiKdSbwlwwqtp7CrQ0WK2RSd+x+XUf2GF3Ydld90Tx9QYRps/Z
P0OME3jnSpKJIkRQTB8ev9rM+KYYEGbSR1rz6g==
</SignatureValue>
<KeyInfo>
<X509Data>

<X509Certificate>MIIEyDCCA7CgAwIBAgIEPssQ2TANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJI
UjENMAsGA1UEChMERklOQTENMAsGA1UECxMEREVNTzAeFw0xMjA5MjcxMDQ5MThaFw0xNDA5Mjc
xMTE5MThaMFkxCzAJBgNVBAYTAkhSMSYwJAYDVQQKEx1BUElTIElUICBELk8uTy4gSFIwMjk5NDY1M
DE5OTEPMA0GA1UEBxMGWkFHUkVCMREwDwYDVQQDEwhGSVNLQUwgMjCCASIwDQYJKoZIhvcNA
QEBBQADggEPADCCAQoCggEBAOEPIO7AMxdO5o6jw5BUy2UAKXdtdYavlEtVPVRwoBxA4YxPzDFjsnJ
GapAH4DW7YKqgLLLT6EjrKkCvjOpgr5LsPUjZk7/gZrVNpcBIzm6ECiywBGjB623/kdWqYdd9Al+1KbOVa+
PRp9D7JzjLQTZaXTc4FR5wGo4w9jC22ixqb+F6aDzF6TLsICJVKFWV4g6glMLlKgsrZxk+O55/1f7o0442dC
GuZ7IQtp1UK7TH9a7KilvLNv+1OKyZDZfzYGyPVkB/Tt7N5NO0R1ICbeATvDcDyl2BQfECYC+z+3dfDybcO
FF+QmBsntlKO4p7+LxR/Yob5/GxPrIi6KVyDdECAwEAAaOCAcQwggHAMAsGA1UdDwQEAwIFoDBCBgN
VHSAEOzA5MDcGCSt8iFAFHwUDATAqMCgGCCsGAQUFBwIBFhxodHRwOi8vZGVtby1wa2kuZmluYS5o
ci9jcHMvMCQGA1UdEQQdMBuBGXNhbmRyYS5wb3BvdmljQGFwaXMtaXQuaHIwgc4GA1UdHwSBxjCBw

zBCoECgPqQ8MDoxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1P
MQ0wCwYDVQQDEwRDUkw3MH2ge6B5hk9sZGFwOi8vZGVtby1sZGFwLmZpbmEuaHIvb3U9REVNTyxv
PUZJTkEsYz1IUj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0JTNCYmluYXJ5hiZodHRwOi8vZGVtby1wa2
kuZmluYS5oci9jcmwvZGVtb2NhLmNybDArBgNVHRAEJDAigA8yMDEyMDkyNzEwNDkxOFqBDzIwMTQw
OTI3MTExOTE4WjAfBgNVHSMEGDAWgBR6YCOOSJ0ya6TILd24WbSU/EJinjAdBgNVHQ4EFgQUK/IWm
nKEKdD/PLV06CddkYi7WrAwCQYDVR0TBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAABb3RnPlwEBNK
EWy3YsFRwJSZoMTBGwv7Q0sWf9nTHMS3vgFqNUSx8iqP99tnoppav7TdWoQ5zBtW935Nkev7rhqGADT
4R/7pYeYc2R+Yjsbn6rxo6zDv/oIrd8LtFHccx3iUYgt/n1J5QiGIQ601fXwYftuaVcaMnwsVBCuFy8vut4PiSPVs
fML/R/oLQ3IqKJmNMXy4Rm8qjeOdgLyYwTuz7oKZ+N4+kq4tpuuJn86EUk3qsQo+FOVfwFi7cew7qtDYHap
qAC4zTb6isqB8/Wcagucb4zNU3Vgeixz5Nsd
8g28hcC/OzhHHGZpQvB0WVF5YlF1Od7AYBL+DDl9Lg==
</X509Certificate>
<X509IssuerSerial>
<X509IssuerName>**OU=DEMO,O=FINA,C=HR**</X509IssuerName>
<X509SerialNumber>**1053495513**</X509SerialNumber>
</X509IssuerSerial>
</X509Data>
</KeyInfo>
</Signature>
</tns:RacunZahtjev>
</soapenv:Body>
</soapenv:Envelope>

9.3 Poruka odgovora za račun u izvornom obliku

Primjer poruke odgovora za račun sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
      <tns:RacunOdgovor
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 ../schema/FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
         <tns:Zaglavlje>
            <tns:IdPoruke>733362f1-063f-11e2-892e-0800200c9a66</tns:IdPoruke>
            <tns:DatumVrijeme>01.09.2012T21:10:38</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <tns:Jir>6b7749c6-56c1-4cf5-b7f7-9f29cebc9f7f</tns:Jir>
      </tns:RacunOdgovor>
   </soap:Body>
</soap:Envelope>
```

9.4 Poruka odgovora za račun s elektroničkim potpisom

Primjer poruke odgovora za račun s elektroničkim potpisom i SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
      <tns:RacunOdgovor Id="G0xcabf5080-4D"
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 ../schema/FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
         <tns:Zaglavlje>
            <tns:IdPoruke>733362f1-063f-11e2-892e-0800200c9a66</tns:IdPoruke>
            <tns:DatumVrijeme>01.09.2012T21:10:38</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <tns:Jir>6b7749c6-56c1-4cf5-b7f7-9f29cebc9f7f</tns:Jir>
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
```

```
            <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <Reference URI="#G0xcabf5080-4D">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
              </Transforms>
              <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>4j9JKFMvg6Mmfx7ERu8R3WkZTtQ=</DigestValue>
            </Reference>
          </SignedInfo>

<SignatureValue>P5bIa6dPJjdIvov/pmmJvML7nMep7Xea4+LiWHEJEfsOz3SSKG4wwuVdGM+7k+CGt799
No4r1KKulaRRPMQW/vh0qtAm/0V/o45cIpgYB1YFUZdCsNktasYh4gkD/RQiF8ph/86W8zmY4fdLrqb45P17
6e/DVcWJkduHeF2t4afUyJANti8czeimMB1uIaHvZwSMlvDKCN93tXoSlwGX3CXDg8kTRzpDC1x3r1aboaR
rLpkgzSZFrnMe4aBCqFnOpZjcXZa321hK3shl0PSij52IN1KWuMP9ekldj+XVNGQa/Ecj8RjuFDKwgoyhxpB9
WZ/jGa81QAQ0DQsckMkF6g==</SignatureValue>
          <KeyInfo>
            <X509Data>

<X509Certificate>MIIExDCCA6ygAwIBAgIEPssQcTANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJI
UjENMAsGA1UEChMERklOQTENMAsGA1UECxMEREVNTzAeFw0xMjA5MjYwODExNDlaFw0xNDA5MjY
wODQxNDlaMHgxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1PM
REwDwYDVQQLEwhQb3Nsb3ZuaTEgMB4GA1UECxMXQVBJUyBJVCBELk8uTy4gODA1NDEzNzIxFjAU
BgNVBAMTDWZpc2thbGNpc3Rlc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC81TtKtJ
84emCS/HK7gSovjNdluZWB0DbIMq3cBFpOpmurcbDCJ1Z17XiPLa+UWYIqyAjHQyDnG/H4c5EeGoli9swz
5QcZFBmyXTpSd3GuMROgUAd4bcvbw1/HDONE5cE8PL11GIy8gi5ANZkujalYmx+1ImnhHxx1Bh2UJ/bcl2
eXPtieBQBwtClATSzseB5FFz8LcSyfzM7h39PsAIZ0p8YzH7W+307gvgrJHYb/n4ADwlxieHqb5j74DVD0rUP
cUE5d0nSZ7hfEkW8xICgs1Ly6Vu3w7Z5M8vb4QmoPnlT1EaHCXiweuK6vjkUk8RQmYY4ITFBs8zHiG7h4n
9bPAgMBAAGjggGhMIIBnTAOBgNVHQ8BAf8EBAMCBaAwQgYDVR0gBDswOTA3BgkrfIhQBR8FBAIwKjA
oBggrBgEFBQcCARYcaHR0cDovL2RlbW8tcGtpLmZpbmEuaHlvY3BzLzCBzgYDVR0fBIHGMIHDMEKgQK
A+pDwwOjELMAkGA1UEBhMCSFIxDTALBgNVBAoTBEZJTkExDTALBgNVBAsTBERFTU8xDTALBgNVB
AMTBENSTDcwfaB7oHmGT2xkYXA6Ly9kZW1vLWxkYXAuZmluYS5oci9vdT1ERU1PLG89RklOQSxjPUhS
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QlM0JiaW5hcnmGJmh0dHA6Ly9kZW1vLXBraS5maW5hLmhyL
2NybC9kZW1vY2EuY3JsMCsGA1UdEAQkMCKADzIwMTIwOTI2MDgxMTQ5WoEPMjAxNDA5MjYwODQx
NDlaMB8GA1UdIwQYMBaAFHpgI45InTJrpOUt3bhZtJT8QmKeMB0GA1UdDgQWBBRgIJsZevSn6kDuSzC
hmaa9Sqr6sjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBBQUAA4IBAQCo5kJWaNjgS+UG7XQHsHersDFk
4K5W/Y2Pbubary0j3IwJrveHbUR3HOb0KiVenF6+1FL3sCI/2tfH3wSszWL8Gkit8jUudTo5vDyLqEUXYDHlF
UBwseudsPkUxPiQ6HuuFd3PiUAWf00chXD38eTjfapNu6VeQt4EORSO+rEXdhWihVb5HxFIVPTkqHmq1KI
NwtV9+thwE3hNMwacRa4gwTB1O+jadVlJQMq+kgwnLGLBcwr0W+x1ye6MPSYEUxSNFGHPG/evP9DRL
wJtR3ngvlCDusnO+A75Nn40VYcoIjw6EN1V+plK+HkLye0zzLsnHIWTSGfZ2sQVG5xCURiI</X509Certificat
e>
              <X509IssuerSerial>
                <X509IssuerName>OU=DEMO, O=FINA, C=HR</X509IssuerName>
                <X509SerialNumber>1053495409</X509SerialNumber>
              </X509IssuerSerial>
            </X509Data>
          </KeyInfo>
        </Signature>
      </tns:RacunOdgovor>
    </soap:Body>
</soap:Envelope>
```

9.5 Poruka zahtjeva za poslovni prostor u izvornom obliku

Primjer poruke zahtjeva za poslovni prostor sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <f73:PoslovniProstorZahtjev xmlns:f73="http://www.apis-it.hr/fin/2012/types/f73">
      <f73:Zaglavlje>
```

```
            <f73:IdPoruke>ca996cc7-fcc3-4c50-961b-40c8b875a5e8</f73:IdPoruke>
            <f73:DatumVrijeme>01.09.2012T21:10:34</f73:DatumVrijeme>
         </f73:Zaglavlje>
         <f73:PoslovniProstor>
            <f73:Oib>98765432198</f73:Oib>
            <f73:OznPoslProstora>Poslovnica1</f73:OznPoslProstora>
            <f73:AdresniPodatak>
               <f73:Adresa>
                  <f73:Ulica>Avenija Marina Drzica</f73:Ulica>
                  <f73:KucniBroj>0014</f73:KucniBroj>
                  <f73:KucniBrojDodatak>B</f73:KucniBrojDodatak>
                  <f73:BrojPoste>10000</f73:BrojPoste>
                  <f73:Naselje>Zagreb</f73:Naselje>
                  <f73:Opcina>12345</f73:Opcina>
               </f73:Adresa>
            </f73:AdresniPodatak>
            <f73:RadnoVrijeme>Pon: 07:00-14:00, Uto: 07:00-17:00, Sri: 18:00-20:00, Čet: 12:00-16:00,
Pet: 09:00-18:00, Sub: 08:00-21:00, Ned: 09:00-14:00</f73:RadnoVrijeme>
            <f73:DatumPocetkaPrimjene>01.01.2013</f73:DatumPocetkaPrimjene>
            <f73:SpecNamj>08765432498</f73:SpecNamj>
         </f73:PoslovniProstor>
      </f73:PoslovniProstorZahtjev>
   </soapenv:Body>
</soapenv:Envelope>
```

9.6 Poruka zahtjeva za poslovni prostor s elektroničkim potpisom

Primjer poruke zahtjeva za poslovni prostor s elektroničkim potpisom i SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header/>
   <soapenv:Body>
      <f73:PoslovniProstorZahtjev xmlns:f73="http://www.apis-it.hr/fin/2012/types/f73"
Id="poslovniProstorId">
         <f73:Zaglavlje>
            <f73:IdPoruke>ca996cc7-fcc3-4c50-961b-40c8b875a5e8</f73:IdPoruke>
            <f73:DatumVrijeme>01.09.2012T21:10:34</f73:DatumVrijeme>
         </f73:Zaglavlje>
         <f73:PoslovniProstor>
            <f73:Oib>98765432198</f73:Oib>
            <f73:OznPoslProstora>Poslovnica1</f73:OznPoslProstora>
            <f73:AdresniPodatak>
               <f73:Adresa>
                  <f73:Ulica>Avenija Marina Drzica</f73:Ulica>
                  <f73:KucniBroj>0014</f73:KucniBroj>
                  <f73:KucniBrojDodatak>B</f73:KucniBrojDodatak>
                  <f73:BrojPoste>10000</f73:BrojPoste>
                  <f73:Naselje>Zagreb</f73:Naselje>
                  <f73:Opcina>12345</f73:Opcina>
               </f73:Adresa>
            </f73:AdresniPodatak>
            <f73:RadnoVrijeme>Pon: 07:00-14:00, Uto: 07:00-17:00, Sri: 18:00-20:00, Čet: 12:00-16:00,
Pet: 09:00-18:00, Sub: 08:00-21:00, Ned: 09:00-14:00</f73:RadnoVrijeme>
            <f73:DatumPocetkaPrimjene>01.01.2013</f73:DatumPocetkaPrimjene>
            <f73:SpecNamj>08765432498</f73:SpecNamj>
         </f73:PoslovniProstor>
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="#poslovniProstorId ">
```

```
                <Transforms>
                  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                  <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>+vic+VWcV/Wv6At1T2mPVHS3Mfs=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>F/RaqwWB80cKk84vToP7A3osABm4JSBHbkGqfMhh7OYz3HskQILxGHnH1Jsy3t+gG5x
VxAffDN6Q/gmQoVgYm/BVUOp7abLg7jQokfE1KU296GQk6Tu+B3X/2G1tXbrtY/sLKxF6L39ayH3ZjZ2Yph
EQlbY+phVxf8c3qLxEJraXdZ+S2KcW5jze0FGX3B8sM9mJ9wDxthC3izH+F7GsTyEcPhrt9/XVc6hPE91njV
B7REDgKb5MnkOwp+3g1QXc053MhSnvZnF/CyTA5o6izXfIeKSrAirR+noZYVY3iTt66rrRSpg6Wt7NtsIyzSIr
QXC8P9VYsfRRLXb3y9pXog==</SignatureValue>
            <KeyInfo>
              <X509Data>
<X509Certificate>MIIEyDCCA7CgAwIBAgIEPssQ1zANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJI
UjENMAsGA1UEChMERklOQTENMAsGA1UECxMEREVNTzAeFw0xMjA5MjcxMDQyMTVaFw0xNDA5Mjc
xMTEyMTVaMFkxCzAJBgNVBAYTAkhSMSYwJAYDVQQKEx1BUElTIElUICBELk8uTy4gSFIwMjk5NDY1M
DE5OTEPMA0GA1UEBxMGWkFHUkVCMREwDwYDVQQDEwhGSVNLQUwgMTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALV8bgiergOm+P4EUu2UTPzsdjv122fOBTQ9CyimNyvwNBHFypSYW
wSJffkdOnmRZkcFhPebhoUCq3/RHbd1gBsi5rUkuihppwJjzoi2YGh9yNEZ0zI/yTSQwbyFvsszkGOcJ/29OM
aDc5/i8zTJb+UX0UYcpXXxup8s/y78hfqnbaKHG2e+YeCwHP5g3m4JXEzpZXvETGE9XUKLOpJpVAKrXkc
F1nn2FdNuF8ijmK6+UYRSK1AkAVNpyDOVCiHWDPqukJZjn+x9b+27glZCZluTlQF+mv9EAY1UsRJpaIvyE
UOnkDstZKIX/S7lLpA1J2BvBmw5NFgzM+Vp9pl79uUCAwEAAaOCAcQwggHAMAsGA1UdDwQEAwIFoD
BCBgNVHSAEOzA5MDcGCSt8iFAFHwUDATAqMCgGCCsGAQUFBwIBFhxodHRwOi8vZGVtby1wa2kuZm
luYS5oci9jcHMvMCQGA1UdEQQdMBuBGXNhbmRyYS5wb3BvdmljQGFwaXMtaXQuaHIwgc4GA1UdHwS
BxjCBwzBCoECgPqQ8MDoxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwR
ERU1PMQ0wCwYDVQQDEwRDUkw3MH2ge6B5hk9sZGFwOi8vZGVtby1sZGFwLmZpbmEuaHIvb3U9RE
VNTyxvPUZJTkEsYz1lUj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0JTNCYmluYXJ5hiZodHRwOi8vZGVt
by1wa2kuZmluYS5oci9jcmwvZGVtb2NhLmNybDArBgNVHRAEJDAigA8yMDEyMDkyNzEwNDIxNVqBDzIw
MTQwOTI3MTExMjE1WjAfBgNVHSMEGDAWgBR6YCOOSJ0ya6TlLd24WbSU/EJinjAdBgNVHQ4EFgQUf
Hua2wrUtvvhCp20GCXDc0fv4VMwCQYDVR0TBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAf7laIW7pM23
HSF6aoSn/OUezF1udcIpewWdjxnoRITyHyAblWc0LRJd7Imhza5gT11Ofv5LKoSDkLID7OgOQN4+ydKEqX
0274HK7ybuieIknu3t2zUtBK1K+hOvM+jL8Be3cHIcQ9JzN89GETBpmTsXk8xZzTmZXh/zCc4NG76Cuta6M
zosRaYpnPBZeqGiSodd3+E5Aeh6yfinoOU0POw4/SYC462mw85V8hS2mYJKOlmjZ6RpxFn9EUr0gFjhzMu
8GjM2yr0sVv+G2vLhUwn3PTFXwKuOQO8ZOgxwgY3BtVYwNr3b/3XO/g/YU8rwTdestkxAQphsClWpxZQS
uJQ==</X509Certificate>
                <X509IssuerSerial>
                  <X509IssuerName>OU=DEMO,O=FINA,C=HR</X509IssuerName>
                  <X509SerialNumber>1053495511</X509SerialNumber>
                </X509IssuerSerial>
              </X509Data>
            </KeyInfo>
          </Signature>
        </f73:PoslovniProstorZahtjev>
    </soapenv:Body>
</soapenv:Envelope>
```

9.7 Poruka odgovora za poslovni prostor u izvornom obliku

Primjer poruke odgovora za poslovni prostor sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
      <tns:PoslovniProstorOdgovor
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
         <tns:Zaglavlje>
```

```
            <tns:IdPoruke>ca996cc7-fcc3-4c50-961b-40c8b875a5e8</tns:IdPoruke>
            <tns:DatumVrijeme>23.10.2012T13:22:34</tns:DatumVrijeme>
         </tns:Zaglavlje>
      </tns:PoslovniProstorOdgovor>
   </soap:Body>
</soap:Envelope>
```

9.8 Poruka odgovora za poslovni prostor s elektroničkim potpisom

Primjer poruke odgovora za poslovni prostor s elektroničkim potpisom i SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
      <tns:PoslovniProstorOdgovor Id="G0xcbfb9080-4D"
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
         <tns:Zaglavlje>
            <tns:IdPoruke>ca996cc7-fcc3-4c50-961b-40c8b875a5e8</tns:IdPoruke>
            <tns:DatumVrijeme>23.10.2012T13:22:34</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="#G0xcbfb9080-4D">
                  <Transforms>
                     <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                     <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                  </Transforms>
                  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <DigestValue>BU3BaMWszPDqMMo+colE7weMHiA=</DigestValue>
               </Reference>
            </SignedInfo>

<SignatureValue>nr4B2pzZCRJsJDo+eWbUlTP1LD5J8RNswim5P/MmwTbc/i6QJ4p7gARQXQ0fn+dHb0aj
18CUnJryOY0q7kRayzGqqgiQyA7va8WOQ6RNc+jcfjyNc7lFF0FiExUrE8RuirKd8nTqqQIeHemZ7guOGiR/li
On24e3cJp27Rgp5s6f3TR2wr7AwtTU977BuH7BIRiGUTDQ2UH/64UoP1VNnnsBVKt2Wias+QF0sNSBEpm
3Le1n6jkvXlMMloncOhvoQfVRRfnMYGJDzUN/knxCTrQ8Ll1Le2I+0T9NmfxDlCbjhhqcNolJnxK3NWIx8+SC
Ub5iFKDWxQDsqpjKGyRK6A==</SignatureValue>
            <KeyInfo>
               <X509Data>
<X509Certificate>MIIExDCCA6ygAwIBAgIEPssQcTANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJI
UjENMAsGA1UEChMERklOQTENMAsGA1UECxMEREVNTzAeFw0xMjA5MjYwODExNDlaFw0xNDA5MjY
wODQxNDlaMHgxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1PM
REwDwYDVQQLEwhQb3Nsb3ZuaTEgMB4GA1UECxMXQVBJUyBJVCBELk8uTy4gODA1NDEzNzIxFjAU
BgNVBAMTDWZpc2thbGNpc3Rlc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC81TtKtJ
84emCS/HK7gSovjNdluZWB0DbIMq3cBFpOpmurcbDCJ1Z17XiPLa+UWYIqyAjHQyDnG/H4c5EeGoli9swz
5QcZFBmyXTpSd3GuMROgUAd4bcvbw1/HDONE5cE8PL11GIy8gi5ANZkujalYmx+1ImnhHxx1Bh2UJ/bcl2
eXPtieBQBwtClATSzseB5FFz8LcSyfzM7h39PsAIZ0p8YzH7W+307gvgrJHYb/n4ADwlxieHqb5j74DVD0rUP
cUE5d0nSZ7hfEkW8xICgs1Ly6Vu3w7Z5M8vb4QmoPnIT1EaHCXiweuK6vjkUk8RQmYY4ITFBs8zHiG7h4n
9bPAgMBAAGjggGhMIIBnTAOBgNVHQ8BAf8EBAMCBaAwQgYDVR0gBDswOTA3BgkrfIhQBR8FBAIwKjA
oBggrBgEFBQcCARYcaHR0cDovL2RlbW8tcGtpLmZpbmEuaHIvY3BzLzCBzgYDVR0fBIHGMIHDMEKgQK
A+pDwwOjELMAkGA1UEBhMCSFIxDTALBgNVBAoTBEZJTkExDTALBgNVBAsTBERFTU8xDTALBgNVB
AMTBENSTDcwfaB7oHmGT2xkYXA6Ly9kZW1vLWxkYXAuZmluYS5oci9vdT1ERU1PLG89RklOQSxjPUhS
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QlM0JiaW5hcnmGJmh0dHA6Ly9kZW1vLXBraS5maW5hLmhyL
2NybC9kZW1vY2EuY3JsMCsGA1UdEAQkMCKADzIwMTIwOTI2MDgxMTQ5WoEPMjAxNDA5MjYwODQx
NDlaMB8GA1UdIwQYMBaAFHpgI45InTJrpOUt3bhZtJT8QmKeMB0GA1UdDgQWBBRgIJsZevSn6kDuSzC
hmaa9Sqr6sjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBBQUAA4IBAQCo5kJWaNjgS+UG7XQHsHersDFk
4K5W/Y2Pbubary0j3IwJrveHbUR3HOb0KiVenF6+1FL3sCI/2tfH3wSszWL8Gkit8jUudTo5vDyLqEUXYDHlF
UBwseudsPkUxPiQ6HuuFd3PiUAWf00chXD38eTjfapNu6VeQt4EORSO+rEXdhWihVb5HxFIVPTkqHmq1KI
```

NwtV9+thwE3hNMwacRa4gwTB1O+jadVlJQMq+kgwnLGLBcwr0W+x1ye6MPSYEUxSNFGHPG/evP9DRL
wJtR3ngvlCDusnO+A75Nn40VYcoIjw6EN1V+plK+HkLye0zzLsnHIWTSGfZ2sQVG5xCURiI</X509Certificate>
<X509IssuerSerial>
<X509IssuerName>**OU=DEMO, O=FINA, C=HR**</X509IssuerName>
<X509SerialNumber>**1053495409**</X509SerialNumber>
</X509IssuerSerial>
</X509Data>
</KeyInfo>
</Signature>
</tns:PoslovniProstorOdgovor>
</soap:Body>
</soap:Envelope>

9.9 Poruka odgovora za račun koja sadrži grešku u izvornom obliku

Primjer poruke odgovora za račun koji sadrži grešku sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
      <tns:RacunOdgovor
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 ../schema/FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
         <tns:Zaglavlje>
            <tns:IdPoruke>733362f3-063f-11e2-892e-080b300c9a66</tns:IdPoruke>
            <tns:DatumVrijeme>23.10.2012T13:22:34</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <tns:Greske>
            <tns:Greska>
               <tns:SifraGreske>s001</tns:SifraGreske>
               <tns:PorukaGreske>
                  Poruka nije u skladu s XML shemom :  cvc-simple-type 1: element {http://www.apis-
it.hr/fin/2012/types/f73}IznosUkupno value '7000000008000990.99' is not a valid instance of type
{http://www.apis-it.hr/fin/2012/types/f73}IznosType</tns:PorukaGreske>
            </tns:Greska>
         </tns:Greske>
      </tns:RacunOdgovor>
   </soap:Body>
</soap:Envelope>
```

9.10 Poruka odgovora za račun koja sadrži grešku s elektroničkim potpisom

Primjer poruke odgovora za račun koji sadrži grešku s elektroničkim potpisom i SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
      <tns:RacunOdgovor Id="G0xc3d48080-4D"
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 ../schema/FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">
         <tns:Zaglavlje>
            <tns:IdPoruke>733362f3-063f-11e2-892e-080b300c9a66</tns:IdPoruke>
            <tns:DatumVrijeme>23.10.2012T13:22:34</tns:DatumVrijeme>
         </tns:Zaglavlje>
         <tns:Greske>
            <tns:Greska>
```

<tns:SifraGreske>**s001**</tns:SifraGreske>
<tns:PorukaGreske>
Poruka nije u skladu s XML shemom : cvc-simple-type 1: element {http://www.apis-it.hr/fin/2012/types/f73}IznosUkupno value '7000000008000990.99' is not a valid instance of type {http://www.apis-it.hr/fin/2012/types/f73}IznosType</tns:PorukaGreske>
</tns:Greska>
</tns:Greske>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#G0xc3d48080-4D">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>**USfG3sQEIropBabTSMfC+z+2QQs=**</DigestValue>
</Reference>
</SignedInfo>

<SignatureValue>OJnC52ayKIHRehSLYOvlJ273u/dR5qqG/4L2WVaAMylJexQ0fDJFyQpAovQqqCMxIjLT4b0pj4OQis93Ll4a/v5+2b+taOcM//0kyloIJkm9wldC+zyo9AqrB3YdPdSiHPWTY7jGtNKYPRg/5SEvYIGDFQCsD5CLa4eJHDp6hl+DN6gnDlCC5q84YTO8Xxa3valkt+3mSl6DaDhbmY0Dq41+MTzie8bdRmTf+Ar8FqiBst82+2TGdVdWrtjtL2lwATR669022Pd9aAJe9W8UZoDpBng6JVSsNH+WViQb1lBNoKfxyESgeLY0fC97f726UlY5J+H8lSedcYEnWb5HDw==</SignatureValue>
<KeyInfo>
<X509Data>

<X509Certificate>MIIExDCCA6ygAwIBAgIEPssQcTANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJIUjENMAsGA1UEChMERklOQTENMAsGA1UECxMEREVNTzAeFw0xMjA5MjYwODExNDlaFw0xNDA5MjYwODQxNDlaMHgxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1PMREwDwYDVQQLEwhQb3Nsb3ZuaTEgMB4GA1UECxMXQVBJUyBJVCBELk8uTy4gODA1NDEzNzIxFjAUBgNVBAMTDWZpc2thbGNpc3Rlc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC81TtKtJ84emCS/HK7gSovjNdluZWB0DbIMq3cBFpOpmurcbDCJ1Z17XiPLa+UWYIqyAjHQyDnG/H4c5EeGoli9swz5QcZFBmyXTpSd3GuMROgUAd4bcvbw1/HDONE5cE8PL11GIy8gi5ANZkujalYmx+1ImnhHxx1Bh2UJ/bcl2eXPtieBQBwtClATSzseB5FFz8LcSyfzM7h39PsAIZ0p8YzH7W+307gvgrJHYb/n4ADwlxieHqb5j74DVD0rUPcUE5d0nSZ7hfEkW8xICgs1Ly6Vu3w7Z5M8vb4QmoPnIT1EaHCXiweuK6vjkUk8RQmYY4ITFBs8zHiG7h4n9bPAgMBAAGjggGhMIIBnTAOBgNVHQ8BAf8EBAMCBaAwQgYDVR0gBDswOTA3BgkrfIhQBR8FBAIwKjAoBggrBgEFBQcCARYcaHR0cDovL2RlbW8tcGtpLmZpbmEuaHIvY3BzLzCBzgYDVR0fBIHGMIHDMEKgQKA+pDwwOjELMAkGA1UEBhMCSFIxDTALBgNVBAoTBEZJTkExDTALBgNVBAsTBERFTU8xDTALBgNVBAMTBENSTDcwfaB7oHmGT2xkYXA6Ly9kZW1vLWxkYXAuZmluYS5oci9vdT1ERU1PLG89RklOQSxjPUhSP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QlM0JiaW5hcnmGJmh0dHA6Ly9kZW1vLXBraS5maW5hLmhyL2NybC9kZW1vY2EuY3JsMCsGA1UdEAQkMCKADzIwMTIwOTI2MDgxMTQ5WoEPMjAxNDA5MjYwODQxNDlaMB8GA1UdIwQYMBaAFHpgI45InTJrpOUt3bhZtJT8QmKeMB0GA1UdDgQWBBRgIJsZevSn6kDuSzChmaa9Sqr6sjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBBQUAA4IBAQCo5kJWaNjgS+UG7XQHsHersDFk4K5W/Y2Pbubary0j3IwJrveHbUR3HOb0KiVenF6+1FL3sCI/2tfH3wSszWL8Gkit8jUudTo5vDyLqEUXYDHlFUBwseudsPkUxPiQ6HuuFd3PiUAWf00chXD38eTjfapNu6VeQt4EORSO+rEXdhWihVb5HxFIVPTkqHmq1KINwtV9+thwE3hNMwacRa4gwTB1O+jadVlJQMq+kgwnLGLBcwr0W+x1ye6MPSYEUxSNFGHPG/evP9DRLwJtR3ngvlCDusnO+A75Nn40VYcoIjw6EN1V+plK+HkLye0zzLsnHIWTSGfZ2sQVG5xCURil</X509Certificate>
<X509IssuerSerial>
<X509IssuerName>**OU=DEMO, O=FINA, C=HR**</X509IssuerName>
<X509SerialNumber>**1053495409**</X509SerialNumber>
</X509IssuerSerial>
</X509Data>
</KeyInfo>
</Signature>
</tns:RacunOdgovor>
</soap:Body>
</soap:Envelope>

9.11 Poruka zahtjeva za echo metodu

Primjer poruke zahtjeva za echo metodu sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:f73="http://www.apis-it.hr/fin/2012/types/f73">
  <soapenv:Body>
    <f73:EchoRequest>proizvoljan tekst</f73:EchoRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

9.12 Poruka odgovora za echo metodu

Primjer poruke odgovora za echo metodu sa SOAP envelopom:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <tns:EchoResponse
xsi:schemaLocation="http://www.apis-it.hr/fin/2012/types/f73 FiskalizacijaSchema.xsd "
xmlns:tns="http://www.apis-it.hr/fin/2012/types/f73">proizvoljan tekst</tns:EchoResponse>
  </soap:Body>
</soap:Envelope>
```

10. Podrška u radu

Upiti obveznika fiskalizacije vezano za pitanja pravne ili poslovne prirode dostavljaju se na email adresu Porezne uprave fiskalizacija@porezna-uprava.hr.

FINA pruža podršku obveznicima fiskalizacije oko postupaka vezanih za izdavanje i korištenje certifikata putem email adrese certifikati-fiskalizacija@fina.hr.

APIS IT pruža podršku proizvođačima/održavateljima softvera vezano za tehničke specifikacije i tehničke probleme u povezivanju na CIS Porezne uprave putem email adrese fiskalizacija.help@apis-it.hr.

11. DODATAK: Informacija o izdavanju FINA certifikata za uključivanje korisnika na CIS

Sve informacije o izdavanju aplikativnog digitalnog certifikata za fiskalizaciju osigurava FINA. Informacije o izdavanju aplikativnog digitalnog certifikata za fiskalizaciju za testnu okolinu dostupne su na http://www.fina.hr/fiskalizacija.

Dodatne informacije mogu se dobiti na telefon 0800 0080.

12. DODATAK: Zaštitni kod izdavatelja

Zaštitni kod izdavatelja obveznika fiskalizacije je alfanumerički zapis kojim se potvrđuje veza između obveznika fiskalizacije i izdanog računa. Zaštitni kod formira obveznik fiskalizacije, ispisuje ga na računu i dostavlja Poreznoj upravi kao obavezni element računa.

Osnovna namjena ovog koda je da se obveznik fiskalizacije zaštiti od mogućih pokušaja nanošenja štete od strane treće osobe. Samo obveznik fiskalizacije može ponovo kreirati isti zaštitni kod temeljem ulaznih parametara za konstrukciju koda. Porezna uprava ne provjerava zaštitni kod ali na njezin zahtjev obveznik fiskalizacije, temeljem istih ulaznih parametara, mora kreirati zaštitni kod jednak onome s računa.

Druga namjena zaštitnog koda je provjera računa putem Weba i SMS-a u slučajevima kad je račun izdan bez JIR-a. U tom slučaju se zaštiti kod može koristiti kao identifikator računa u kombinaciji s drugim podacima.

Kako bi se osigurale prije navedene namjene, zaštitni kod mora biti određen s nekoliko parametara koji osiguravaju:

a) jedinstvenost računa: OIB obveznika, datum i vrijeme izdavanja računa, brojčana oznaka računa, oznaka poslovnog prostora, oznaka naplatnog uređaja, ukupni iznos računa,
b) autentičnost korisnika: elektronički potpis s FINA certifikatom za fiskalizaciju koji je dodijeljen obvezniku.

Pri računanju zaštitnog koda koristi se UTF-8 (Unicode Transformation Format 8) kodiranje. Kao decimalni separator kod podatka ukupni iznos potrebno je koristiti točku, a ne zarez (npr. 1245.56).
Elektroničko potpisivanje vrši se koristeći RSA-SHA1 elektronički potpis s važećim FINA certifikatom za fiskalizaciju koji je dodijeljen obvezniku.

Koristeći MD5 kriptografsku hash funkciju (po standardu RFC 1321 The MD5 Message-Digest Algorithm) dobiva se rezultat: 32-znamenkasti broj zapisan u heksadecimalnom formatu (brojevi i mala slova: 0-9, a-f) koji se ispisuje na račun.

Primjer zaštitnog koda:

a1e6b1428f0cc755f0c82aa7a1327e35

Algoritam za izračun zaštitnog koda može se sažeto prikazati na sljedeći način:
MD5 hash (Elektronički potpis privatnim ključem (OIB+datum i vrijeme izdavanja+brojčana oznaka računa+oznaka poslovnog prostora+oznaka naplatnog uređaja+ukupni iznos računa))

U nastavku je opisan pseudokod algoritma i daju se primjeri dvije implementacije algoritma, jedan u Java i drugi u .NET tehnologiji. Primjeri implementacije isključivo se navode kao pomoć korisnicima u lakšem razumijevanju algoritma i pseudokoda i mogu se koristiti samo za tu namjenu.

12.1 Pesudokod algoritma

U nastavku je opisan pseudokod algoritma za izračun zaštitnog koda izdavatelja:

```
početak

pročitaj (oib)

medjurezultat = oib

pročitaj (datVrij – datum i vrijeme izdavanja računa zapisani kao tekst
u formatu 'dd.MM.gggg HH:mm:ss')

medjurezultat = medjurezultat + datVrij

pročitaj (bor – brojčana oznaka računa)
```

```
medjurezultat = medjurezultat + bor

pročitaj (opp – oznaka poslovnog prostora)

medjurezultat = medjurezultat + opp

pročitaj (onu – oznaka naplatnog uređaja)

medjurezultat = medjurezultat + onu

pročitaj (uir - ukupni iznos računa)

medjurezultat = medjurezultat + uir

elektronički potpiši medjurezultat koristeći RSA-SHA1 potpis

rezultatIspis = izračunajMD5(elektronički potpisani medjurezultat)

kraj
```

12.2 Implementacija Java

U nastavku se navodi primjer izvornog koda za izračun zaštitnog koda izdavatelja napravljen u Java tehnologiji. Primjer implementacije isključivo se navodi kao pomoć korisnicima u lakšem razumijevanju algoritma i pseudokoda i može se koristiti samo za tu namjenu.

```
/*
 * @(#)ZastitniKodIzracun.java
 *
 * Project: Fiskalizacija
 *
 * Copyright (c) APIS IT d.o.o. Paljetkova 18 Zagreb, Hrvatska
 */
package primjer;

import java.io.FileInputStream;
import java.security.Key;
import java.security.KeyStore;
import java.security.PrivateKey;
import java.security.Signature;

import org.apache.commons.codec.digest.DigestUtils;

/**
 * ZastitniKodIzracun - klasa za izračun zaštitnog broja napisana tako da prati
pseudokod.
*/
public class ZastitniKodIzracun {

    public static void main( String[] args ) {
        // početak
        // pročitaj (oib)
        String oib = "00169331406";
        // medjurezultat = oib
        String medjurezultat = oib;
        // pročitaj (datVrij – datum i vrijeme izdavanja računa zapisain kao tekst u
formatu 'dd.MM.gggg HH:mm:ss')
        String datVrij = new SimpleDateFormat( "dd.MM.yyyy HH:mm:ss" ).format( new
Date() );
        // medjurezultat = medjurezultat + datVrij
        medjurezultat = medjurezultat + datVrij;
        // pročitaj (bor – brojčana oznaka računa)
        String bor = "12345";
```

```
        // medjurezultat = medjurezultat + bor
        medjurezultat = medjurezultat + bor;
        // pročitaj (opp – oznaka poslovnog prostora)
        String opp = "blag001";
        // medjurezultat = medjurezultat + opp
        medjurezultat = medjurezultat + opp;
        // pročitaj (onu – oznaka naplatnog uređaja)
        String onu = "11245";
        // medjurezultat = medjurezultat + onu
        medjurezultat = medjurezultat + onu;
        // pročitaj (  uir - ukupni iznos računa )
        String uir = "1245.56";
        // medjurezultat = medjurezultat + uir
        medjurezultat = medjurezultat + uir;
        // elektronički potpiši medjurezultat koristeći RSA-SHA1 potpis
        byte[] potpisano = null;
        try {
            FileInputStream file_inputstream = new
FileInputStream("D:\\Certifikat\\key.jks");
            KeyStore keyStore = KeyStore.getInstance( "JKS" );
            keyStore.load( file_inputstream, "lozinka".toCharArray() );
            Key privatni = keyStore.getKey( "alias", " lozinka ".toCharArray() );
            Signature biljeznik = Signature.getInstance( "SHA1withRSA" );
            biljeznik.initSign( ( PrivateKey )privatni );
            biljeznik.update( medjurezultat.getBytes() );
            potpisano = biljeznik.sign();
        }
        catch ( Exception e ) {
            // nije uspjelo čitanje privatnog ključa
            e.printStackTrace();
        }
        // rezultatIspis = izračunajMD5(elektronički potpisani medjurezultat)
        String rezultatIspis = DigestUtils.md5Hex( potpisano );
        // kraj
        System.out.println( "Dobiveni 32-znamenkasti zaštitni kod je: " + rezultatIspis
);
    }
}
```

12.3 Implementacija .NET (C#)

U nastavku se navodi primjer izvornog koda za izračun zaštitnog koda izdavatelja napravljen u .NET tehnologiji. Primjer implementacije isključivo se navodi kao pomoć korisnicima u lakšem razumijevanju algoritma i pseudokoda i može se koristiti samo za tu namjenu.

```
/*
 * Copyright (c) APIS IT d.o.o. Paljetkova 18 Zagreb, Hrvatska
 */

using System;
using System.Collections.Generic;
using System.Text;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;

namespace ZastitniKod
{
    // ZastitniKodIzracun - klasa za izračun zaštitnog broja napisana tako da prati pseudokod.
    class ZastitniKodIzracun
    {
        static void Main(string[] args)
        {
            // početak
            // pročitaj (oib)
            string oib = "00169331406";
            // medjurezultat = oib
            string medjurezultat = oib;
```

```
            // pročitaj (datVrij – datum i vrijeme izdavanja računa zapisani kao tekst u formatu
'dd.MM.gggg HH:mm:ss')
            string datVrij = "01.10.2012 16:04:25";
            // medjurezultat = medjurezultat + datVrij
            medjurezultat = medjurezultat + datVrij;
            // pročitaj (bor – brojčana oznaka računa)
            string bor = "12345";
            // medjurezultat = medjurezultat + bor
            medjurezultat = medjurezultat + bor;
            // pročitaj (opp – oznaka poslovnog prostora)
            string opp = "blag001";
            // medjurezultat = medjurezultat + opp
            medjurezultat = medjurezultat + opp;
            // pročitaj (onu – oznaka naplatnog uređaja)
            string onu = "11245";
            // medjurezultat = medjurezultat + onu
            medjurezultat = medjurezultat + onu;
            // pročitaj (uir - ukupni iznos računa)
            string uir = "1245.56";
            // medjurezultat = medjurezultat + uir
            medjurezultat = medjurezultat + uir;
            // elektronički potpiši medjurezultat koristeći RSA-SHA1 potpis
            byte[] potpisano = null;
            try
            {
                X509Certificate2 certifikat = new X509Certificate2("c:\\certifikat.p12",
"lozinka");
                RSACryptoServiceProvider rsa = (RSACryptoServiceProvider)certifikat.PrivateKey;
                byte[] podaci = Encoding.ASCII.GetBytes(medjurezultat);
                potpisano = rsa.SignData(podaci, new SHA1CryptoServiceProvider());

                // rezultatIspis = izračunajMD5(elektronički potpisani medjurezultat)
                MD5 md5Hash = MD5.Create();
                string rezultatIspis = GetMd5Hash(md5Hash, potpisano);
                // kraj
                Console.WriteLine("Dobiveni 32-znamenkasti zaštitni kod je: " + rezultatIspis);
            }
            catch (Exception ex)
            {
                // greška
                Console.WriteLine(ex.Message);
            }
        }

        // Metoda za izračun MD5 hash
        static string GetMd5Hash(MD5 md5Hash, byte[] input)
        {
            byte[] data = md5Hash.ComputeHash(input);
            StringBuilder sBuilder = new StringBuilder();
            for (int i = 0; i < data.Length; i++)
            {
                sBuilder.Append(data[i].ToString("x2"));
            }
            return sBuilder.ToString();
        }
    }
}
```

13. Prilozi

Kao prilog ovom dokumentu dolazi datoteka „Fiskalizacija-WSDL_v1.1.zip“.