

# **Fiskalizacija - Tehnička specifikacija za korisnike**

## **Verzija 1.7**

---

## 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
1.2	4.12.2012.	Izmjene i dopune u poglavljima 1, 2.1, 2.2, 2.2.1, 2.2.2, 2.3, 3, 3.1, 3.2, 4.1, 4.2, 5, 6, 6.1, 7, 9, 9.5, 9.6, 11, 13	APIS IT
1.3	14.04.2016.	Izmjene i dopune u poglavljima: 2.1, 2.2, 2.3, 3, 4, 5, 6, 7, 8, 9.	APIS IT
1.4	28.07.2016.	Izmijenjena i dodana poglavlja 2, 2.4, 9.13, 9.14, 9.15, 9.16 i 13	APIS IT
1.5	27.04.2017.	Izbačeno poglavlje 2.2 i pripadajuća potpoglavlja, izbačeno poglavlje 9.5, 9.6, 9.7, 9.8. Izmijenjena poglavlja 1, 2 i pripadajuća potpoglavlja, 4, 5, 6, 7, 10, 14.	APIS IT
1.6	18.12.2017.	Izmijenjeno poglavlje 2.2.1(izbačen navod članka PDV-a vezan za maržu), dodatak: šifarnik grešaka kod provjere računa (izbačena greška 138, dodana greška 148).	APIS IT
1.7	31.12.2018.	Izmjena šifarnika grešaka kod provjere računa: dodane greške 149 i 150, izbačena greška 102.	APIS IT

---

# Sadržaj

1.	Uvod	5
1.1	Definicije i skraćenice	5
2.	Poslovna interakcija korisnika sustava	6
2.1	Račun	6
2.1.1	Podatkovni skup zahtjeva za račun	9
2.1.2	Primjer poruke zahtjeva za račun	14
2.1.3	Podatkovni skup odgovora za račun	15
2.1.4	Primjer poruke odgovora za račun	16
2.2	Echo metoda	16
2.2.1	Primjer poruke zahtjeva za echo metodu	17
2.2.2	Primjer poruke odgovora za echo metodu	17
2.3	Provjera računa koji su dostavljeni u Poreznu upravu	17
2.3.1	Podatkovni skup zahtjeva za provjeru računa	18
2.3.2	Primjer poruke zahtjeva za provjeru računa	18
2.3.3	Podatkovni skup odgovora za provjeru računa	19
2.3.4	Primjer poruke odgovora za provjeru računa	20
2.4	Šifarnik grešaka	22
3.	Pregled preduvjeta za spajanje na CIS Porezne uprave	24
3.1	Mrežni preduvjeti i preporuke	24
3.2	Sigurnosni preduvjeti	24
3.3	Aplikacijski preduvjeti	24
4.	Topologija pristupa CIS-u Porezne uprave	26
4.1	Sigurnost (zaštita od uplitanja treće strane)	26
4.2	Kontrola pristupa	27
5.	Public Key Infrastructure (PKI)	28
6.	Postupak spajanja obveznika fiskalizacije na CIS Porezne uprave	29
6.1	Url adrese za spajanje na CIS Porezne uprave	29
7.	Elektronički potpis poruke zahtjeva	30
8.	Pregled tehnologija korištenih u komunikaciji s pristupnom točkom CIS-a	33
8.1	XML	33
8.2	SOAP	33
8.3	WS-x	33
8.4	WSDL	33
8.5	HTTP	33
8.6	HTTPS	34
8.7	XMLDsig	34
8.7.1	XML Canonicalization	34
8.8	UUID	34

9.	Primjeri poruka	35
9.1	Poruka zahtjeva za račun u izvornom obliku	35
9.2	Poruka zahtjeva za račun s elektroničkim potpisom	36
9.3	Poruka odgovora za račun u izvornom obliku	38
9.4	Poruka odgovora za račun s elektroničkim potpisom	38
9.5	Poruka odgovora za račun koja sadrži grešku u izvornom obliku	39
9.6	Poruka odgovora za račun koja sadrži grešku s elektroničkim potpisom	40
9.7	Poruka zahtjeva za echo metodu	41
9.8	Poruka odgovora za echo metodu	41
9.9	Poruka zahtjeva za provjeru računa u izvornom obliku	41
9.10	Poruka zahtjeva za provjeru računa s elektroničkim potpisom	43
9.11	Poruka odgovora za provjeru računa u izvornom obliku	45
9.12	Poruka odgovora za provjeru računa s elektroničkim potpisom	46
10.	Podrška u radu	49
11.	DODATAK: Informacija o izdavanju FINA certifikata za uključivanje korisnika na CIS	50
12.	DODATAK: Zaštitni kod izdavatelja	51
12.1	Pseudokod algoritma	51
12.2	Implementacija Java	52
12.3	Implementacija .NET (C#)	53
13.	DODATAK: Šifarnik grešaka kod provjere računa	55
14.	Prilozi	59

---

---

# 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 računa 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.

### 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

Jedan je tip poslovnih poruka koje su obveznici fiskalizacije dužni dostavljati Poreznoj upravi:

- Račun

Osim razmjene poslovnih poruka računa, servisom je predviđena mogućnost provjere dostupnosti servisa tehničkom porukom *echo*. Dodatno, u testnoj okolini je omogućena provjera računa.

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.

### Napomena:

*Podatke o poslovnom prostoru obveznici fiskalizacije od 01. srpnja 2017. godine prijavljuju putem elektroničkog servisa Porezne uprave ePorezna.*

*Obveznici koji su do 1. srpnja 2017. godine prijavili poslovne prostore na postojeći način slanjem XML poruka u sustav fiskalizacije, dužni su te poslovne prostore ponovo prijaviti putem servisa ePorezna i to u razdoblju od 1. srpnja 2017. godine i najkasnije do 31. srpnja 2017. godine.*

### 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 privatnim ključem aplikativnog certifikata koji je izdan obvezniku u svrhu fiskalizacije (u testnoj okolini koristi se DEMO aplikativni certifikat). Nakon toga inicira 1-way TLS komunikaciju pri čemu se poslužitelj Porezne uprave predstavlja s poslužiteljskim certifikatom *cis.porezna-uprava.hr* (u testnoj okolini koristi se DEMO poslužiteljski certifikat *cistest.apis-it.hr*). Nakon uspješno uspostavljene TLS 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 privatnim ključem aplikativnog certifikata *fiskalcis* (u testnoj okolini koristi se DEMO aplikativni certifikat *fiskalcistest*) i šalje natrag naplatnom uređaju (ili informacijskom sustavu) obveznika.

Naplatni uređaj (ili informacijski sustav) obveznika zaprima poruku odgovora i provjerava elektronički potpis s javnim ključem aplikativnog certifikata *fiskalcis* (u testnoj okolini koristi se DEMO aplikativni certifikat *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.

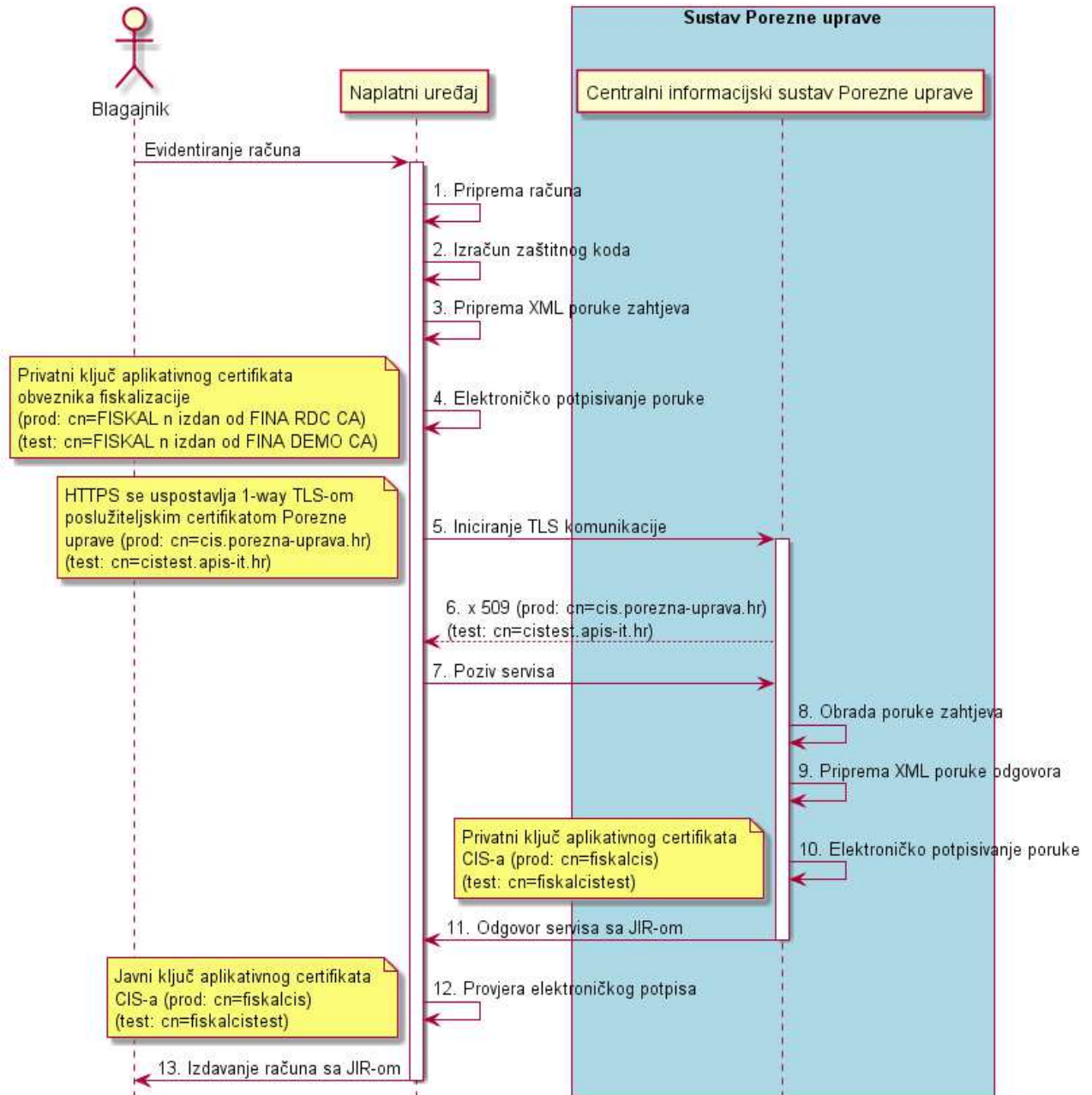
U slučaju da se prilikom obrade poruke zahtjeva dogodi greška (poruka neispravna po XML shemi, neispravan elektronički potpis i sl.) CIS vraća XML poruku odgovora koja sadrži opis greške. U tom slučaju odgovor ne sadrži JIR i operater na naplatnom uređaju (blagajnik) izdaje kupcu račun bez JIR-a. Poslovni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

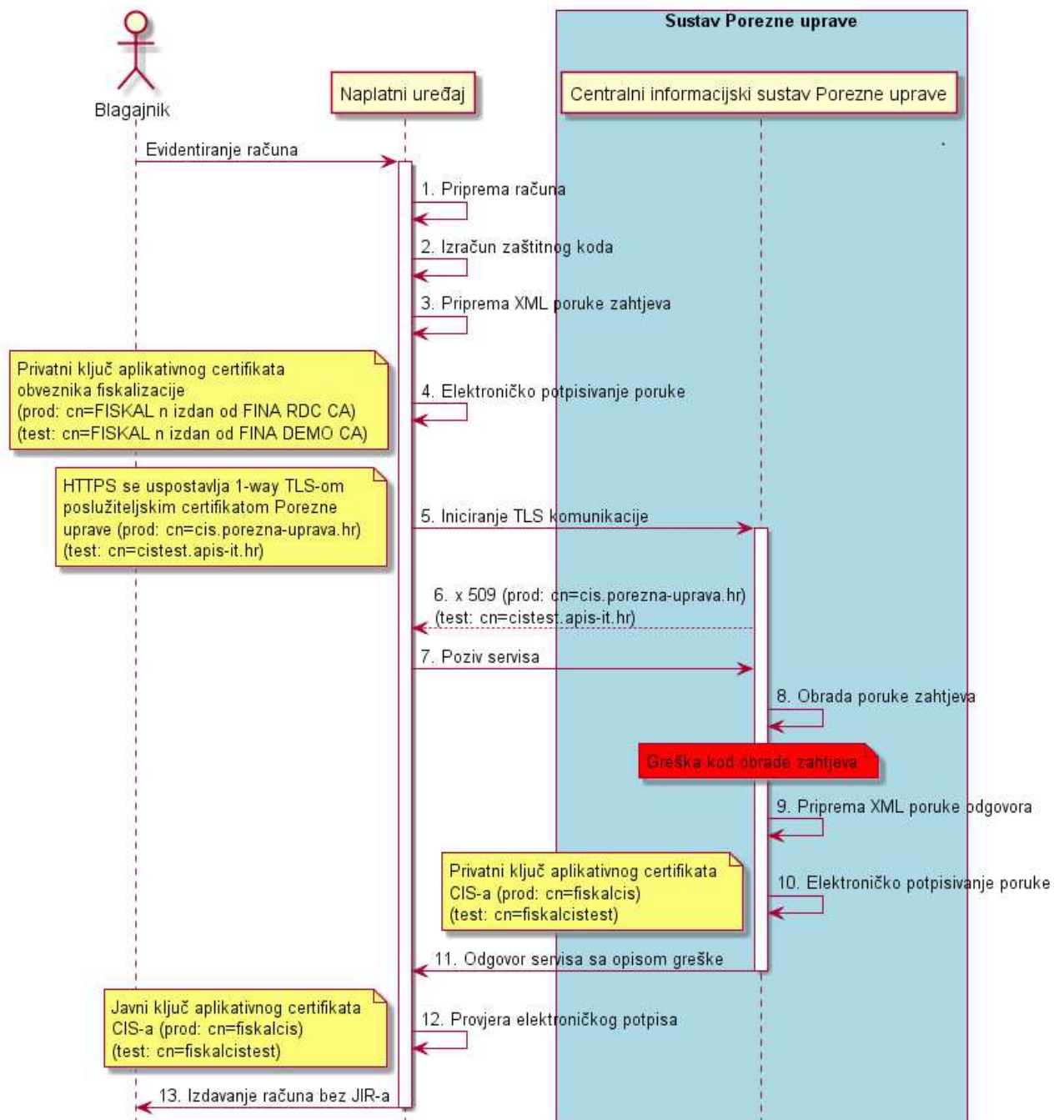
U slučajevima kad obveznik ne može dobiti JIR, npr. prekid Internet veze, i veza se ponovo uspostavi prioritet imaju poruke kojima se prijavljuju tekući računi koji se izdaju kako bi oni dobili JIR. Poruke koje nisu dobile JIR treba dostaviti naknadno u periodu manjeg opterećenja. U budućim verzijama 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.

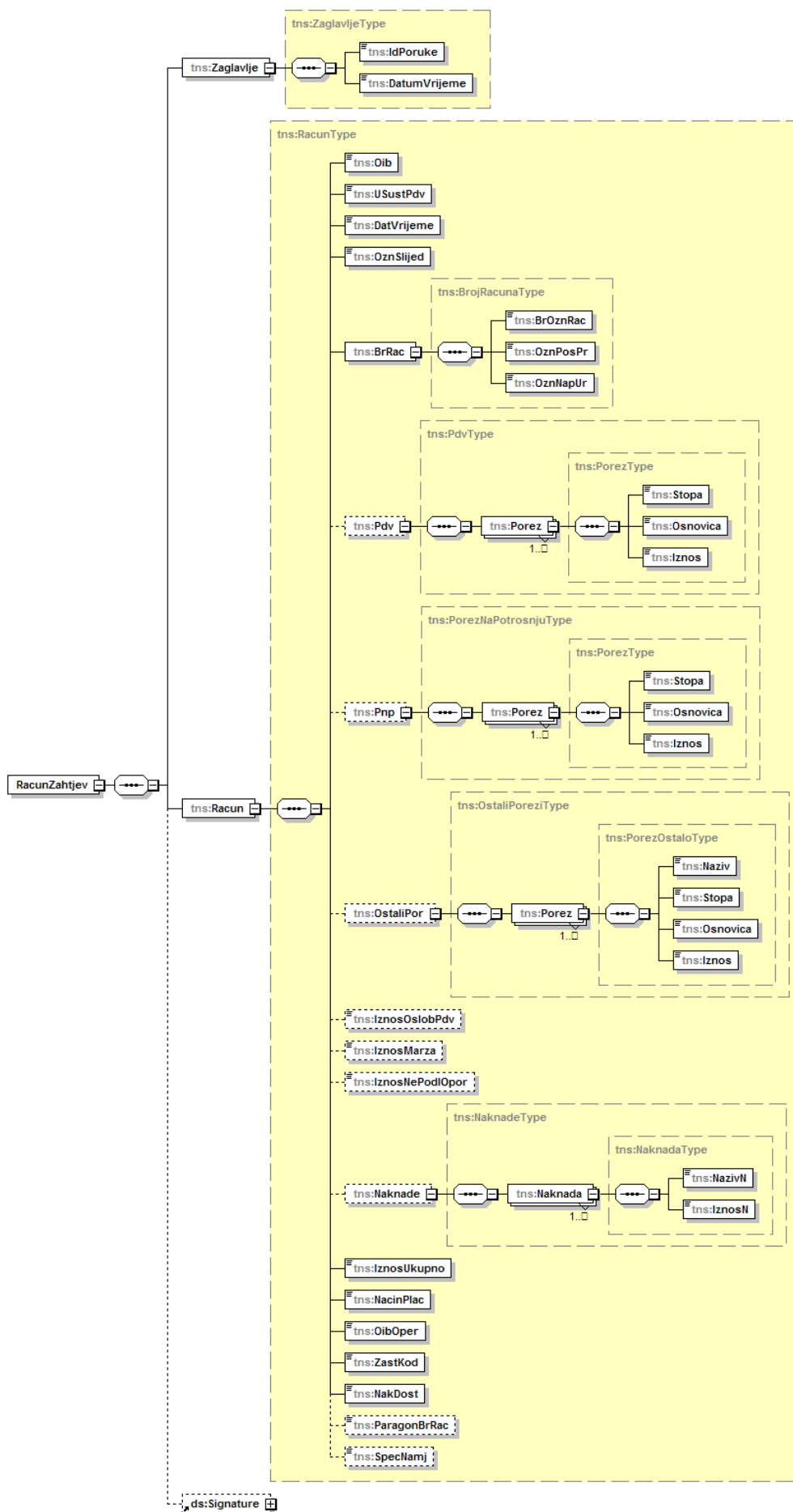
Podatak	Opis/Napomena	Obavezan DA/NE	Tip/Duljina
<b>Zaglavlje</b>			
Identifikator poruke	ID poruke (UUID). Svaka poruka koja se šalje prema CIS-u mora sadržavati različiti ID poruke. Isto vrijedi i u slučaju kad se ponavlja slanje poruke zbog greške u razmjeni poruka.	DA	Char(36)
Datum i vrijeme slanja	Datum i vrijeme slanja poruke zahtjeva. dd.mm.ggggThh:mm:ss	DA	Date & Time
<b>Račun</b>			
OIB	OIB obveznika fiskalizacije.	DA	Char(11)
U sustavu PDV	Oznaka je li obveznik u sustavu PDV-a ili nije. <i>True</i> ako je obveznik u sustavu PDV-a, u suprotnom <i>false</i> . 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.	NE	Decimal(15,2)

	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). <i>True</i> ako je riječ o naknadnoj dostavi računa, u suprotnom <i>false</i> . 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>

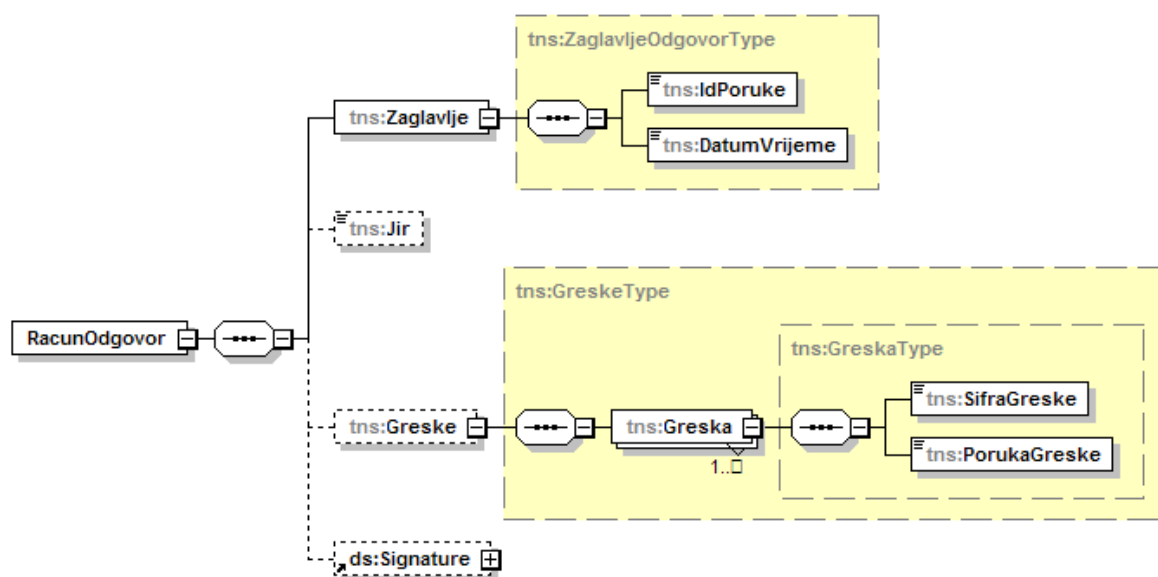
```

### 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
<b>Zaglavlje</b>			
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
<b>Jedinstveni identifikator računa</b>			
JIR	Jedinstveni identifikator računa. U slučaju greške, JIR se ne šalje u odgovoru.	NE	Char(36)
<b>Greške</b>			
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>
```

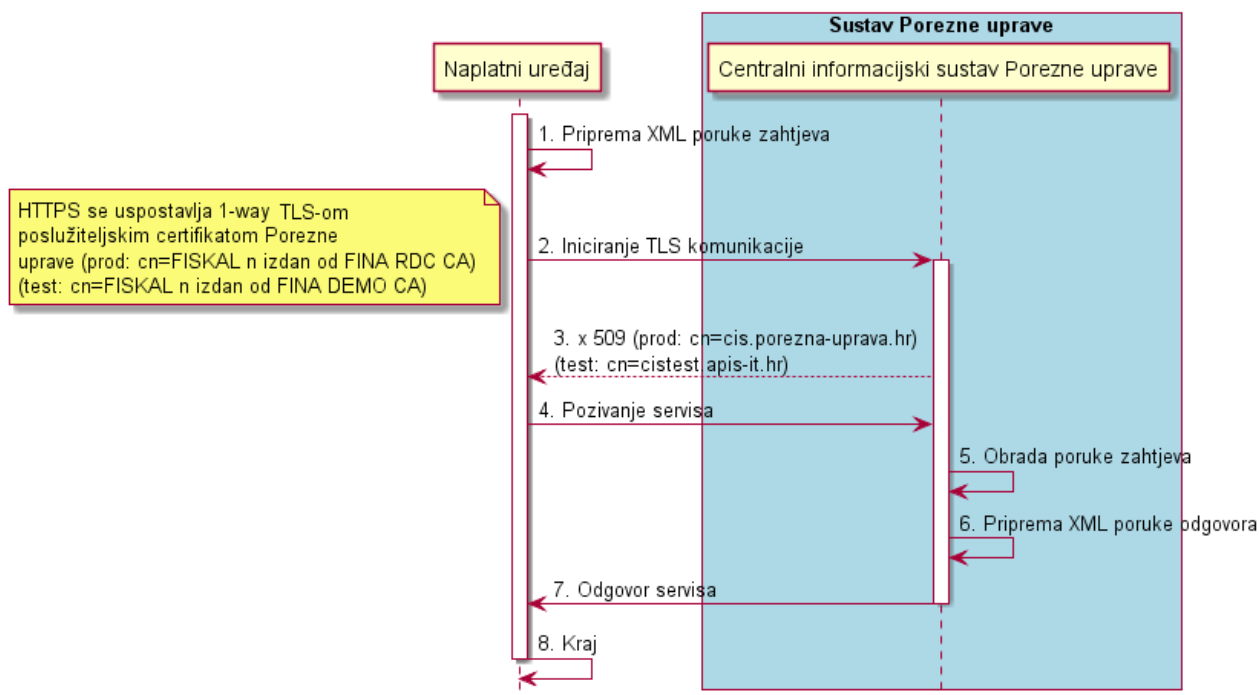
## 2.2 Echo metoda

Echo metoda je implementirana u svrhu testiranja ispravnog povezivanja s Web servisom, što indirektno uključuje uspješnu uspostavu TLS 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 (računa) biti uspješan.

Proces je prikazan slijednim dijagramom na slici 5.





Slika 5. Slijedni dijagram procesa slanja *echo* poruke

### 2.2.1 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>
```

### 2.2.2 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>
```

## 2.3 Provjera računa koji su dostavljeni u Poreznu upravu

Ova metoda je implementirana kako bi obveznik fiskalizacije/proizvođač softverskog rješenja za fiskalizaciju u testnoj okolini mogao pobliže provjeriti račune koji su dostavljeni u PU za potrebe testiranja softverskog rješenja. Provjera računa odvija se po 39 različitih pravila. Proces razmjene poruka je isti kao i u slučaju slanja računa u CIS. Ako su dostavljeni podaci o računu ispravni prema zadanim pravilima, CIS vraća odgovor sa šifrom v100 – 'Poruka je ispravna'. Ako su dostavljeni podaci o računu neispravni, CIS vraća popis grešaka prema šifarniku grešaka kod provjere računa koji se nalazi u dodatku ovog dokumenta (poglavlje 13). Poruka odgovora sadrži i originalne podatke o računu prepisane iz poruke zahtjeva.

**Napomena:** Navedena provjera računa koji su dostavljeni u PU obuhvaća provjeru po 39 različitih pravila temeljem podataka iz računa. U fazi analize zaprimljenih podataka Porezna uprava može utvrditi i druge nepravilnosti vezane za ispravnost zaprimljenih podataka od obveznika, a koje nisu pokrivena ovom provjerom.

**Metoda za provjeru računa je dostupna samo u testnoj okolini.**

### 2.3.1 Podatkovni skup zahtjeva za provjeru računa

Podatkovni skup zahtjeva za provjeru računa identičan je podatkovnom skupu za račun, koji je opisan u točki 2.1.1 ovog dokumenta.

### 2.3.2 Primjer poruke zahtjeva za provjeru računa

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

```
<tns:ProvjeraZahtjev
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>01.07.2016T12:00:00</tns:DatumVrijeme>
  </tns:Zaglavlje>
  <tns:Racun>
    <tns:Oib>98765432198</tns:Oib>
    <tns:USustPdv>true</tns:USustPdv>
    <tns:DatVrijeme>01.07.2016T12:00:14</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:ProvjeraZahtjev>

```

### 2.3.3 Podatkovni skup odgovora za provjeru računa

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

Podatak	Opis/Napomena	Obavezan DA/NE	Tip/Duljina
<b>Zaglavlje</b>			
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
<b>Račun</b>			
OIB	Prepisano iz poruke zahtjeva.	DA	Char(11)
U sustavu PDV	Prepisano iz poruke zahtjeva.	DA	Boolean
Datum i vrijeme izdavanja	Prepisano iz poruke zahtjeva.	DA	Date & Time
Oznaka slijednosti	Prepisano iz poruke zahtjeva.	DA	Char(1)
Broj računa	Prepisano iz poruke zahtjeva.	DA	
Brojčana oznaka računa	Prepisano iz poruke zahtjeva.	DA	Varchar(20)
Oznaka poslovnog prostora	Prepisano iz poruke zahtjeva.	DA	Varchar(20)
Oznaka naplatnog uređaja	Prepisano iz poruke zahtjeva.	DA	Varchar(20)
PDV	Prepisano iz poruke zahtjeva.	NE	
Porezna stopa	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(3,2)
Osnovica	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(15,2)
Iznos poreza	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(15,2)
PNP	Prepisano iz poruke zahtjeva.	NE	
Porezna stopa	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(3,2)
Osnovica	Prepisano iz poruke zahtjeva.	DA, ako	Decimal(15,2)

		postoji porez	
Iznos poreza	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(15,2)
Ostali porezi	Prepisano iz poruke zahtjeva.	NE	
Naziv poreza	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Varchar(100)
Porezna stopa	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(3,2)
Osnovica	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(15,2)
Iznos poreza	Prepisano iz poruke zahtjeva.	DA, ako postoji porez	Decimal(15,2)
Iznos oslobođenja	Prepisano iz poruke zahtjeva.	NE	Decimal(15,2)
Iznos na koji se odnosi poseban postupak oporezivanja marže	Prepisano iz poruke zahtjeva.	NE	Decimal(15,2)
Iznos koji ne podliježe oporezivanju	Prepisano iz poruke zahtjeva.	NE	Decimal(15,2)
Naknade	Prepisano iz poruke zahtjeva.	NE	
Naziv naknade	Prepisano iz poruke zahtjeva.	DA, ako postoji naknada	Varchar(100)
Iznos naknade	Prepisano iz poruke zahtjeva.	DA, ako postoji naknada	Decimal(15,2)
Ukupan iznos	Prepisano iz poruke zahtjeva.	DA	Decimal(15,2)
Način plaćanja	Prepisano iz poruke zahtjeva.	DA	Char(1)
OIB operatera na naplatnom uređaju	Prepisano iz poruke zahtjeva.	DA	Char(11)
Zaštitni kod izdavatelja	Prepisano iz poruke zahtjeva.	DA	Char(32)
Oznaka naknadne dostave računa	Prepisano iz poruke zahtjeva.	DA	Boolean
Oznaka paragon računa	Prepisano iz poruke zahtjeva.	NE	Varchar(100)
Specifična namjena	Prepisano iz poruke zahtjeva.	NE	Varchar(1000)
<b>Greške</b>			
Šifra greške	Šifra greške je u formatu vXXX gdje je XXX troznamenkasti prirodni broj, sukladno šifarniku grešaka.	DA	Varchar(4)
Poruka	Poruka greške je tekstualni opis greške sukladno šifarniku grešaka.	DA	Varchar(500)

### 2.3.4 Primjer poruke odgovora za provjeru računa

#### A. Primjer odgovora (bez grešaka u računu)

```
<tns:ProvjeraOdgovor 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>04.07.2016T12:00:35</tns:DatumVrijeme>
</tns:Zaglavlje>
<tns:Racun>
  <tns:Oib>98765432198</tns:Oib>
  <tns:USustPdv>true</tns:USustPdv>
  <tns:DatVrijeme>04.07.2016T12:00:14</tns:DatVrijeme>
  <tns:OznSlijed>P</tns:OznSlijed>
  <tns:BrRac>
    <tns:BrOznRac>12</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: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:IznosOslobPdv>12.00</tns:IznosOslobPdv>
  <tns:Naknade>
    <tns:Naknada>
      <tns:NazivN>Povratna naknada</tns:NazivN>
      <tns:IznosN>1.00</tns:IznosN>
    </tns:Naknada>
  </tns:Naknade>
  <tns:IznosUkupno>25.80</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:Racun>
<tns:Greske>
  <tns:Greska>
    <tns:SifraGreske>v100</tns:SifraGreske>
    <tns:PorukaGreske>Poruka je ispravna.</tns:PorukaGreske>
  </tns:Greska>
</tns:Greske>
</tns:ProvjeraOdgovor>

```

## B. Primjer odgovora (s greškama u računu)

```

<tns:ProvjeraOdgovor 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>01.07.2016T21:10:34</tns:DatumVrijeme>
  </tns:Zaglavlje>
  <tns:Racun>
    <tns:Oib>98765432198</tns:Oib>
    <tns:USustPdv>true</tns:USustPdv>
    <tns:DatVrijeme>01.07.2016T12:00:14</tns:DatVrijeme>

```

```

<tns:OznSlijed>P</tns:OznSlijed>
<tns:BrRac>
  <tns:BrOznRac>12</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: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:IznosOslobPdv>12.00</tns:IznosOslobPdv>
<tns:Naknade>
  <tns:Naknada>
    <tns:NazivN>Povratna naknada</tns:NazivN>
    <tns:IznosN>1.00</tns:IznosN>
  </tns:Naknada>
</tns:Naknade>
<tns:IznosUkupno>25.80</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:Greske>
  <tns:Greska>
    <tns:SifraGreske>v106</tns:SifraGreske>
  </tns:Greska>
  <tns:Greska>
    <tns:SifraGreske>v141</tns:SifraGreske>
    <tns:PorukaGreske>Polje "Specifična namjena" nije prazno. </tns:PorukaGreske>
  </tns:Greska>
</tns:Greske>
</tns:ProvjeraOdgovor>

```

## 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. Produkcijaska
2. Testna

Uvjeti spajanja su slični, a razlikuju se u različitim adresama pristupnih točaka i certifikatima. U produkcijskoj okolini koriste se certifikati izdani od FINA RDC CA, a u testnoj okolini certifikati izdani od FINA DEMO CA. Funkcionalno se okoline neće razlikovati (osim kod razvoja novih funkcionalnosti), samo što će se u testnoj okolini koristiti testni podaci.

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

#### 3.1 Mrežni preduvjeti i preporuke

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

<b>Vrsta mreže</b>	Internet
<b>Preporučeni otvoreni TCP portovi prema CIS sustavu</b>	8449

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

<b>Karakteristike linka</b>	Stalni simetrični link
<b>Propusnost</b>	min. 2 Mb/s (do 40 poruka/sec vršnog opterećenja, uz pretpostavku da je veličina poruke 6KB)

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

#### 3.2 Sigurnosni preduvjeti

Sva komunikacija s CIS-om Porezne uprave zaštićena je 1-way TLS enkripcijom na transportnom sloju. U produkcijskoj okolini se CIS Porezne uprave predstavlja klijentu TLS certifikatom izdanim od FINA RDC CA, a u testnoj okolini TLS certifikatom izdanim od FINA DEMO CA (<http://www.fina.hr/finadigicert>).

<b>Zaštita na transportnom sloju</b>	HTTPS (TLS v1.1 i v1.2, minimalno AES_256 enkripcija)
<b>Certifikati za elektroničko potpisivanje izdani od FINA RDC CA za produkcijsku i od FINA DEMO CA za testnu okolinu</b>	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:

<b>Standardi kreiranja klijenta</b>	WS-I
-------------------------------------	------



<b>Tip servisa</b>	document-literal
<b>Aplikacijski protokol</b>	SOAP/HTTPS (SOAP 1.1)
<b>Kodna stranica XML poruke zahtjeva</b>	UTF-8

## 4. Topologija pristupa CIS-u Porezne uprave

Korisnici pristupaju CIS-u Porezne uprave iniciranjem 1-way TLS veze. Koristeći TLS 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. Format i poruka zahtjeva i odgovora specificirani su kroz XML shemu.

### CIS pristupna točka

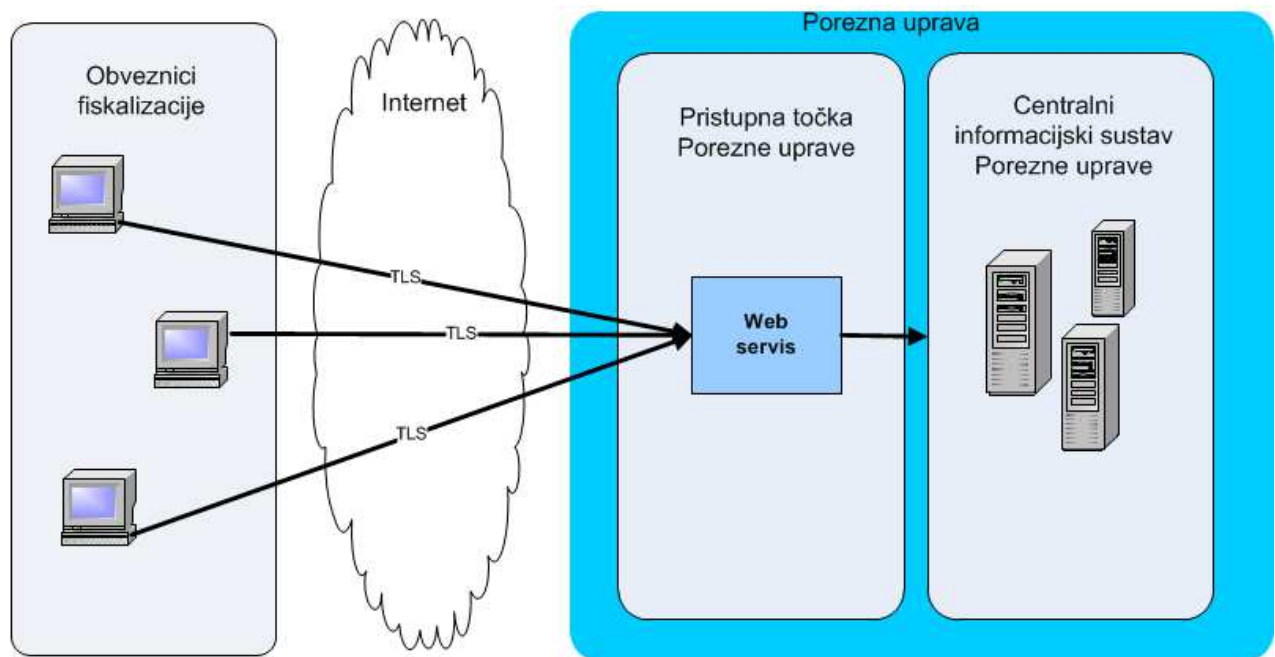
Implementacija i održavanje pristupne točke je zadaća APIS IT-a. APIS IT će klijentima omogućiti spajanje na pristupnu točku i to u dvije okoline: produkcijskoj i testnoj.

### 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 6, nije predviđen razvoj „posredničke komponente“. Razvoj hardversko-softverskog rješenja je u domeni klijenta. Klijent je također dužan osigurati Internet vezu prema CIS pristupnoj točki s potrebnom propusnošću. Odabir platforme i implementacija softverskog rješenja je u domeni klijenta i takve informacije nije potrebno dojaviti APIS IT-u.



Slika 6. 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 TLS s poslužiteljskim certifikatom Porezne uprave za terminaciju TLS-a u kojem se poslužitelj Porezne uprave predstavlja klijentima.

U produkcijskoj okolini će se kao Certificate Authority koristiti usluge FINA RDC CA, a u testnoj okolini 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 RDC CA u produkcijskoj okolini, odnosno FINA DEMO CA u testnoj okolini. Nije dozvoljeno slanje poruka u testnoj okolini potpisanih produkcijskim certifikatom i obrnuto.

Za povezivanje se koristi 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 produkcijsku okolinu moraju imati izdan certifikat od FINA RDC CA. Klijentski sustavi za testnu okolinu moraju imati izdan certifikat od FINA DEMO CA (<http://www.fina.hr/finadigicert>).

Uporaba certifikata na strani CIS pristupne točke Porezne uprave je:

- uspostava TLS veze prema CIS-u Porezne uprave
- elektroničko potpisivanje poruka

Certifikati koje koristi CIS pristupna točka Porezne uprave po okolinama imaju sljedeće nazive:

1. Produkcijska
  - Poslužiteljski: **cis.porezna-uprava.hr**
  - Aplikacijski: **fiskalcis**
2. Testna
  - Poslužiteljski: **cistest.apis-it.hr**
  - Aplikacijski: **fiskalcistest**

Detalji FINA PKI sustava su dostupni na web stranicama FINA-e:  
<http://www.fina.hr/Default.aspx?sec=1799>.

### Postupak preuzimanja CIS certifikata/javnih ključeva

Postupak izdavanja i preuzimanja certifikata potrebnih za pristup CIS-u Porezne uprave je dostupan na web stranicama FINA-e: <http://www.fina.hr/Default.aspx?sec=1541>.

---

## 6. Postupak spajanja obveznika fiskalizacije na CIS Porezne uprave

1. Nabaviti minimalno jedan aplikativni digitalni certifikat za fiskalizaciju od FINA RDC CA za produkcijsku okolinu, odnosno FINA DEMO CA za testnu okolinu. Broj ukupno izdanih aplikativnih digitalnih certifikata za fiskalizaciju ovisi o obvezniku fiskalizacije i potrebi. Postupak je opisan u poglavlju 11.
2. Nakon što FINA izda potrebne certifikate, obveznik fiskalizacije ih implementira u svoju okolinu.
3. Preuzeti CIS certifikate/javne ključeve od FINA RDC CA za produkcijsku okolinu, odnosno FINA DEMO CA za testnu okolinu. Postupak je opisan na web stranici FINA-e.
4. Preporuča se minimalno dva dana neprekidnog i stabilnog rada u testnoj okolini prije prelaska u produkcijsku okolinu.  
U slučaju kad informatička tvrtka izrađuje aplikacije za više krajnjih obveznika fiskalizacije, također se preporuča testiranje aplikacije i na lokaciji obveznika minimalno dva dana u testnoj okolini. U tom slučaju obveznik fiskalizacije ne mora nabaviti DEMO certifikat, već informatička tvrtka može koristiti svoj DEMO certifikat.

### 6.1 Url adrese za spajanje na CIS Porezne uprave

#### 1. TEST

<b>Okolina:</b>	TEST
<b>Servis:</b>	Prihvat podataka o računima (FiskalizacijaServiceTest)
<b>URL:</b>	<a href="https://cistest.apis-it.hr:8449/FiskalizacijaServiceTest">https://cistest.apis-it.hr:8449/FiskalizacijaServiceTest</a>

#### 2. PRODUKCIJA

<b>Okolina:</b>	PRODUKCIJA
<b>Servis:</b>	Prihvat podataka o računima (FiskalizacijaService)
<b>URL:</b>	<a href="https://cis.porezna-uprava.hr:8449/FiskalizacijaService">https://cis.porezna-uprava.hr:8449/FiskalizacijaService</a>

**Servis je stalno dostupan za testiranje u testnoj okolini, osim u servisnim intervalima navedenim u nastavku:**

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

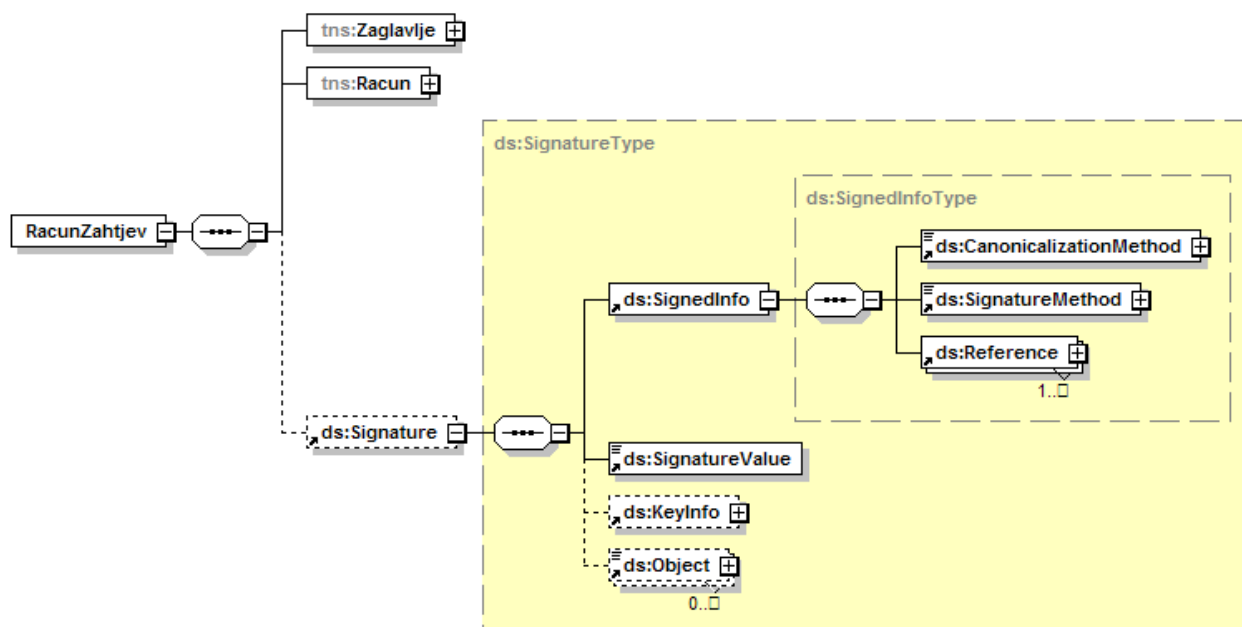
## 7. Elektronički potpis poruke zahtjeva

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 uz elektroničko potpisivanje sadržane su u elementu <Signature> čija struktura je propisana shemom

<http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/xmlsig-core-schema.xsd> i definirane su unutar <http://www.w3.org/2000/09/xmlsig#> namespace URI-ja definiranog kroz W3C preporuku "XML Signature Syntax and Processing" (*xmlsig-core*), prikazano na slici 7.



Slika 7. Shema <Signature> elementa

U nastavku je primjer elektronički potpisane poruke zahtjeva DEMO certifikatom iz 2012. godine u testnoj okolini:

```
<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/xmlsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmlsig#rsa-sha1" />
      <Reference URI="#RacunZahtjev">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmlsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
      </Reference>
    </SignedInfo>
    <SignatureValue>
      ...
    </SignatureValue>
    <KeyInfo>
      ...
    </KeyInfo>
    <Object>
      ...
    </Object>
  </Signature>
</RacunZahtjev>
```

```

    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>VltfxY/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 kanonikalizaciji i metodi potpisivanja. Potpisi su kanonikalizirani i metoda potpisivanja je uvijek RSA-SHA1, što se vidi kroz elemente <CanonicalizationMethod> i <SignatureMethod> koji imaju fiksni sadržaj:

Kanonikalizacijska metoda koja se koristi prilikom potpisa poruke zahtjeva 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" />
```

(Napomena: U poruci odgovora koju vraća CIS uvijek će se koristiti kanonikalizacijska metoda

```
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>)
```

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 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 definirana 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 na putu 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, pretežno 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; a 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 asimetričnog 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 osnovni kanonikalizacijski algoritam obrađuje namespace deklaracije. Često se potpisani XML dokument nalazi unutar nekog drugog XML dokumenta, što je i naš slučaj. Osnovna kanonikalizacijska metoda tada neće dati identične rezultate pa je potrebno 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 identifikator 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 razumnom dozom sigurnosti da nitko nenamjerno neće kreirati isti identifikator. Shodno tome, podaci označeni UUID-om mogu 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 - nasumično generiran broj
5. verzija - generiran izračunom SHA-1 hash-a iz podataka istih kao u verziji 3.

---

## 9. Primjeri poruka

U nastavku su dani primjeri poruka u izvornom obliku i s elektroničkim potpisom. Svi primjeri poruka odnose se na testnu okolinu i poruke su potpisane DEMO certifikatom. Poruke potpisane produkcijskim certifikatom imaju identičnu strukturu, s razlikom u izdavatelju certifikata.

Napomena: Podaci u primjerima su testni i ne moraju biti poslovno ispravni ili logični. Također, izdavatelji certifikata (FINA RDC i FINA DEMO) se tokom vremena mogu (i od prve verzije ovog dokumenta jesu) promijeniti, što će biti reflektirano u sadržaju elementa <X509IssuerName>.

### 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:Racun>
    </tns:RacunZahtjev>
  </soapenv:Body>
</soapenv:Envelope>

```

```

</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+dX6VurJmL52Ob7FDNNH8U3Nltxlo7fUvU1ra6HPSyCd4H3O
QEvZlb3xv1yqvLGYr0M5yzVGbu9o4IXG3qITTVtEWu1MCC7OYeyltnKwr9/QRAbFrA3QWZu/F8qnc4dKg6o
hl8X8hZLLh2wIzNxtOrzbtJO6lZciCyfptR6u1vwwmUxIlo7lSCTLXw/UC9LqC86C5HBbQU+QT1i9rTsUdYZZ0
kTel4Z/ZPkYO+OqZmpiKdSbwlwwqtp7CrQ0WK2RSd+x+XUf2GF3Ydld90Tx9QYRps/Z
P0OME3jnSpKJlKRTB8ev9rM+KYYEGbSR1rz6g==

```

```

</SignatureValue>
  <KeyInfo>
    <X509Data>

```

```

<X509Certificate>MIIEyDCCA7CgAwIBAgIEPssQ2TANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJl
UjENMAAsGA1UEChMERkiOQTENMAAsGA1UECxMEREVNTzAeFw0xMjM0MjM0MDQ5MDUwNDA5Mjc
xMTE5MThaMFkxZzA5BjBGNVBAZTAkxSMYSyWJAYDVQQKEwE1BUEITIEIUICBELk8uTy4gSF1wMjk5NDY1M
DE5OTEPMMA0GA1UEBxMGWkFHUKVCMREwDwYDVQQDEwhGSVNLQUwgMjCCASlWdQYJKoZIhvcNA
QEBBQADggEPADCCAQoCggEBAOEPIO7AMxdO5o6jw5BUy2UAKXdtYaviEtVPVRwoBxA4YxPzDFjsN
GapAH4DW7YKqgLLLT6EjrKkCvjOpgr5LsPUjZk7/gZrVNpcBlzm6ECiywBGjB623/kdWqYdd9AI+1KbOVa+

```

```

PRp9D7JzjLQTZaXTc4FR5wGo4w9jC22ixqb+F6aDzF6TLsICJVKFWV4g6gIMLIKgsrZxk+O55/1f7o0442dC
GuZ7IQtp1UK7TH9a7KilvLNv+1OKyZDZfzYGyPvKb/Tt7N5NO0R1ICbeATvDcDyl2BQfECYC+z+3dfDybcO
FF+QmBsntIKO4p7+LxR/Yob5/GxPrli6KVyDdECAwEAAaOCaCQwggHAMAsGA1UdDwQEAwIFoDBCBgN
VHSAEOzA5MDcGCSt8iFAFHwUDATAqMCgGCCsGAQUFBwIBFhxodHRwOi8vZGVtby1wa2kuZmluYS5o
ci9jcHMvMCMQGA1UdEQQdMBuBGXNhbMRYYS5wb3BvdmljQGFWaXMtaXQuaHlwgc4GA1UdHwSBxjCBw
zBCoECgPqQ8MDoxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1P
MQ0wCwYDVQQDEwRDUkw3MH2ge6B5hk9sZGFwOi8vZGVtby1sZGFwLmZpbmEuaHlwZ3U9REVNTyxv
PUZJTkEsYz11Uj9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0JTNCYmluYXJ5J5hiZodHRwOi8vZGVtby1wa2
kuZmluYS5oci9jcmwvZGVtb2NhLmNybdArBgNVHRAEJDAigA8yMDEyMDkyNzEwNDkxOFqBDzlwMTQw
OTI3MTEExOTE4WjAFBgNVHSMEGDAWgBR6YCOOSJ0ya6TILd24WbSU/EJinjAdBgNVHQ4EFgQUK/IWm
nKEKdD/PLV06CddkYi7WrAwCQYDVR0TBAlwADANBgkqhkiG9w0BAQUFAAOCAQEAABb3RnPlwEBNK
EWy3YsFRwJSZoMTBGwv7Q0sWf9nTHMS3vgFqNUSx8iqP99tnoppav7TdWoQ5zBtW935Nkev7rhqGADT
4R/7pYeYc2R+Yjsbn6rxo6zDv/olrd8LtfHccx3iUYgt/n1J5QiGIQ601fXwYftuaVcaMnwsVBCuFy8vut4PiSPVs
fMLR/oLQ3IqKJmNMXY4Rm8qjeOdgLyYwTuz7oKZ+N4+kq4tpuuJn86EUK3qsQo+FOVfWi7cew7qtDYHap
qAC4zTb6isqB8/Wcagucb4zNU3Vgeixz5Nsd
8g28hcC/OzhHHGZpQvB0WVF5YIF1Od7AYBL+DDI9Lg==</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>P5bla6dPJdlvov/pmmJvML7nMep7Xea4+LiWHEJEfsOz3SSKG4wwuVdGM+7k+CGt799
    No4r1KKulaRRPMQW/vh0qtAm/0V/o45clpgYB1YFUZdCsNktasYh4gkD/RQiF8ph/86W8zmY4fdLrqb45P17
    6e/DVcWJkduHeF2t4afUyJANti8czeimMB1ulaHvZwSMlvDKCN93tXoSlwGX3CXDg8kTRzpDC1x3r1aboaR
    rLpkgzSZFrnMe4aBCqFnOpZjcXZa321hK3shl0PSij52IN1KWuMP9ekldj+XVNGQa/Ecj8RjuFDKwgoyhxpB9
    WZ/jGa81QAQ0DQsckMkF6g==</SignatureValue>

    <KeyInfo>
      <X509Data>

        <X509Certificate>MIIExDCCA6ygAwIBAgIEPssQcTANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJl
        UjENMAsGA1UEChMERklOQTENMAsGA1UECXMEREVNTzAeFw0xMjA5MjYwODExNDIaFw0xNDA5MjY
        wODQxNDIaMHgxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1PM
        REwDwYDVQQLEwhQb3Ns3ZuaTEgMB4GA1UECxMXQVBJUyBjVjCBELk8uTy4gODA1NDEzNzIxZjAU
        BgNVBAMTDWZpc2thbGNpc3Rlc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC81TtKtJ
        84emCS/HK7gSovjNdluZWB0DbIMq3cBFpOpmurcbDCJ1Z17XiPLa+UWYlqyAjHqYDnG/H4c5EeGoli9swz
        5QcZFBmyXTPsd3GuMR0gUAd4bcvbw1/HDONE5cE8PL11Gly8gi5ANZkujalYmx+1ImnhHxx1Bh2UJ/bcl2
        eXPtieBQBwtCIATSzseB5FFz8LcSyfz8LcSyfz8LcSyfz8LcSyfz8LcSyfz8LcSyfz8LcSyfz8LcSyfz8Lc
        cUE5d0nSZ7hfEkW8xlCgs1Ly6Vu3w7Z5M8vb4QmoPnIT1EaHCXiweuK6vjkUk8RQmYY4ITFBs8zHiG7h4n
        9bPAgMBAAGjggGhMIIBnTAOBgNVHQ8BAf8EBAMCBAwAwQgYDVR0gBDswOTA3BgkrfhQBR8FBAIwKjA
        oBggrBgEFBQcCARYcaHR0cDovL2RlbW8tcGtpLmZpbmEuaHlVY3BzLzCBZgYDVR0fBIHGMIHDMEKqQK
        A+pDwwOjELMAkGA1UEBhMCSFIxDTALBgNVBAoTBEZJTkExDTALBgNVBAsTBBERFTU8xDTALBgNVB
        AMTBENSTDCwfaB7oHmGT2xkYXA6Ly9kZW1vLWxkYXAUZmluYS5oci9vdT1ERU1PLG89RkIOQsXjPUhS
        P2NlcnRpZmlyYXRlUmV2b2NhdGlvbkxpc3QIM0JiaW5hcnmGJmh0dHA6Ly9kZW1vLXBras5maW5hLmhyL
        2NybC9kZW1vY2EuY3JsMCA1UdEAQkMCKADzlwMTIwOTI2MDgxMTQ5W0oEPMjAxNDA5MjYwODQx
        NDlaMB8GA1UdIwQYMBaAFHpgl45lnTJrpOUt3bhZtJT8QmKeMB0GA1UdDgQWBRRglJsZevSn6kDuSzC
        hmaa9Sqr6sjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBAQUAA4IBAQC05kJWanJgS+UG7XQHsHersDFk
        4K5W/Y2Ppubary0j3lwJrveHbUR3HObo0KiVenF6+1FL3sCI/2tfH3wSszWL8Gkit8jUudTo5vDyLqEUXYDHIF
        UBwseudsPkUxPiQ6HuuF3PiUAWf00chXD38eTjapNu6VeQt4EORSO+rEXdhWihVb5HxFIVPTkqHmq1KI
        NwtV9+thwE3hNMwacRa4gwTB1O+jadVIJQMq+kgwnLGLBcwr0W+x1ye6MPSYEUxSNFGHPG/evP9DRL
        wJtR3ngvlCDusnO+A75Nn40VYcoljw6EN1V+plK+HkLye0zzLsnHIWTSgFz2sQVG5xCURil</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 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>

```

## 9.6 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>OJnC52ayKIHRehSLYOvIJ273u/dR5qqG/4L2WVaAMylJexQ0fDJFyQpAovQqqCMxljLT4
b0pj4OQis93LI4a/v5+2b+taOcM//0kylolJkm9wldC+zyo9AqrB3YdPdSiHPWY7jGtNKYPRg/5SEvYIGDFQC
sD5CLa4eJHDp6hl+DN6gnDICC5q84YTO8Xxa3valkt+3mSi6DaDhbmY0Dq41+MTzie8bdRmTf+Ar8FqiBst8
2+2TGdVdWrtjtL2lWATR669022Pd9aAJe9W8UZoDpBng6JVSsNH+WViQb1IBNoKfxyESgeLY0fC97f726UI
Y5J+H8ISedcYEnWb5HDw==</SignatureValue><KeyInfo>
        <X509Data>

```



```

<X509Certificate>MIIExDCCA6ygAwIBAgIEPssQcTANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJl
UjENMAAsGA1UEChMERkiOQTENMAAsGA1UECXMEREVNTzAeFw0xMjA5MjYwODExNDIaFw0xNDA5MjY
wODQxNDIaMHgxGzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1PM
REwDwYDVQQLEwhQb3Nsb3ZuaTEgMB4GA1UECxMXQVBJUyBjVCBELk8uTy4gODA1NDEzNzIxZjAU
BgNVBAMTDWZpc2thbGNpc3Rlc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC81TtKtJ
84emCS/HK7gSovjNdluZWB0DbIMq3cBFpOpmurcbDCJ1Z17XiPLa+UWYlqyAjHQyDnG/H4c5EeGoli9swz
5QcZFBmyXTpSd3GuMROgUAd4bcvbw1/HDONE5cE8PL11Gly8gi5ANZkujalYmx+1ImnhHxx1Bh2UJ/bcl2
eXPtieBQBwtCIATSzseB5FFz8LcSyfzM7h39PsAlZ0p8YzH7W+307gvgrJHYb/n4ADwixieHqb5j74DVD0rUP
cUE5d0nSZ7hfEkW8xlCgs1Ly6Vu3w7Z5M8vb4QmoPnlT1EaHCXiweuK6vjKuk8RQmYY4ITFBs8zHiG7h4n
9bPAgMBAAGjggGhMIIBnTAOBgNVHQ8BAf8EBAMCBaAwQgYDVR0gBDswOTA3BgkrlhQBR8FBAIwKJA
oBggRBgEFBQCARYcaHR0cDovL2RibW8tcGtpLmZpbmEuaHlvY3BzLzCBzgYDVR0fBIHGMIHDMEKqK
A+pDwwOjELMAkGA1UEBhMCSFIxDTALBgNVBAoTBEZJTkExDTALBgNVBAsTBERTU8xDTALBgNVB
AMTBENSTDCwfaB7oHmGT2xkYXA6Ly9kZW1vLWxkYXAuZmluYS5oci9vdT1ERU1PLG89RkIOQsXjPUHs
P2NlcnRpZmlyYXRlUmV2b2NhdGlvbkxpc3QIM0JiaW5hcnmGJmh0dHA6Ly9kZW1vLXBraS5maW5hLmhyL
2NybC9kZW1vY2EuY3JsMCA1UdEAQkMCKADzlwMTIwOTI2MDgxMTQ5W0EPMjAxNDA5MjYwODQx
NDIaMB8GA1UdIwQYMBaAFHpgl45lnTJrpOUt3bhZtJT8QmKeMB0GA1UdDgQWBRRglJsZevSn6kDuSzc
hmaa9Sqr6sjaJBgNVHRMEAjAAMA0GCSqGSIb3DQEBAQUAA4IBAQC05kJWaNjgS+UG7XQHsHersDFk
4K5W/Y2Pbubary0j3lwJrveHbUR3HOOb0KiVenF6+1FL3sCI/2tfH3wSszWL8Gkit8jUudTo5vDyLqEUXYDHIF
UBwseudsPkUxPiQ6HuuFd3PiUAWf00chXD38eTjfpNu6VeQt4EORSO+rEXdhWihVb5HxFIVPTkqHmq1KI
NwtV9+thwE3hNMwacRa4gwTB1O+jadVIJQMq+kgwnLGLBcwr0W+x1ye6MPSYEUXSNFGHPG/evP9DRL
wJtR3ngvlCDusnO+A75Nn40VYcoljw6EN1V+plK+HkLye0zzLsnHIWTSgfZ2sQVG5xCURil</X509Certificat
e><X509IssuerSerial>
      <X509IssuerName>OU=DEMO, O=FINA,
C=HR</X509IssuerName><X509SerialNumber>1053495409</X509SerialNumber>
    </X509IssuerSerial></X509Data>
  </KeyInfo>
</Signature>
</tns:RacunOdgovor></soap:Body>
</soap:Envelope>

```

## 9.7 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>

```

## 9.8 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>

```

## 9.9 Poruka zahtjeva za provjeru računa 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:ProvjeraZahtjev 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:ProvjeraZahtjev>
    </tns:Body>
  </tns:Envelope>

```

```

    <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:ProvjeraZahtjev>
</soapenv:Body>
</soapenv:Envelope>

```

## 9.10 Poruka zahtjeva za provjeru računa 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:ProvjeraZahtjev 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:Racun>
    </tns:ProvjeraZahtjev>
  </soapenv:Body>
</soapenv:Envelope>

```



```

8g28hcC/OzhHHGZpQvB0WVF5YIF1Od7AYBL+DDI9Lg==</X509Certificate>
  <X509IssuerSerial>
    <X509IssuerName>OU=DEMO,O=FINA,C=HR</X509IssuerName>
    <X509SerialNumber>1053495513</X509SerialNumber>
  </X509IssuerSerial>
</X509Data>
</KeyInfo>
</Signature>
</tns:ProvjeraZahtjev>
</soapenv:Body>
</soapenv:Envelope>

```

## 9.11 Poruka odgovora za provjeru računa 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:ProvjeraOdgovor
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>04.07.2016T21:10:38</tns:DatumVrijeme>
      </tns:Zaglavlje>
      <tns:Racun>
        <tns:Oib>98765432198</tns:Oib>
        <tns:USustPdv>true</tns:USustPdv>
        <tns:DatVrijeme>04.07.2016T12:00:14</tns:DatVrijeme>
        <tns:OznSlijed>P</tns:OznSlijed>
        <tns:BrRac>
          <tns:BrOznRac>12</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: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:IznosOslobPdv>12.00</tns:IznosOslobPdv>
        <tns:Naknade>
          <tns:Naknada>
            <tns:NazivN>Povratna naknada</tns:NazivN>
            <tns:IznosN>1.00</tns:IznosN>
          </tns:Naknada>
        </tns:Naknade>
        <tns:IznosUkupno>25.80</tns:IznosUkupno>
        <tns:NacinPlac>K</tns:NacinPlac>
        <tns:OibOper>01234567890</tns:OibOper>
        <tns:ZastKod>e4d909c290d0fb1ca068ffaddf22cbd0</tns:ZastKod>
        <tns:NakDost>false</tns:NakDost>
      </tns:Racun>
    </tns:ProvjeraOdgovor>
  </soap:Body>
</soap:Envelope>

```

```

    <tns:ParagonBrRac>123/458/5</tns:ParagonBrRac>
    <tns:SpecNamj></tns:SpecNamj>
  </tns:Racun>
  <tns:Greske>
    <tns:Greska>
      <tns:SifraGreske>v100</tns:SifraGreske>
      <tns:PorukaGreske>Poruka je ispravna.</tns:PorukaGreske>
    </tns:Greska>
  </tns:Greske>
</tns:ProvjeraOdgovor>
</soap:Body>
</soap:Envelope>

```

## 9.12 Poruka odgovora za provjeru računa 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:ProvjeraOdgovor 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>04.07.2016T21:10:38</tns:DatumVrijeme>
      </tns:Zaglavlje>
      <tns:Racun>
        <tns:Oib>98765432198</tns:Oib>
        <tns:USustPdv>true</tns:USustPdv>
        <tns:DatVrijeme>04.07.2016T12:00:14</tns:DatVrijeme>
        <tns:OznSlijed>P</tns:OznSlijed>
        <tns:BrRac>
          <tns:BrOznRac>12</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: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:IznosOslobPdv>12.00</tns:IznosOslobPdv>
        <tns:Naknade>
          <tns:Naknada>
            <tns:NazivN>Povratna naknada</tns:NazivN>
            <tns:IznosN>1.00</tns:IznosN>
          </tns:Naknada>
        </tns:Naknade>
        <tns:IznosUkupno>25.80</tns:IznosUkupno>
        <tns:NacinPlac>K</tns:NacinPlac>
      </tns:ProvjeraOdgovor>
    </soap:Body>
  </soap:Envelope>

```

```

<tns:OibOper>01234567890</tns:OibOper>
<tns:ZastKod>e4d909c290d0fb1ca068ffaddf22cbd0</tns:ZastKod>
<tns:NakDost>false</tns:NakDost>
<tns:ParagonBrRac>123/458/5</tns:ParagonBrRac>
</tns:Racun>
<tns:Greske>
  <tns:Greska>
    <tns:SifraGreske>v100</tns:SifraGreske>
    <tns:PorukaGreske>Poruka je ispravna.</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="#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>P5bla6dPJdlvov/pmmJvML7nMep7Xea4+LiWHEJEfsOz3SSKG4wwuVdGM+7k+CGt799
No4r1KKulaRRPMQW/vh0qtAm/0V/o45clpgYB1YFUZdCsNktasYh4gkD/RQIF8ph/86W8zmY4fdLrqb45P17
6e/DVcWJkduHeF2t4afUyJANti8czeimMB1ulaHvZwSMlVDKCN93tXoSlwGX3CXDg8kTRzpDC1x3r1aboar
rLpkgzSZFrnMe4aBCqFnOpZjcXZa321hK3shl0PSij52IN1KWuMPP9ekldj+XVNGQa/Ecj8RjuFDKwgoyhxpB9
WZjGa81QAQ0DQsckMkF6g==</SignatureValue>

```

```

  <KeyInfo>
    <X509Data>

```

```

<X509Certificate>MIIExDCCA6ygAwIBAgIEPssQcTANBgkqhkiG9w0BAQUFADArMQswCQYDVQQGEwJI
UjENMAAsGA1UEChMERkiOQTENMAAsGA1UECXMEREVENTzAeFw0xMjA5MjYwODExNDIaFw0xNDU5MjY
wODQxNDIaMHgxCzAJBgNVBAYTAkhSMQ0wCwYDVQQKEwRGSU5BMQ0wCwYDVQQLEwRERU1PM
REwDwYDVQQLEwhQb3Ns3ZuaTEgMB4GA1UECxMXQVBJUyBJVCBELk8uTy4gODA1NDEzNzIxZjAU
BgNVBAMTDWZpc2thbGNpc3Rlc3QwgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC81TtKtJ
84emCS/HK7gSovjNdluZWB0DbIMq3cBFpOpmurcbDCJ1Z17XiPLa+UWYlqyAjHQyDnG/H4c5EeGoli9swz
5QcZFBmyXTpSd3GuMROgUAd4bcvbw1/HDONE5cE8PL11Gly8gi5ANZkujalYmx+1ImnhHxx1Bh2UJ/bcl2
eXPtieBQBwtCIATSzseB5FFz8LcSyfzM7h39PsAlZ0p8YzH7W+307gvgrJHYb/n4ADwixieHqb5j74DVD0rUP
cUE5d0nSZ7hfEkW8xICgs1Ly6Vu3w7Z5M8vb4QmoPnIT1EaHCXiweuK6vjkUk8RQmYY4ITFBs8zHiG7h4n
9bPAgMBAAGiggGhMIIBnTAOBgNVHQ8BAf8EBAMCBaAwQgYDVR0gBDswOTA3BgkrflhQBR8FBAlwKjA
oBggrBgEFBQcCARYcaHR0cDovL2RibW8tcGtpLmZpbmEuaHlvY3BzLzCBZgYDVR0fBIHGMiHDMEMKqQK
A+pDwwOjELMAkGA1UEBhMCSFJxDTALBgNVBAoTBEBZJTkExDTALBgNVBAsTBBERFTU8xDTALBgNVB
AMTBENSTDCwfaB7oHmGT2xkYXA6Ly9kZW1vLWxkYXUzmluYS5oci9vdT1ERU1PLG89RkIOQsXjPUhS
P2NlcnRpZmlyXRIUmV2b2NhdGlvbkxpc3QIM0JiaW5hcnmGJmh0dHA6Ly9kZW1vLXBraS5maW5hLmhyL
2NybC9kZW1vY2EuY3JsMCSGA1UdEAAQMKADZlWMTIwOTI2MDgxMTQ5W0EPMjAxNDU5MjYwODQx
NDIaMB8GA1UdIwQYMBaAFHpgl45InTJrpOUt3bhZtJT8QmKeMB0GA1UdDgQWBRRglJsZevSn6kDuSzC
hmaa9Sqr6sjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBBQUAA4IBAQC05kJWaNjgS+UG7XQHsHersDFk
4K5W/Y2Pbubary0j3lwJrveHbUR3HObo0KiVenF6+1FL3sCI/2tfH3wSszWL8Gkit8jUudT05vDyLqEUXYDHIF
UBwseudsPkUxPiQ6HuuFd3PiUAWf00chXD38eTjfpNu6VeQt4EORSO+rEXdhWihVb5HxFIVPTkqHmq1KI
NwtV9+thwE3hNMwacRa4gwTB1O+jadVIJQMq+kgwnLGLBcwr0W+x1ye6MPSYEUxSNFGHPG/evP9DRL
wJtR3ngvlCDusnO+A75Nn40VYcoljw6EN1V+plK+HkLye0zzLsnHIWTSgfZ2sQVG5xCURil</X509Certificat
e>

```

```

  <X509IssuerSerial>
    <X509IssuerName>OU=DEMO, O=FINA, C=HR</X509IssuerName>
    <X509SerialNumber>1053495409</X509SerialNumber>
  </X509IssuerSerial>
</X509Data>
</KeyInfo>
</Signature>
</tns:ProvjeraOdgovor>

```

```
</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](mailto:fiskalizacija@porezna-uprava.hr) ili putem telefona 0800 1001

FINA pruža podršku obveznicima fiskalizacije oko postupaka vezanih za izdavanje i korištenje certifikata putem email adrese [certifikati-fiskalizacija@fina.hr](mailto: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](mailto: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 i produkcijsku 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-znamenasti 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 Pseudokod 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. DODATAK: Šifarnik grešaka kod provjere računa

U nastavku je šifarnik (potencijalnih) grešaka koji se koristi prilikom provjere računa dostavljenih u Poreznu upravu u testnoj okolini.

Šifra greške	Poruka greške	Opis greške
v100	'Poruka je ispravna'	Poruka ne sadrži ni jednu od u nastavku navedenih grešaka.
v101	'Datum i vrijeme slanja' je za više od 6 sati manje ili veće od 'Datum i vrijeme obrade'.	Datum i vrijeme slanja računa je za više od 6 sati manje ili veće od datuma i vremena zaprimanja računa u sustav fiskalizacije.
v103	'Datum i vrijeme izdavanja' računa je za više od 6 sati veće od 'Datum i vrijeme obrade'.	Datum i vrijeme izdavanja računa je za više od 6 sati veće od datuma i vremena zaprimanja računa u sustav fiskalizacije.
v104	'Datum i vrijeme izdavanja' računa je veće od 'Datum i vrijeme slanja'.	Oba datuma i vremena se generiraju na strani obveznika. Prvo se generira datum i vrijeme izdavanja računa, a tek kasnije datum i vrijeme slanja računa, stoga bi datum i vrijeme izdavanja trebao biti manji ili jednak datumu i vremenu slanja računa.
v105	'Brojčana oznaka računa' ima vrijednost '0'.	Brojčana oznaka računa ne smije biti manja od broja 1.
v106	'Brojčana oznaka računa' ima više od 6 znamenki.	
v110	'Porezna stopa PDV-a' nije iz dozvoljenog skupa poreznih stopa.	Porezna stopa PDV-a je definirana Zakonom o PDV-u. Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a.
v112	'Osnovica PDV-a' je veća od podatka 'Ukupni iznos' kada je 'Ukupni iznos' pozitivnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako je imao grešku 'v137'. Kod ove provjere se sumiraju sve osnovice i onda se iznos uspoređuje s ukupnim iznosom.
v113	'Osnovica PDV-a' je manja od podatka 'Ukupni iznos' kada je 'Ukupni iznos' negativnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako je imao grešku 'v137'. Kod ove provjere se sumiraju sve osnovice i onda se iznos uspoređuje s ukupnim iznosom.
v114	'Osnovica PDV-a' nije istog predznaka kao i 'Ukupni iznos'.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako je imao grešku 'v137'. Kod ove provjere se sumiraju sve osnovice i onda se iznos uspoređuje s ukupnim iznosom.
v115	'Iznos poreza PDV-a' je za više od 1 kn manji od izračuna iznosa PDV-a.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a. Izračuna se iznos PDV-a po formuli Osnovica*Stopa. Dobiveni iznos se ne zaokružuje. Postavlja se raspon dozvoljenih vrijednosti na način: dobiveni iznos +/- 1 kn. Iznos PDV iz poruke se uspoređuje s navedenim rasponom. Koriste se stroge

		nejednakosti. Ako iznos iz poruke naruši donju granicu dozvoljenog raspona onda ova greška.
V116	'Iznos poreza PDV-a' je za više od 1 kn veći od izračuna iznosa poreza PDV-a.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a. Izračuna se iznos PDV-a po formuli Osnovica*Stopa. Dobiveni iznos se ne zaokružuje. Postavlja se raspon dozvoljenih vrijednosti na način: Dobiveni iznos +/- 1 kn. Iznos PDV iz poruke se uspoređuje s navedenim rasponom. Koriste se stroge nejednakosti. Ako iznos iz poruke naruši gornju granicu dozvoljenog raspona onda ova greška.
v117	'Porezna stopa PNP-a' ja manja od 0,00.	
v118	'Porezna stopa PNP-a' ja veća od 3,00.	
v120	'Osnovica PNP-a' je veća od podatka 'Ukupni iznos' kada je 'Ukupni iznos' pozitivnog predznaka ili je jednak 0.	Za obveznika koji je na računu iskazao da je u sustavu PDV-a ova provjera se radi ako ima grešku 'v137'. Kod ove provjere prvo se sumiraju sve osnovice i onda se iznos uspoređuje s ukupnim iznosom. Ako je obveznik na računu iskazao da nije u sustavu PDV-a onda treba uvijek provjeravati ovu grešku.
v121	'Osnovica PNP-a' je manja od podatka 'Ukupni iznos' kada je 'Ukupni iznos' negativnog predznaka ili je jednak 0.	Ako je obveznik na računu iskazao da je u sustavu PDV-a te ako ima grešku 'v137' onda se radi ova provjera. Kod ove provjere prvo se sumiraju sve osnovice i onda se iznos uspoređuje s ukupnim iznosom. Ako je obveznik na računu iskazao da nije u sustavu PDV-a onda treba uvijek provjeravati ovu grešku.
v122	'Osnovica PNP-a' nije istog predznaka kao i 'Ukupni iznos'.	Ako je obveznik na računu iskazao da je u sustavu PDV-a te ako ima grešku 'v137' onda se radi ova provjera. Kod ove provjere prvo se sumiraju sve osnovice i onda se iznos uspoređuje s ukupnim iznosom. Ako je obveznik na računu iskazao da nije u sustavu PDV-a onda treba uvijek provjeravati ovu grešku.
v123	'Iznos poreza PNP-a' je za više od 1 kn manji od izračuna iznosa poreza PNP -a.	Izračuna se iznos PNP-a po formuli Osnovica*Stopa. Dobiveni iznos se ne zaokružuje. Postavlja se raspon dozvoljenih vrijednosti na način: Dobiveni iznos +/- 1 kn. Iznos PNP iz poruke se uspoređuje s navedenim rasponom. Koriste se stroge nejednakosti. Ako iznos iz poruke naruši donju granicu dozvoljenog raspona onda ova greška.
v124	'Iznos poreza PNP -a' je za više od 1 kn veći od izračuna iznosa poreza PNP-a.	Izračuna se iznos PNP-a po formuli Osnovica*Stopa. Dobiveni iznos se ne zaokružuje. Postavlja se raspon dozvoljenih vrijednosti na način: Dobiveni iznos +/- 1 kn. Iznos PNP iz poruke se uspoređuje s navedenim rasponom. Koriste se stroge



		nejednakosti. Ako iznos iz poruke naruši gornju granicu dozvoljenog raspona onda ova greška.
v125	'Na računu postoji podatak 'Ostali porezi' različit od '0,00'.	Trenutno ne postoje 'Ostali porezi'. Provjerava se postoji li stopa, osnovica ili iznos poreza različiti od 0.
v126	Iznos oslobođenja' je veći od podatka 'Ukupni iznos' kada je 'Ukupni iznos' pozitivnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v127	Iznos oslobođenja' je manji od podatka 'Ukupni iznos' kada je 'Ukupni iznos' negativnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v128	Iznos oslobođenja' nije istog predznaka kao i 'Ukupni iznos'.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v129	'Iznos marže' je veći od podatka 'Ukupni iznos' kada je 'Ukupni iznos' pozitivnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v130	'Iznos marže' je manji od podatka 'Ukupni iznos' kada je 'Ukupni iznos' negativnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v131	'Iznos marže' nije istog predznaka kao i 'Ukupni iznos'.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v132	Iznos koji ne podliježe oporezivanju' je veći od podatka 'Ukupni iznos' kada je 'Ukupni iznos' pozitivnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v133	Iznos koji ne podliježe oporezivanju' je manji od podatka 'Ukupni iznos' kada je 'Ukupni iznos' negativnog predznaka ili je jednak 0.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v134	Iznos koji ne podliježe oporezivanju' nije istog predznaka kao i 'Ukupni iznos'.	Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a te ako ima grešku 'v137'.
v135	'Iznos naknade' je veći od 1.000,00 kn.	
v136	'Iznos naknade' je manji od -1.000,00 kn.	
v137	'Ukupan iznos na računu' nije ispravan prema formuli.	Formula za kontrolu ukupnog iznosa je: $SUM(Iznos\ osnovica\ PDV) + SUM(Iznos\ PDV) + (Iznos\ PNP) + (Iznos\ oslobođenja) + (Iznos\ koji\ ne\ podliježe\ oporezivanju) + SUM(Iznos\ naknada)$ . Dopusštena tolerancija je +/- 0,01 kuna. Ova provjera se vrši ako je na računu obveznik iskazao da je u sustavu PDV-a.
v139	Maksimalni ukupni iznos za vrstu plaćanja 'Transakcijski račun' i 'Ostalo' je veći ili manji od 1 mil kn kada je Ukupni iznos pozitivnog/negativnog predznaka.	
v141	Polje 'Specifična namjena' nije prazno.	Polje 'Specifična namjena' je namijenjeno za buduće potrebe.
v142	Na računu postoji podatak 'PDV' različit od '0,00'.	Provjerava se postoji li osnovica, stopa ili iznos PDV-a različit od 0,00 kn. Ova provjera se vrši ako je na računu obveznik iskazao da nije u sustavu PDV-a.
v143	Na računu postoji podatak 'Iznos oslobođenja' različit od 0,00 kn.	Ova provjera se vrši ako je na računu obveznik iskazao da nije u sustavu PDV-a.

v144	Na računu postoji podatak 'Iznos marže' različit od 0,00 kn.	Ova provjera se vrši ako je na računu obveznik iskazao da nije u sustavu PDV-a.
v145	Na računu postoji podatak 'Iznos koji ne podliježe oporezivanju' različit od 0,00 kn.	Ova provjera se vrši ako je na računu obveznik iskazao da nije u sustavu PDV-a.
v148	Maksimalni ukupni iznos za vrstu plaćanja 'Gotovina', 'Kartica' ili 'Ček' je veći ili manji od +/- 75.000,00 kn kada je Ukupni iznos pozitivnog/negativnog predznaka.	
v149	'Datum i vrijeme izdavanja' računa je za više od 120 sati manje od 'Datum i vrijeme obrade'.	Račun je dostavljen u sustav fiskalizacije nakon 120 sati od trenutka izdavanja računa.
V150	'Datum i vrijeme izdavanja' računa je za više od 48 sati do 120 sati manje od 'Datum i vrijeme obrade'.	Račun je dostavljen u sustav fiskalizacije nakon 48 do 120 sati od trenutka izdavanja računa.

---

## **14. Prilozi**

Kao prilog ovom dokumentu dolazi datoteka „Fiskalizacija-WSDL\_v1.4.zip“.