

MINISTARSTVO UPRAVE e-Hrvatska	Dokument tehničke specifikacije		
	Tehnička specifikacija za spajanje na Osobni korisnički pretinac		
	Projekt: e-Građani	Komponenta: OKP	Djelokrug: APIS IT
	Datum: 01.02.2017.	Namjena: Za dionike u projektu	Verzija: 2.0

Projekt e-Građani

Sustav Osobnog korisničkog pretinca

Tehnička specifikacija za spajanje na Osobni korisnički pretinac

VERZIJA 2.0

Sadržaj

1.	Uvod	5
1.1	Svrha	5
1.2	Definicije i skraćenice	5
2.	Poslovna interakcija korisnika (Institucije) i Osobnog korisničkog pretinca	6
2.1	Osobni korisnički pretinac i sustav za zaprimanje poruka	6
2.2	Poslovni procesi između Institucije i Sustava za zaprimanje poruka	6
2.3	Prosljeđivanje poruke za Osobni korisnički pretinac	7
2.3.1	Poruka koja se šalje u Sustav za zaprimanje poruka	9
2.3.2	Poslovna poruka za Osobni korisnički pretinac	13
2.4	Šifrnik grešaka	16
3.	Pregled preduvjeta za spajanje na Sustav za zaprimanje poruka	17
3.1	Mrežni preduvjeti	17
3.2	Sigurnosni preduvjeti	18
3.3	Aplikacijski preduvjeti	18
4.	Topologija pristupa u produkcijskoj okolini	19
4.1	Sigurnost (zaštita od uplitanja treće strane)	20
4.2	Autentikacija, autorizacija i kontrola pristupa	20
4.2.1	Autentikacija, autorizacija na sustavu za zaprimanje poruka	20
4.2.2	Autentikacija, autorizacija na Osobni korisnički pretinac	20
5.	Public Key Infrastructure (PKI)	21
6.	Pregled tehnologija korištenih u komunikaciji s pristupnom točkom sustava za zaprimanje poruka za Osobni korisnički pretinac	22
6.1	XML	22
6.2	SOAP	22
6.3	WS-x	22
6.4	WSDL	23
6.5	HTTP	23
6.6	HTTPS	23
7.	Podrška u radu	24
8.	Dodatak	25
8.1	Uključivanje korisnika u Sustav za zaprimanje poruka i u OKP	25
8.1.1	Podaci koje treba dostaviti institucija prije slanja podataka u OKP	25
8.1.2	Podaci koji će biti dodijeljeni instituciji za slanje poruka u OKP	26
8.2	Registracija e-poruka u sustavu OKP	26
8.2.1	Podaci koje treba dostaviti institucija prije slanja nove e-poruke u OKP	26
8.2.2	Podaci koji će biti dodijeljeni instituciji za slanje nove e-poruke u OKP	26
8.3	Dohvat podataka o personalizaciji e-poruka	27
8.3.1	Postupak upita u servis za Dohvat podataka o personalizaciji e-poruka	27
8.3.2	Poslovna poruka ZAHTJEVA za provjerom/dohvatom podataka o personalizaciji e-poruka (za točno određeni tip e-poruke)	28
8.3.3	Poslovna poruka ODGOVORA s provjerom/dohvatom podataka o personalizaciji e-poruka (za točno određeni tip e-poruke)	30
8.4	Šifrnik grešaka	33
8.5	Dostava liste OIB-ova korisnika koji imaju otvoreni OKP	34
8.5.1	Mrežni preduvjeti	34

8.5.2	Sigurnosni preduvjeti	34
9.	Popis priloga	35

Povijest promjena

Verzija	Datum	Sažetak	Autor	Vrijedi od
1.0	31.05.2013	Inicijalna verzija	APIS IT	
1.0.1	05.06.2013	Ažurirano poglavlje: 2.4. – dodana nova greška „K011 – KP je zapunjen“	APIS IT	
1.1.	09.07.2013	Ažurirana poglavlja: 2.3.1 Poruka koja se šalje u Sustav za zaprimanje poruka 2.3.2 Poslovna poruka za Korisnički pretinac 3.1. Mrežni preduvjeti Dodano poglavlje: 8.1. Dostava liste OIB-ova korisnika koji imaju otvoreni Korisnički pretinac 8.2 Zahtjev i proces za uključivanje korisnika u Sustav za zaprimanje poruka i u Korisnički pretinac	APIS IT	
1.1.1	06.09.2013	Ažurirana poglavlja: 7. Podrška u radu 8. Dodatak	APIS IT	
1.1.2	23.09.2013	Ažurirana naslovna stranica – dodano zaglavlje	APIS IT	
1.1.3	29.10.2013	Ažurirano poglavlje: 8.2.2. Sigurnosni preduvjeti 9. Dodatak	APIS IT	
1.2	01.06.2015	Ažurirana poglavlja radi uvođenja polja „Tip poruke“ u servisu za slanje poruka u OKP: <i>2.3 Objavljen datum produkcije nove verzije servisa</i> <i>2.3.2 Poslovna poruka za Osobni korisnički pretinac</i> <i>2.4 Šifarnik grešaka</i> <i>8.2 Registracija e-poruka u sustavu OKP</i> Dorada dokumenta vezano uz personalizaciju e-poruka. Dodana poglavlja: <i>8.3 Dohvat podataka o personalizaciji e-poruka</i> <i>8.4 Šifarnik grešaka</i>	APIS IT	01.09.2015.
1.3	12.01.2016	Ažurirana poglavlja radi zamjene SSL-a TLS protokolom : 2.2 Poslovni procesi između Institucije i Sustava za zaprimanje poruka 2.3 Napomena 3.2 Sigurnosni preduvjeti 4. Topologija pristupa u produkcijskoj okolini 4.1 Sigurnost (zaštita od uplitanja treće strane) 4.2 Autentikacija, autorizacija i kontrola pristupa 4.2.1 Autentikacija, autorizacija na sustavu za zaprimanje poruka 5. Public Key Infrastructure (PKI) 8.5 Napomena 8.5.2 Sigurnosni preduvjeti	APIS IT	01.02.2016.
1.4	10.02.2016	Ažurirano poglavlje : 8.1 Uključivanje korisnika u Sustav za zaprimanje poruka i u OKP	APIS IT	10.02.2016.
1.5	30.03.2016	Ažurirano poglavlje : 8.4 Šifarnik grešaka Napravljena dopuna kontrole grešaka na sustavu za zaprimanje poruka	APIS IT	30.03.2016.
1.5	20.04.2016	Ažurirano poglavlje : 8.5.2 Sigurnosni preduvjeti Predstavljanje klijentskoj strani s TLS certifikatom u	APIS IT	25.04.2016.

		testnoj i produkcijskoj okolini		
1.5	20.04.2016	9.0 Popis priloga Izbačena točka 6. „APIS IT.cer“	APIS IT	25.04.2016.
1.6	25.04.2016	Ažurirano poglavlje : 8.1 Uključivanje korisnika u Sustav za zaprimanje poruka i u OKP 8.2 Registracija e-poruka u sustavu OKP 8.3 Dohvat podataka za slanje (ili personalizaciju) e-poruka Dodana nova greška K015		13.12.2016
2.0	01.02.2017	Nova verzija servisa 124 (poglavlje 8.5) je u produkcijskoj okolini	APIS IT	01.02.2017

1. Uvod

1.1 Svrha

Ovim dokumentom opisuje se način informatičkog povezivanja među tijelima javne uprave s ciljem dostave poruke u Osobni korisnički pretinac posredstvom sustava za zaprimanje poruka.

U dokumentu se detaljno opisuju:

- podatkovni skupovi i poruke koje sustavi uključenih strana razmjenjuju,
- slijed razmjene poruka (slijedni dijagram),
- tehnički preduvjeti za uspostavljanje informatičke povezanosti, te
- opis korištenih tehnoloških standarda.

1.2 Definicije i skraćenice

Pojam	Opis
Institucija	Institucija koja želi poslati e-poruke u Osobni korisnički pretinac.
Sustav za zaprimanje poruka	Sustav koji zaprima zahtjeve te vrši sigurnosnu kontrolu e-poruka za Osobni korisnički pretinac.
OKP	„Osobni korisnički pretinac“ – Osobni korisnički pretinac je jedna od tri komponente koja se razvija po načelima sustava e-Građani. Služi za komunikaciju tijela državne uprave prema građanima.
Registar korisnika	Registar korisnika ovlaštenih za rad sa sustavom za zaprimanje e-poruka.

2. Poslovna interakcija korisnika (Institucije) i Osobnog korisničkog pretinca

2.1 Osobni korisnički pretinac i sustav za zaprimanje poruka

Osobni korisnički pretinac je jedna od tri komponente koja se u razvija po načelima sustava e-Građani. Osnovna funkcija Osobnog korisničkog pretinca je zaprimanje poruka za OIB (fizičku osobu) koje su poslone od strane institucija – tijela javne uprave.

Sustav za zaprimanje poruka ima funkciju formalne i sigurnosne kontrole poruka zaprimljenih od institucija te prosljeđivanje poruka u Osobni korisnički pretinac.

Institucija koja želi poslati poruku u Osobni korisnički pretinac prije početka slanja poruka mora zatražiti registraciju u sustav za zaprimanje poruka, kao i registraciju u Osobni korisnički pretinac.

2.2 Poslovni procesi između Institucije i Sustava za zaprimanje poruka

Institucija iz svojih poslovnih procesa kreira poruku koju želi poslati u Osobni korisnički pretinac. Pritom institucija kreira poruku prema dogovorenoj shemi koju propisuje Sustav za zaprimanje poruka. Poruka koja se šalje u sustav za zaprimanje poruka je opisana u poglavlju 2.3.1.

Poslovnu poruku za Osobni korisnički pretinac institucija kreira prema dogovorenoj shemi koju propisuje Osobni korisnički pretinac. Poruka koja se šalje u Osobni korisnički pretinac je opisana u poglavlju 2.3.2..

Ukoliko je zahtjev prema Sustavu za zaprimanje poruka ispravan, Sustav za zaprimanje poruka prosljeđuje poruku u Osobni korisnički pretinac. Ukoliko zahtjev nije prošao sigurnosnu kontrolu ili nije ispravno popunjen, vraća se odgovor o grešci (npr. ako institucija nema ovlasti koristiti sustav za zaprimanje poruka, poruka nije u zadanoj shemi i sl.).

Sustav za zaprimanje poruka tehnološki je realiziran kao web servis (SOAP/HTTPS) i koristi Internet ili Hitronet kao komunikacijski kanal, te isti koristi HTTPS protokol te autentikaciju na komunikacijskoj razini (tzv. uzajamna autentikacija na razini TLS protokola).

Sustav za zaprimanje poruka podržava dostavu poruke maksimalne veličine poruke zahtjeva do 1MB (ovojnica + poslovna poruka).

2.3 Prosljeđivanje poruke za Osobni korisnički pretinac

Za dostavu poruka u Osobni korisnički pretinac (OKP) predviđen je sinkroni model komunikacije preko Sustava za zaprimanje poruka.

Ukoliko je zahtjev koji je stigao u sustav za zaprimanje poruka od strane institucije ispravan, Sustav za zaprimanje poruka prosljeđuje zahtjev prema Osobnom korisničkom pretincu.

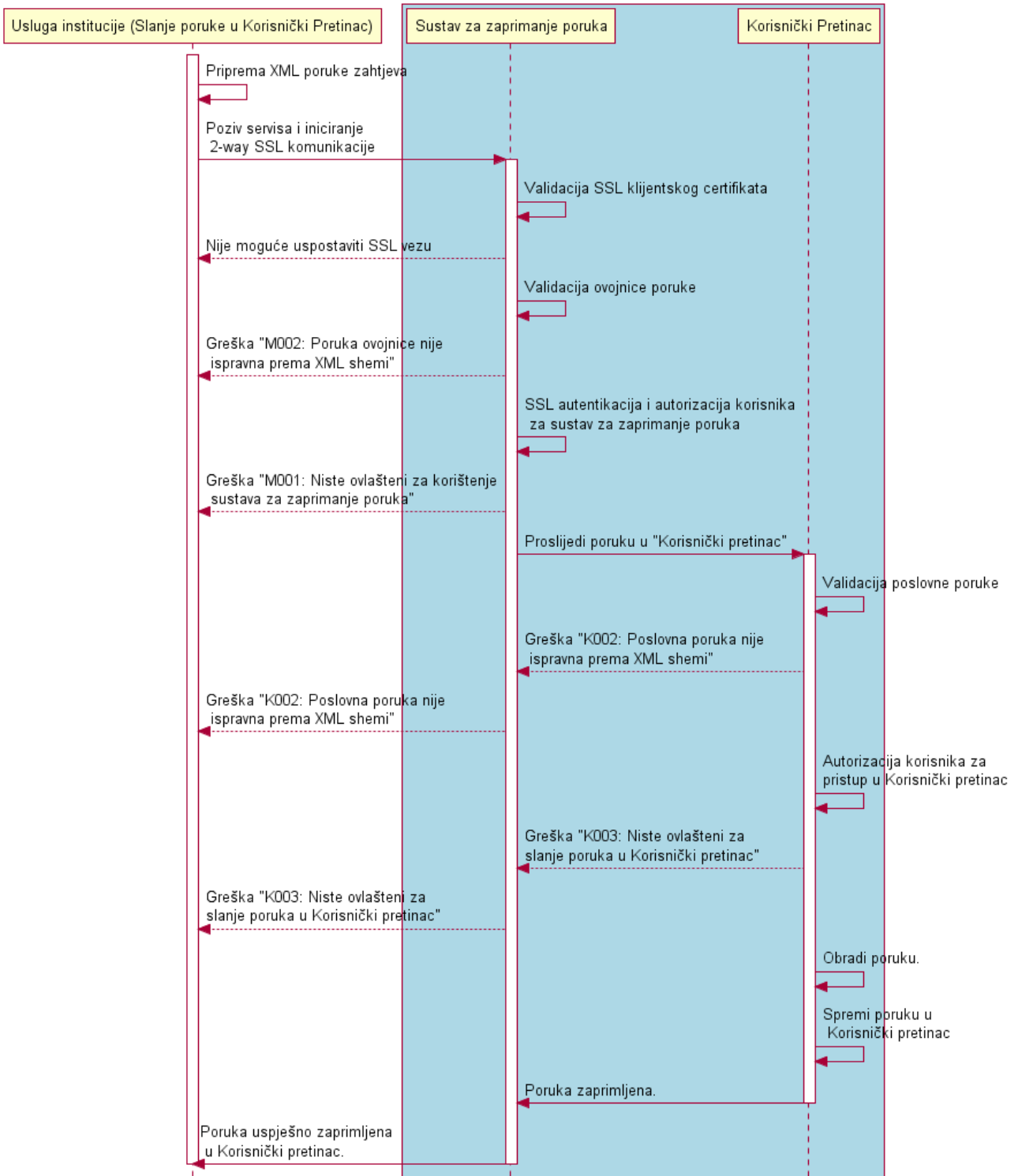
Osobni korisnički pretinac skida ovojnici koja je propisana prema Sustavu za zaprimanje poruka, te obavlja formalnu i sigurnosnu kontrolu poslovne poruke za Osobni korisnički pretinac.

Ukoliko je poslovna poruka ispravna, instituciji se vraća odgovor s informacijom o zaprimanju poruke u Osobni korisnički pretinac posredstvom sustava za zaprimanje poruka, a sukladno propisanoj shemi Sustava za zaprimanje poruka i Osobnog korisničkog pretinca.

Ukoliko poslovna poruka nije prošla sigurnosnu kontrolu ili nije ispravno popunjena, vraća se odgovor o grešci (npr. ako institucija nema ovlasti za slanje poruka u Osobni korisnički pretinac ili poruka nije u zadanoj shemi i sl.).

Poruka koja se dostavlja u Osobni korisnički pretinac se odnosi na jednu fizičku osobu (OIB) koja može imati jedan ili više primitaka, ali da ukupna poruka zahtjeva ne prelazi zadanu veličinu (1 MB).

Na slici 1 prikazan je slijedni dijagram prosljeđivanja poruke preko Sustava za zaprimanje poruka u Osobni korisnički pretinac. (Slika prikazuje i dijagram prosljeđivanja poruka prilikom javljanja nekih grešaka. Popis svih grešaka naveden je u poglavlju 2.4.).



Slika 1. Slijedni dijagram slanja poruke u Osobni korisnički pretinac

2.3.1 Poruka koja se šalje u Sustav za zaprimanje poruka

2.3.1.1 Podatkovni skup za zahtjev koji se prosljeđuje preko Sustava za zaprimanje poruka (poslovni dio poruke je opisan pod 2.3.2.)

Polje	Obavezan	Opis / Napomena
ZAGLAVLJE		
SenderId	DA	ID korisnika iz registra korisnika Sustava za zaprimanje poruka. Podatak mora biti naveden.
ServiceId	DA	ID usluge iz registra usluga Sustava za zaprimanje poruka. Podatak mora biti naveden.
AdditionalServiceId	NE	ID usluge iz registra usluga Sustava za zaprimanje poruka. Podatak može ali ne mora biti naveden.
MessageId	DA	UUID format. ID poruke pošiljatelja. Podatak mora biti naveden.
SenderTimeStamp	DA	Datum i vrijeme slanja poruke pošiljatelja. Podatak mora biti naveden.
GSBId	NE	UUID format. Jedinstveni identifikator razmjene koji dodjeljuje Sustav za zaprimanje poruka u trenutku zaprimanja poruke zahtjeva od pošiljatelja. Podatak ne smije biti naveden.
ReceivingTimeStamp	NE	Datum i vrijeme zaprimanja poruke od pošiljatelja u Sustav za zaprimanje poruka. Podatak ne smije biti naveden.
ForwardingTimeStamp	NE	Datum i vrijeme prosljeđivanja poruke od Sustava za zaprimanje poruka prema usluzi. Podatak ne smije biti naveden.
ReceiverTimeStamp	NE	Datum i vrijeme zaprimanja poruke od Sustava za zaprimanje poruka na strani usluge (primatelja). Podatak ne smije biti naveden.
ExchangeStatus	NE	Status razmjene govori je li poruka uspješno prosljeđena usluzi (primatelju). Podatak ne smije biti naveden.
POSLOVNA PORUKA		
MimeType	DA	Tip poruke
Description	NE	Opis poruke
Data	DA	Poruka u formatu definiranom od usluge ili sukladno dogovoru između pošiljatelja i usluge. Poslovna poruka mora biti navedena.
DIGITALNI POTPIS		
Signature	NE	Predviđeno za digitalno potpisivanje poruke.

2.3.1.2 Primjer poruke koji se prosljeđuje preko Sustava za zaprimanje poruka

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:SendMessageRequest
  xmlns:tns="http://apis-it.hr/umu/2013/types/gsb"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://apis-it.hr/umu/2013/types/gsb ../schema/GSBSchema.xsd"
  ">
  <tns:GsbEnvelope>
    <tns:MessageHeader>
      <tns:SenderId>000000001</tns:SenderId>
      <tns:ServiceId>000000002</tns:ServiceId>
      <tns:MessageId>733362f1-063f-11e2-892e-0802200c9a62</tns:MessageId>
      <tns:SenderTimeStamp>2013-05-31T12:00:00</tns:SenderTimeStamp>
    </tns:MessageHeader>
    <tns:Content>
      <tns:MimeType>application/xml</tns:MimeType>
      <tns>Data encoding="EMBEDDED">
        <tns:KorisnickiPretinacPoruka
          xmlns:tns="http://apis-it.hr/umu/2013/types/kp"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://apis-it.hr/umu/2013/types/kp
            ../schema/KorisnickiPretinacSchema.xsd ">
          ....
        </tns:KorisnickiPretinacPoruka>
      </tns>Data>
    </tns:Content>
  </tns:GsbEnvelope>
</tns:SendMessageRequest>
```

2.3.1.3 Podatkovni skup za odgovor od Sustava za zaprimanje poruka

Polje	Obavezan	Opis / Napomena
ZAGLAVLJE		
SenderId	DA	Prepisano iz poruke zahtjeva.
ServiceId	DA	Prepisano iz poruke zahtjeva.
AdditionalServiceId	NE	Prepisano iz poruke zahtjeva.
MessageId	DA	Prepisano iz poruke zahtjeva.
SenderTimeStamp	DA	Prepisano iz poruke zahtjeva.
GSBId	NE	UUID format. Jedinstveni identifikator razmjene koji dodjeljuje Sustav za zaprimanje poruka u trenutku zaprimanja poruke zahtjeva od pošiljatelja.
ReceivingTimeStamp	NE	Datum i vrijeme zaprimanja poruke od pošiljatelja u Sustav za zaprimanje poruka.
ForwardingTimeStamp	NE	Datum i vrijeme prosljeđivanja poruke od Sustava za zaprimanje poruka prema usluzi.
ReceiverTimeStamp	NE	Datum i vrijeme zaprimanja poruke od Sustava za zaprimanje poruka na strani usluge (primatelja).
ExchangeStatus	NE	Status razmjene govori je li poruka uspješno prosljeđena usluzi (primatelju).
POSLOVNA PORUKA		
MimeType	NE	Tip poruke
Description	NE	Opis poruke
Data	NE	Poruka u formatu definiranom od usluge ili sukladno dogovoru između pošiljatelja i usluge.
DIGITALNI POTPIS		
Signature	NE	Predviđeno za digitalno potpisivanje poruke.
GREŠKE (može biti lista greški)		
ErrorCode	NE	Šifra greške prema šifarniku grešaka.
ErrorMessage	NE	Opis greške prema šifarniku grešaka.

2.3.1.4 Primjer poruke za odgovor od Sustava za zaprimanje poruka

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:SendMessageResponse xmlns:tns="http://apis-it.hr/umu/2013/types/gsb"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://apis-it.hr/umu/2013/types/gsb
../schema/GSBSchema.xsd ">
  <tns:MessageHeader>
    <tns:SenderId>000000001</tns:SenderId>
    <tns:ServiceId>000000002</tns:ServiceId>
    <tns:MessageId>733362f1-063f-11e2-892e-0802200c9a62</tns:MessageId>
    <tns:GsbId>712362f1-089f-11e2-892e-0803214c9a62</tns:GsbId>
    <tns:SenderTimeStamp>2013-05-31T12:00:00</tns:SenderTimeStamp>
    <tns:ReceivingTimeStamp>2001-12-
31T12:00:00</tns:ReceivingTimeStamp>
    <tns:ForwardingTimeStamp>2001-12-
31T12:00:00</tns:ForwardingTimeStamp>
    <tns:ReceiverTimeStamp>2001-12-31T12:00:00</tns:ReceiverTimeStamp>
    <tns:ExchangeStatus>2</tns:ExchangeStatus>
  </tns:MessageHeader>
  <tns:Content>
    <tns:MimeType>tns:MimeType</tns:MimeType>
    <tns:Description>tns:Description</tns:Description>
    <tns>Data encoding="EMBEDDED">
      <tns:Odgovor xmlns:tns="http://apis-it.hr/umu/2013/types/kp"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://apis-it.hr/umu/2013/types/kp
../schema/KorisnickiPretinacSchema.xsd ">
        <tns:IdPorukePosiljatelja>732262f1-063f-11e2-892e-
0812200c9a68</tns:IdPorukePosiljatelja>
        <tns:DatumVrijemeObrade>2013-05-
31T12:05:00</tns:DatumVrijemeObrade>
      </tns:Odgovor>
    </tns>Data>
  </tns:Content>
</tns:SendMessageResponse>
```

2.3.2 Poslovna poruka za Osobni korisnički pretinac

2.3.2.1 Poslovna poruka zahtjeva za Osobni korisnički pretinac:

Polje	Obavezan	Opis / Napomena
ZAGLAVLJE (obavezno jedan zapis)		
IdPosiljatelja	DA	ID pošiljatelja u registru Osobnog korisničkog pretinca
TipPoruke	DA	Tip poruke registriran u Registru e-poruka
IdPoruke	DA	ID poruke u sustavu pošiljatelja
DatumVrijemeSlanja	DA	Datum i vrijeme slanja poruke u sustavu pošiljatelja
RazinaSigurnosti	DA	Razina sigurnosti koju poruka zahtjeva da bi se prikazala u 'Osobnom korisničkom pretincu'
PODACI O PORUCI (obavezno jedan zapis)		
PinPrimatelja	DA	Za hrvatske građane – OIB (od 01.07. 2013. samo jedan primatelj)
OznakaDrzave	DA	Oznaka države prema šifarniku. Za hrvatske građane oznaka 'HR'
Predmet	DA	Naslov poruke
Sadržaj	DA	Tekst unutar elementa sadržaj mora biti base64 encodiran *
PODACI O PRIVICIMA (0...n zapisa)		
Naziv	DA	Naslov/naziv dokumenta*
MimeType	DA	Tip poruke
Opis	NE	Opis dokumenta
Data	DA	Mogućnost slanja attachmenta (BLOB)

* Polje „Sadržaj „ mora biti base 64 enkodiran. Razlog base 64 enkodiranja je omogućavanje prikazivanja različitih načina formatiranja poruke. Na ovaj način je omogućen prijenos ne strukturiranog teksta, teksta s određenim formatiranjem ili kompletne html stranice. Također treba napomenuti da je maksimalna duljina stringa unutar elementa 2000 znakova u što su ubrojani i svi html tagovi.

*Pošiljatelju je dozvoljeno slati samo privitke koji u nazivu ne sadržavaju znakove \ / : * ? < > | ; , !
(PRAVILO : A file name can't contain any of the following)

2.3.2.2 Primjer poslovne poruke zahtjeva za Osobni korisnički pretinac

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:KorisnickiPretinacPoruka
  xmlns:tns="http://apis-it.hr/umu/2013/types/kp"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://apis-it.hr/umu/2013/types/kp
  ../schema/KorisnickiPretinacSchema.xsd ">
  <tns:Zaglavlje>
    <tns:IdPosiljatelja>000000001</tns:IdPosiljatelja>
    <tns:TipPoruke>000000253</tns:TipPoruke>
    <tns:IdPoruke>732262f1-063f-11e2-892e-0812200c9a68</tns:IdPoruke>
    <tns:DatumVrijemeSlanja>2001-12-31T12:00:00</tns:DatumVrijemeSlanja>
    <tns:RazinaSigurnosti>2</tns:RazinaSigurnosti>
  </tns:Zaglavlje>
  <tns:Poruka>
    <tns:PinPrimatelja>012345678901</tns:PinPrimatelja>
    <tns:OznakaDrzave>HR</tns:OznakaDrzave>
    <tns:Predmet>Neka testna poruka</tns:Predmet>
    <tns:Sadrzaj>U2FkcsW+YWogbmVrZSB0ZXN0bmUgcG9ydWt1</tns:Sadrzaj>
  </tns:Poruka>
  <tns:Privici>
    <tns:Privitak>
      <tns:Naziv>TestniPrivitak</tns:Naziv>
      <tns:MimeType>aplication/pdf</tns:MimeType>
      <tns:Opis>tns:Opis</tns:Opis>
      <tns>Data
encoding="BASE64">JVBERi0xLjcNJeLjz9MNCjcxIDAgb2JqDTw8L0ZpbHRlci9GbGF0ZURl.....
      </tns>Data>
    </tns:Privitak>
  </tns:Privici>
</tns:KorisnickiPretinacPoruka>
```

2.3.2.3 Poslovna poruka odgovora od Osobnog korisničkog pretinca:

Polje	Obavezan	Opis / Napomena
ZAGLAVLJE (obavezno jedan zapis)		
IdPorukePosiljatelja	NE	Prepisano iz zahtjeva
ODGOVOR		
DatumVrijemeObrade	NE	Datum i vrijeme obrade poruke u 'Osobnom korisničkom pretincu'
GREŠKE		
SifraGreske	DA, ako ima grešaka	Šifra greške prema šifarniku grešaka
OpisGreske	DA, ako ima grešaka	Opis greške prema šifarniku grešaka

2.3.2.4 Primjer poslovne poruke odgovora od Osobnog korisničkog pretinca

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:Odgovor xmlns:tns="http://apis-it.hr/umu/2013/types/kp"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://apis-it.hr/umu/2013/types/kp
  ../schema/KorisnickiPretinacSchema.xsd ">
  <tns:IdPorukePosiljatelja>732262f1-063f-11e2-892e-
  0812200c9a68</tns:IdPorukePosiljatelja>
  <tns:DatumVrijemeObrade>2013-05-31T12:05:00</tns:DatumVrijemeObrade>
</tns:Odgovor>
```

2.4 Šifarnik grešaka

1. Šifarnik grešaka za greške koje se mogu dogoditi u Sustavu za zaprimanje poruka

Šifra	Poruka
M001	Niste ovlašteni za korištenje sustava za zaprimanje poruka.
M002	Poruka nije ispravna prema XML shemi: #element ili lista elemenata koji nisu ispravni prema shemi#.
M003	ID pošiljatelja naveden u poruci ne odgovara pošiljatelju prema registru korisnika.
M004	ID usluge naveden u poruci nije evidentiran u registru usluga.
M005	ID dodatne usluge naveden u poruci nije evidentiran u registru usluga.
M006	U poruci su navedeni podaci koji ne smiju biti navedeni: #element ili lista elemenata koji poslovno ne smiju biti navedeni, a navedeni su#.
M007	Datum i vrijeme pošiljatelja navedeni u poruci nisu formalno i/ili logički ispravni.
M008	Usluga je nedostupna.
M009	Usluga je vratila neispravan odgovor.
M010	Sistemska pogreška.
M011	ID usluge naveden u poruci je evidentiran u registru usluga ali usluga nije aktivna.
M012	ID dodatne usluge naveden u poruci je evidentiran u registru usluga ali usluga nije aktivna.

2. Šifarnik grešaka za greške koje se mogu dogoditi u sustavu Osobnog korisničkog pretinca

Šifra	Poruka
K001	Poruka je prevelika. Dozvoljena je veličina poruke do 1 MB.
K002	Poruka nije ispravna prema XML shemi: #element ili lista elemenata koji nisu ispravni prema shemi#.
K003	Niste ovlašteni za slanje poruka u Korisnički pretinac.
K004	Datum i vrijeme navedeni u poruci nisu formalno i/ili logički ispravni.
K005	OIB iz poruke nije formalno ispravan.
K006	OIB iz poruke nema aktivan Korisnički pretinac.
K007	Neispravna vrijednost za podatak 'Oznaka države'.
K008	Poruka nije ispravna po formatu.
K009	Poruka sadrži već postojeći jedinstveni identifikator poruke (ID_PORUKE).
K010	Id pošiljatelja ne odgovara onom iz poruke!
K011	Korisnički pretinac je zapunjen
K012	Sadržaj poruke nije Base64 kodiran.
K013	Niste registrirani za slanje navedenog tipa poruke.
K014	OIB iz poruke ne želi primiti navedeni tip poruke u svoj OKP.
K015	Razina sigurnosti iz poruke ne odgovara definiranoj razini za poslani tip poruke!

3. Pregled preduvjeta za spajanje na Sustav za zaprimanje poruka

Centralni informacijski sustav za zaprimanje poruka biti će dostupan u dvije okoline:

1. Testna
2. Produkcijaska

Uvjeti spajanja su slični, a razlikuju se u različitim adresama pristupnih točaka i certifikatima. U testnoj okolini koriste se certifikati za testnu okolinu, a u produkcijskoj za produkcijsku okolinu. U produkcijskoj okolini koriste se certifikati izdani od FINA RDC. U testnoj okolini koriste se certifikati izdani od FINA DEMO RDC.

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

3.1 Mrežni preduvjeti

Za spajanje na Sustav za zaprimanje poruka za Osobni korisnički pretinac klijentski sustav mora zadovoljiti sljedeće mrežne preduvjete:

Vrsta mreže	Internet, Hitronet
Potrebni otvoreni TCP port-ovi	8450
Internet adresa pristupnog poslužitelja u testnoj okolini	https://cistest.apis-it.hr:8450/GSBServiceTest
Internet adresa pristupnog poslužitelja u produkcijskoj okolini	https://cis.apis-it.hr:8450/GSBService

3.2 Sigurnosni preuvjeti

Sva komunikacija sa Sustavom za zaprimanje poruka zaštićena je 2-way TLS enkripcijom na transportnom sloju. U produkcijskoj okolini sustav za zaprimanje poruka predstavlja se klijentu TLS certifikatom izdanim od FINA RDC. A za testnu okolinu TLS certifikatom izdanim od FINA DEMO RDC.

Zaštita na transportnom sloju	HTTPS (TLS v1.1 ili v1.2, AES enkripcija)
Certifikat za TLS izdan od FINA RDS	Tip certifikata: poslužiteljski

3.3 Aplikacijski preuvjeti

Funkcionalnost Sustava za zaprimanje poruka je dostupna klijentima koristeći tehnologiju Web servisa. Iz tog razloga klijentska aplikacija (ili infrastruktura, ovisno o realizaciji) mora zadovoljiti sljedeće preuvjete:

Standardi kreiranja klijenta	WS-I
Tip servisa	document-literal
Aplikacijski protokol	SOAP/HTTPS (SOAP 1.1)
Kodne stranice	UTF-8

4. Topologija pristupa u produkcijskoj okolini

Institucije pristupaju Sustavu za zaprimanje poruka iniciranjem 2-way TLS veze. Koristeći TLS kanal institucije prema opisanoj proceduri razmjenjuju poruke s pristupnom točkom sustava. Razmjena podataka je sinkrona što znači da pristupna točka odmah odgovara na zahtjev korisnika. Format poruka zahtjeva i odgovora specificirani su kroz XML shemu.

Pristupna točka Sustava za zaprimanje poruka

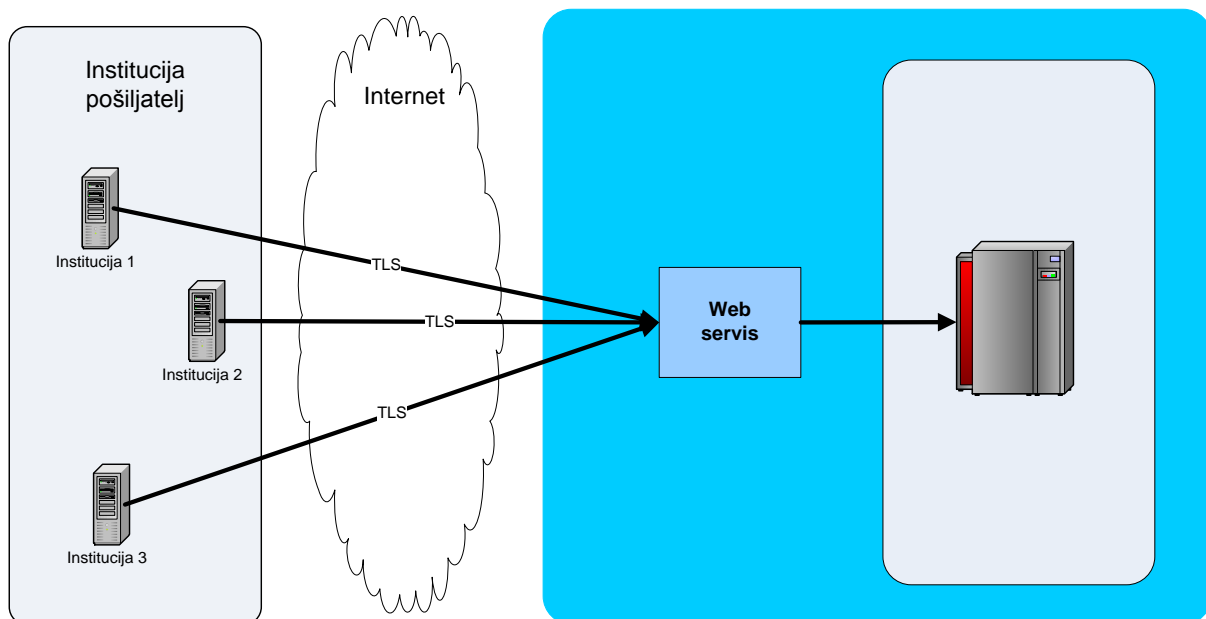
Implementacija i održavanje pristupne točke je zadaća APIS IT-a. APIS IT će institucijama omogućiti spajanje na pristupnu točku i to u dvije okoline, testnoj i produkcijskoj.

Internet veza

Pristupna točka će biti dostupna preko Internet i Hitronet mreže HTTPS protokolom.

Informacijski sustav institucije pošiljatelja (klijenti)

Institucije su zaduženi osigurati hardversku i softversku podršku za slanje poruka s pristupnom točkom. Razvoj hardversko-softverskog rješenja je u domeni institucije. Institucija je također dužna osigurati Internet ili Hitronet vezu prema pristupnoj točki.



Slika 2. Topologija pristupa Sustavu za zaprimanje poruka za KP

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) sa sustavom za zaprimanje poruka.

Konkretno koristi se 2-way TLS sa poslužiteljskim certifikatom za terminaciju TLS-a sa autentikacijom klijenta. Taj mehanizam onemogućava nepoznatim stranama spajanje na pristupnu točku, a ujedno se poslužitelj sustava za zaprimanje poruka predstavlja klijentima.

Kao Certificate Authority koristiti će se usluge FINA CA. To znači da poslužitelji na krajnjim točkama sustava u produkcijskoj okolini (APIS IT i korisnici) moraju imati valjan certifikat izdan od FINA CA.

Klijenti će se spajati preko SOAP/HTTPS protokola. Treba napomenuti da je primijenjena verzija SOAP protokola 1.1.

4.2 Autentikacija, autorizacija i kontrola pristupa

Kontrola pristupa realizirana je na dva nivoa:

- na Sustavu za zaprimanje poruka,
- na sustavu Osobni korisnički pretinac.

4.2.1 Autentikacija, autorizacija na sustavu za zaprimanje poruka

Kako je već ranije opisano, kontrola pristupa realizirana je dvostrukom provjerom certifikata kod uspostave TLS veze. Na taj način pristup je omogućen samo unaprijed poznatim udaljenim poslužiteljima sa važećim X.509 certifikatima prema FINA RDC-u. Kontrola pristupa se nužno ne obavlja svakim pristupom poslužitelju. Postavkom keep-alive u HTTP konekciji jednu konekciju je moguće koristiti za više upita.

Preduvjet za uspješnu kontrolu pristupa u sustav za zaprimanje poruka je registracija institucije.

4.2.2 Autentikacija, autorizacija na Osobni korisnički pretinac

Autorizacija provjerava da li institucija ima pravo slanja poruka u Osobni korisnički pretinac. Ukoliko se u procesu autorizacije pokaže da institucija nema pravo slanje poruka u Osobni korisnički pretinac vraća mu se odgovor sa porukom o grešci.

Preduvjet za uspješnu kontrolu pristupa u sustav Osobnog korisničkog pretinca je registracija institucije.

5. Public Key Infrastructure (PKI)

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

Uporaba certifikata na strani pristupne točke sustava za zaprimanje poruka je:

- uspostava TLS veze prema sustavu za zaprimanje poruka
- autentikacija i identifikacija klijenta (institucije)

Certifikati koje koristi pristupna točka sustava za zaprimanje poruke po okolinama imaju sljedeće nazive:

1. Testna

- Poslužiteljski: `cistest.apis-it.hr` (izdan od FINA DEMO RDC)

2. Produkcijska

- Poslužiteljski: `cis.apis-it.hr` (izdan od FINA RDC)

Ovaj dokument ne prati promjene u domeni FINA-e kao certifikacijskog tijela (CA). Ažurne informacije nalaze se na gore navedenim stranicama FINA-e. Novi certifikati izdani su od npr. FINA RDC 2015 ili Fina Demo CA 2014.

Sve promjene koje provodi CA trebaju pratiti svi dionici uključeni u ovu razmjenu.

6. Pregled tehnologija korištenih u komunikaciji s pristupnom točkom sustava za zaprimanje poruka za Osobni korisnički pretinac

6.1 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.

6.2 SOAP

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

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

6.3 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.

6.4 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, izašla sredinom prošle godine, to postala.

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

6.5 HTTP

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

HTTP protokol radi na principu zahtjeva i odgovora (engl. 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.

6.6 HTTPS

Hypertext Transfer Protocol Secure (HTTPS) je kombinacija HTTP-a i protokola koji ostvaruje mrežnu sigurnost.

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

7. Podrška u radu

Za pomoć u radu kako na testnoj, tako i na produkcijskoj okolini, predviđena je komunikacija mail-om preko središnje točke za podršku korisnicima:

Help Deska APIS IT-a (helpdesk@apis-it.hr)

Naslov mail-a treba sadržavati:

- 'Osobni korisnički pretinac **PROD**' kada je riječ o produkcijskom radu, odnosno
- 'Osobni korisnički pretinac **TEST**' kada se radi o radu na testnoj okolini.

8. Dodatak

8.1 Uključivanje korisnika u Sustav za zaprimanje poruka i u OKP

Potrebno je da institucija dostavi skup podataka potrebnih za registraciju (**OKP - Obrazac za pošiljatelja e-poruke**), propisan od strane Ministarstva uprave. Popunjeni obrazac prosljeđuje se na APIS IT Help Desk (helpdesk@apis-it.hr) kao zahtjev za uključivanje institucije u Sustav za zaprimanje poruka u OKP s nazivom :

„Osobni korisnički pretinac – zahtjev za registraciju **TEST**“ za testnu okolinu, ili
„Osobni korisnički pretinac – zahtjev za registraciju **PROD**“ za produkcijsku okolinu.

Nakon obrade zahtjeva i registracije, institucija dobiva povratnu informaciju:

- ID u Sustavu za zaprimanje poruka.** Institucija će koristiti podatak prilikom izrade XML poruke zahtjeva u elementu „SenderId“.
- ID u Osobnom korisničkom pretincu.** Institucija će koristiti podatak prilikom izrade XML poruke zahtjeva u elementu „IdPosiljatelja“.
- ID Usluge.** Institucija će koristiti podatak prilikom izrade XML poruke zahtjeva u elementu "ServiceId".

Ukoliko postoji potreba da ista institucija (ili institucija koja je već uključena) pristupa u Sustav za zaprimanje poruka u OKP s različitim certifikatima, postupak uključjenja je potrebno provesti za svaki certifikat posebno, znači dostaviti zahtjeve za uključjenje za svaki od njih.

Ukoliko postoji potreba za produljenjem isteklog certifikata potrebno je informaciju s podacima o produljenom certifikatu poslati na APIS IT Help Desk (helpdesk@apis-it.hr) kao zahtjev za produljenje certifikata za Sustav za zaprimanje poruka u OKP s nazivom :

„Osobni korisnički pretinac – zahtjev za produljenje certifikata **TEST**“ za testnu okolinu, ili
„Osobni korisnički pretinac – zahtjev za produljenje certifikata **PROD**“ za produkcijsku okolinu.

8.1.1 Podaci koje treba dostaviti institucija prije slanja podataka u OKP

	Napomena
OIB institucije	
Naziv institucije	Službeni naziv institucije. Trebao bi odgovarati nazivu institucije koji je evidentiran u OIB sustavu.
Kratki naziv	Uobičajeni kratki naziv institucije koji je u upotrebi ako postoji. Trebao bi odgovarati skraćenom nazivu institucije evidentiranom u OIB sustavu. Npr. Središnji registar osiguranika -> Regos.
DN certifikata	DN (Distinguished Name)certifikata institucije koji će se koristiti za slanje poruka. Budući da postoje dvije okoline (test i produkcija) u kojima se koriste različiti certifikati sukladno Tehničkoj specifikaciji trebati će dostaviti DN-ove oba certifikata, prvo za testnu okolinu, a zatim i za produkcijsku okolinu.
Okolina	TEST ili PROD
Kontakt osoba	Ime prezime, email, telefon.

8.1.2 Podaci koji će biti dodijeljeni instituciji za slanje poruka u OKP

	Napomena
ID u Sustavu za zaprimanje poruka	ID koji će biti dodijeljen instituciji u Sustavu za zaprimanje poruka. Institucija će koristiti podatak pri izradi XML poruke zahtjeva u elementu „SenderId“.
ID u Osobnom korisničkom pretincu	ID koji će biti dodijeljen instituciji u Osobnom korisničkom pretincu. Institucija će koristiti podatak pri izradi XML poruke zahtjeva u elementu „IdPosiljatelja“.
ID usluge	ID koji je definiran za uslugu „Osobni korisnički pretinac“. Institucija će koristiti podatak pri izradi XML poruke zahtjeva u elementu „ServiceId“.

8.2 Registracija e-poruka u sustavu OKP

Institucija mora dostaviti skup određenih podataka (**OKP - Obrazac za pošiljatelja e-poruke**), propisan od strane Ministarstva uprave. Nakon što su podaci dostavljeni i zahtjev se obradi, institucija dobiva od strane Ministarstva uprave povratnu informaciju - **Tip poruke registriran u Registru e-poruka**.

Institucija će taj podatak koristiti prilikom izrade XML poslovne poruke zahtjeva za Osobni korisnički pretinac u elementu „TipPoruke“.

NAPOMENA: Podatak u elementu „TipPoruke“ usko je vezan za naslov (element „Predmet“) i sadržaj poruke (element „Sadržaj“). Zbog toga, nije dozvoljena izmjena tih podataka na način da se bitno izmijeni bit.

8.2.1 Podaci koje treba dostaviti institucija prije slanja nove e-poruke u OKP

Za proceduru prijave nove e-poruke potrebno je da se institucija s popunjenim podacima u obrascu **OKP - Obrazac za pošiljatelja e-poruke** obratiti Ministarstvu uprave.

8.2.2 Podaci koji će biti dodijeljeni instituciji za slanje nove e-poruke u OKP

	Napomena
Tip e-poruke registriran u Registru e-poruka	ID koji će biti dodijeljen pojedinačnom tipu e-poruke u Sustavu za zaprimanje poruka. Institucija će koristiti podatak pri izradi XML poslovne poruke zahtjeva u elementu „TipPoruke“

8.3 Dohvat podataka za slanje (ili personalizaciju) e-poruka

Servis Dohvat podataka za slanje e-poruka zamijeniti će listu OIB-ova građana, koja je opisana u poglavlju 8.5. *Dostava liste OIB-ova korisnika koji imaju otvoreni OKP.*

Preporuka za svaku instituciju – Pošiljatelja je da prije slanja e-poruka u OKP, putem servisa Dohvat podataka o personalizaciji e-poruka napravi provjeru.

Instituciji (Pošiljatelju) su na taj način dostupni podaci o:

- listi korisnika OKP-a koji žele od Pošiljatelja primati točno određeni tip e-poruke ili
- provjera da li pojedini korisnik OKP-a želi primati točno određeni tip e-poruke od Pošiljatelja.

Ako je korisnik OKP-a registriran u sustavu, u odgovoru će biti vraćen OIB korisnika + OznakaDrzave korisnika.

8.3.1 Postupak upita u servis za Dohvat podataka o personalizaciji e-poruka

Kao i prilikom slanja poruka u OKP, institucija kreira poruku prema dogovorenoj shemi koju propisuje Sustav za zaprimanje poruka. Poruka koja se šalje u sustav za zaprimanje poruka je opisana u poglavlju 2.3.1.

U polje <ServiceId> poruke koja se šalje u Sustav za zaprimanje poruka potrebno je upisati šifru usluge **124**.

```
<tns:ServiceId>124</tns:ServiceId>
```

Poslovnu poruku za upit u servis za Dohvat podataka o personalizaciji e-poruka institucija kreira prema dogovorenoj shemi. Poruka koja se šalje u servis za Dohvat podataka o personalizaciji e-poruka opisana je u poglavlju 8.3.2.

8.3.2.2 Primjer poslovne poruke ZAHTJEVA provjere da li pojedini korisnik OKP-a želi primiti točno određeni tip e-poruke od Pošiljatelja

```
<?xml version="1.0"?>
<GSBOvojnica xmlns:tns="http://apis-it.hr/umu/2015/types/kp">
  .
  .
  .
  <tns:GsbIdPosiljatelja>1</tns:GsbIdPosiljatelja>
  <tns:Upit>
    <tns:IdPosiljatelja>1</tns:IdPosiljatelja>
    <tns:TipPoruke>1</tns:TipPoruke>
    <tns:IdUpita>732262f1-063f-11e2-892e-0812200c9a68</tns:IdUpita>
    <tns:PinCountryCodeId>
      <tns:CountryCodeId>HR</tns:CountryCodeId>
      <tns:PinPrimatelja>45572228924</tns:PinPrimatelja>
    </tns:PinCountryCodeId>
    <tns:DatumVrijemeUpita>2015-03-
26T23:12:29.371+01:00</tns:DatumVrijemeUpita>
  </tns:Upit>
  .
  .
  .
</GSBOvojnica>
```

8.3.3 Poslovna poruka ODGOVORA s provjerom/dohvatom podataka o personalizaciji e-poruka (za točno određeni tip e-poruke)

Polje	Obavezan	Opis / Napomena
ZAGLAVLJE (obavezno jedan zapis)		
GsbIdPosiljatelja	DA	Prepisano iz zahtjeva
IdPosiljatelja	DA	Prepisano iz zahtjeva
TipPoruke	DA	Prepisano iz zahtjeva
IdUpitaPosiljatelja	DA	Prepisano iz zahtjeva
DatumVrijemeObrade	DA	Datum i vrijeme obrade zahtjeva u sustavu OKP
SifraGreske	DA, ako ima grešaka	Šifra greške prema šifarniku grešaka.
OpisGreske	DA, ako ima grešaka	Šifra greške prema šifarniku grešaka.
LISTA OIB-ova (0 ili više zapisa)		
PinsCcIdsAsXmlZipBase64	NE	XML datoteka koja je zipana i Base64 enkodirana
PinPrimatelja	NE	Ako postoji korisnik koji želi primiti TipPoruke -> Za hrvatske građane – OIB (samo jedan korisnik)
OznakaDrzave	NE	Ako postoji korisnik koji želi primiti TipPoruke -> Za hrvatske građane oznaka 'HR', inače oznaka države prema šifarniku.
EmptyData	NE	U slučaju da je lista OIB-ova prazna tj. da ne postoji niti jedan korisnik koji želi primiti navedeni tip poruke -> 'Za navedeni tip poruke nema pretplatnika u sustavu OKP.' U slučaju da je poslana provjera za 1 OIB -> 'Korisnik nije pretplaćen za navedeni tip poruke.'

8.3.3.1 Primjer poslovne poruke ODGOVORA za provjerom/dohvatom podataka o personalizaciji e-poruka

```
<GSBOvojnica>
.
.
.
<Odgovor xmlns:a="http://apis-it.hr/umu/2015/types/kp">
    <a:EmptyResultSet>Nema podataka za zatrazeni broj
stranice!</a:EmptyResultSet>
    <a:IdUpitaPosiljatelja>732262f1-063f-11e2-892e-
0812200c9a68</a:IdUpitaPosiljatelja>
    <a:DatumVrijemeObrade>2016-06-
02T16:41:27.389+02:00</a:DatumVrijemeObrade>
    </Odgovor>
.
.
.
</GSBOvojnica>
```

8.3.3.2 Primjer poruke zahtjeva s GSB ovojnicom

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tns="http://apis-it.hr/umu/2015/types/kp" xmlns:gsb="http://apis-
it.hr/umu/2013/types/gsb">
  <soapenv:Header/>
  <soapenv:Body>
    <gsb:SendMessageRequest>
      <gsb:GsbEnvelope>
        <gsb:MessageHeader>
          <gsb:SenderId>1</gsb:SenderId>
          <gsb:ServiceId>124</gsb:ServiceId>
          <gsb:MessageId>c4413331-1cff-11e2-f516-242d656ac4b3</gsb:MessageId>
          <gsb:SenderTimeStamp>2015-05-31T12:00:01</gsb:SenderTimeStamp>
        </gsb:MessageHeader>
        <gsb:Content>
          <gsb:MimeType>aa5</gsb:MimeType>
          <gsb:Data encoding="EMBEDDED">
            <tns:GsbIdPosiljatelja>1</tns:GsbIdPosiljatelja>
            <tns:Upit>
              <tns:IdPosiljatelja>1</tns:IdPosiljatelja>
              <tns:TipPoruke>1</tns:TipPoruke>
              <tns:IdUpita>732262f1-063f-11e2-892e-0812200c9a68</tns:IdUpita>
              <tns:BrojStranice>0</tns:BrojStranice>
              <tns:DatumVrijemeUpita>2015-03-
26T23:12:29.371+01:00</tns:DatumVrijemeUpita>
            </tns:Upit>
          </gsb:Data>
        </gsb:Content>
      </gsb:GsbEnvelope>
    </gsb:SendMessageRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

8.3.3.3 Primjer poruke odgovora s Gsb ovojnicom

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <tns:SendMessageResponse xsi:schemaLocation="http://apis-it.hr/umu/2013/types/gsb
GSBSchema.xsd " xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:tns="http://apis-it.hr/umu/2013/types/gsb">
      <tns:MessageHeader>
        <SenderId xmlns="http://apis-it.hr/umu/2013/types/gsb">1</SenderId>
        <ServiceId xmlns="http://apis-it.hr/umu/2013/types/gsb">124</ServiceId>
        <MessageId xmlns="http://apis-it.hr/umu/2013/types/gsb">c4413331-1cff-11e2-
f516-242d656ac4b3</MessageId>
        <GsbId xmlns="http://apis-it.hr/umu/2013/types/gsb">3b9f5a09-6096-41fd-9ebd-
315e858d568b</GsbId>
        <SenderTimeStamp xmlns="http://apis-it.hr/umu/2013/types/gsb">2015-05-
31T12:00:01</SenderTimeStamp>
        <ReceivingTimeStamp xmlns="http://apis-it.hr/umu/2013/types/gsb">2016-06-
02T16:45:09</ReceivingTimeStamp>
        <ForwardingTimeStamp xmlns="http://apis-it.hr/umu/2013/types/gsb">2016-06-
02T16:45:10</ForwardingTimeStamp>
        <ReceiverTimeStamp xmlns="http://apis-it.hr/umu/2013/types/gsb">2016-06-
02T16:45:12</ReceiverTimeStamp>
        <ReplyReceivingTimeStamp xmlns="http://apis-it.hr/umu/2013/types/gsb">2016-
06-02T16:45:12</ReplyReceivingTimeStamp>
        <ReplyForwardingTimeStamp xmlns="http://apis-it.hr/umu/2013/types/gsb">2016-
06-02T16:45:12</ReplyForwardingTimeStamp>
      </tns:MessageHeader>
      <tns:Content>
        <tns:MimeType>text/xml</tns:MimeType>
        <tns:Data encoding="EMBEDDED">
          <Odgovor xmlns:a="http://apis-it.hr/umu/2015/types/kp">
            <a:PinsCcIdsAsXmlZipBase64>UEsDBBQACAAIAKWFW.....</a:PinsCcIdsAsXmlZipBase64>
              <a:IdUpitaPosiljatelja>732262f1-063f-11e2-892e-
0812200c9a68</a:IdUpitaPosiljatelja>
              <a:DatumVrijemeObrade>2016-06-
02T16:45:10.424+02:00</a:DatumVrijemeObrade>
            </Odgovor>
          </tns:Data>
        </tns:Content>
      </tns:SendMessageResponse>
    </soapenv:Body>
  </soapenv:Envelope>
```

8.3.3.4 Napomene pri korištenju servisa

Prilikom dohvata svih oib-ova po elementu TipPoruke, koristi se straničenje cijelog skupa podataka, tj. skup podataka se dijeli na N stranica, a svaka stranica ima maksimalno po 50000 PinCountryCodeId-ova.

Stranica je u biti XML datoteka koja je zipana i Base64 enkodirana - PinsCcIdsAsXmlZipBase64 element.

Da bi se dohvatio cijeli skup podataka servis je potrebno pozvati N+1 puta i pri svakom pozivu inkrementirati element BrojStranice za 1 (počinje od 0). Servis je potrebno tako zvati sve dok se u Odgovoru ne dobije poruka <a:EmptyResultSet>Nema podataka za zatraženi broj stranice!</a:EmptyResultSet>.

8.4 Šifrnik grešaka

Šifra	Poruka
L001	Zahtjev nije ispravan prema XML shemi.
L002	Datum i vrijeme navedeni u poruci nisu formalno i/ili logički ispravni.
L003	Za navedeni IdPosiljatelja nije registriran navedeni TipPoruke.
L004	Navedeni IdPosiljatelja ne postoji u Registru pošiljatelja.
L005	Sistemska pogreška.
L006	ID GSB pošiljatelja ne odgovara onom iz poruke!
L007	OIB iz poruke nije formalno ispravan.
L008	Neispravna vrijednost za podatak 'Oznaka države'.
L009	OIB iz poruke nema aktivan Korisnički pretinac.

8.5 Dostava liste OIB-ova korisnika koji imaju otvoreni OKP

Ukoliko institucija želi, može dohvatiti listu OIB-ova građana koji imaju otvoreni Osobni korisnički pretinac. Listu je moguće dohvatiti u dvije okoline, testnoj i produkcijskoj. Lista u testnoj okolini sadrži testne podatke.

Lista će svakog dana u 9:00 (devet sati ujutro) biti osvježena s novim podacima.

NAPOMENA: stari način dostave liste OIB-ova NIJE ukinut, te se do daljnjega može koristiti!

Preporuka je da nove institucije prilikom uključanja u sustav počnu s korištenjem servisa za Dohvat podataka za slanje e-poruka , dok institucije uključene u projekt trebaju napraviti zamjenu i implementirati korištenje servisa za Dohvat podataka za slanje e-poruka.

Lista OIB-ova će biti ukinuta u času uključanja funkcionalnosti personalizacije zaprimanja e-poruka i od tada će biti dostupan biti samo servis za Dohvat podataka za slanje e-poruka

8.5.1 Mrežni preduvjeti

Za dostavu liste OIB-ova klijentski sustav mora zadovoljiti sljedeće mrežne preduvjete:

Vrsta mreže	Internet, Hitronet
Potrebni otvoreni TCP port-ovi	8444
Adresa pristupnog poslužitelja u testnoj okolini	https://demo.apis-it.hr:8444/kpoib/kp_lista_aktiviranih_korisnika.txt
Adresa pristupnog poslužitelja u produkcijskoj okolini	https://e-biz.apis-it.hr:8444/kpoib/kp_lista_aktiviranih_korisnika.txt

8.5.2 Sigurnosni preduvjeti

Komunikacija je zaštićena sa 2-way TLS-om sa poslužiteljskim certifikatom za terminaciju TLS-a s autentikacijom klijenta. Taj mehanizam onemogućava nepoznatim stranama spajanje na pristupnu točku, a ujedno se poslužitelj za dohvat liste predstavlja klijentima.

U produkcijskoj i testnoj okolini sustav se predstavlja klijentu TLS certifikatom izdanim od Verisign CA.

Klijenti se poslužiteljskom sustavu mogu predstaviti certifikatima koje koriste i za spajanje na Sustav za zaprimanje poruka u KP.

9. Popis priloga

Kao prilozi ovom dokumentu dolaze datoteke:

1. „Korisnički pretinac-WSDL v1.2.zip“.
-nalazi se WSDL i XML schema
2. „Primjeri poruka v1.2.zip“
-primjeri poruka zahtjeva i odgovora za Sustav za razmjenu poruka
-primjeri poruka zahtjeva i odgovora za Korisnički pretinac
3. „KP Kompletna poruka v1.2.zip“
„Primjer kompletne poruke zahtjeva sa prilogom“
4. „Dohvat podataka o personalizaciji ePoruka v1.2.zip“
-nalazi se WSDL i XML schema
5. „OKP - Često postavljena pitanja i odgovori.doc“