MINISTARSTVO FINANCIJA
POREZNA UPRAVA
www.porezna-uprava.hr

Tehnički standardi i specifikacija povezivanja - Pristupna točka i standardni AS4 profil

Financira Europska unija – NextGenerationEU

SADRŽAJ:

1. RJEČNIK SKRAĆENICA I POJMOVA

Pojam	Skraćenica
AS4	Aplicability Statement 4, standard koji opisuje prijenos poruka putem web servisa
BDXL	OASIS Business Document Metadata Service Location (BDX Location)
SML	Service Metadata Locator
BDX-SMP	OASIS Business Document Service Metadata Publisher
PKI	Public Key Infrastructure – infrastruktura javnog ključa
XML	Extensible Markup Language – standard za elektroničke strukturirane dokumente
SOAP	Simple Object Access Protocol – protokol za razmjenu podataka putem web servisa
HTTP	Hypertext Transfer Protocol
CA	Certification Authority – servis za upravljanje digitalnim X.509 certifikatima (vjerodajnicama)
ebMS	ebXML Messaging Services – bazni standard na kojem je baziran eDelivery AS4 profil
AMS	Adresar Metapodatkovnih Servisa
PT	Pristupna točka
MPS	Metapodatkovni servis
ID	Identifikator sudionika
IP	Informacijski posrednik

Tablica 1 – Rječnik skraćenica i pojmova

2. UVOD

Kako bi osigurali nesmetanu komunikaciju u razmjeni eRačuna, između pristupnih točaka u RH koje koriste različita tehnička rješenja, odabran je AS4 profil. Ovaj dokument opisuje tehničke standarde i specifikaciju implementacije pristupne točke (PT) te definira AS4 profil (eRačun-AS4) i njegovu implementaciju za potrebe razmjene eRačuna. Implementacija mora slijediti CEF eDelivery AS4 Profile v1.15 i aspekte opisane u ovom dokumentu kojima se dodatno definiraju i ograničavaju značajke i atributi koji nisu profilirani u specifikaciji CEF-a ili su neobvezni i ne upotrebljavaju se. Osim same razmjene poruka korištenjem AS4 protokola svaka implementacija PT mora podržati i proces lociranja pristupne točke primatelja odnosno pristupne točke na koju se radi isporuka eRačuna.

Kompletan model razmjene eRačuna definiran je ovim dokumentom tehničke specifikacije zajedno sa sljedećim dokumentima:

- *Tehnički standardi i specifikacije povezivanja – Adresar metapodatkovnih servisa (AMS)*
- *Tehnički standardi i specifikacije povezivanja – Metapodatkovni servis (MPS).*

AS4 rješenje ima sljedeće značajke:

- Svaka pristupna točka mora osigurati AS4 protokol kao standard za razmjenu eRačuna i ne smije odbiti poruku koja dolazi putem tog standarda
- AS4 protokol je tehničko rješenje koje omogućava jednoznačnu komunikaciju između pristupnih točaka koje koriste različita tehnička rješenja za samu razmjenu eRačuna
- Na ovaj način više nisu neophodne međusobne integracije između pojedinih pristupnih točaka i prilagodbe njihovih tehničkih rješenja za razmjenu eRačuna
- Ovakav način osigurava da svaka PT zna komunicirati sa svakom PT, ali ne ograničava međusobnu integraciju pojedinih pristupnih točaka na način koji je njima najprihvatljiviji
- Ovim standardom je osigurana sigurna i strukturirana razmjena eRačuna
    - Sigurnost je postignuta korištenjem certifikata i potpisivanjem poruka, a poruka je strukturirana u XML formatu.

3. ČETVEROKUTNA TOPOLOGIJA

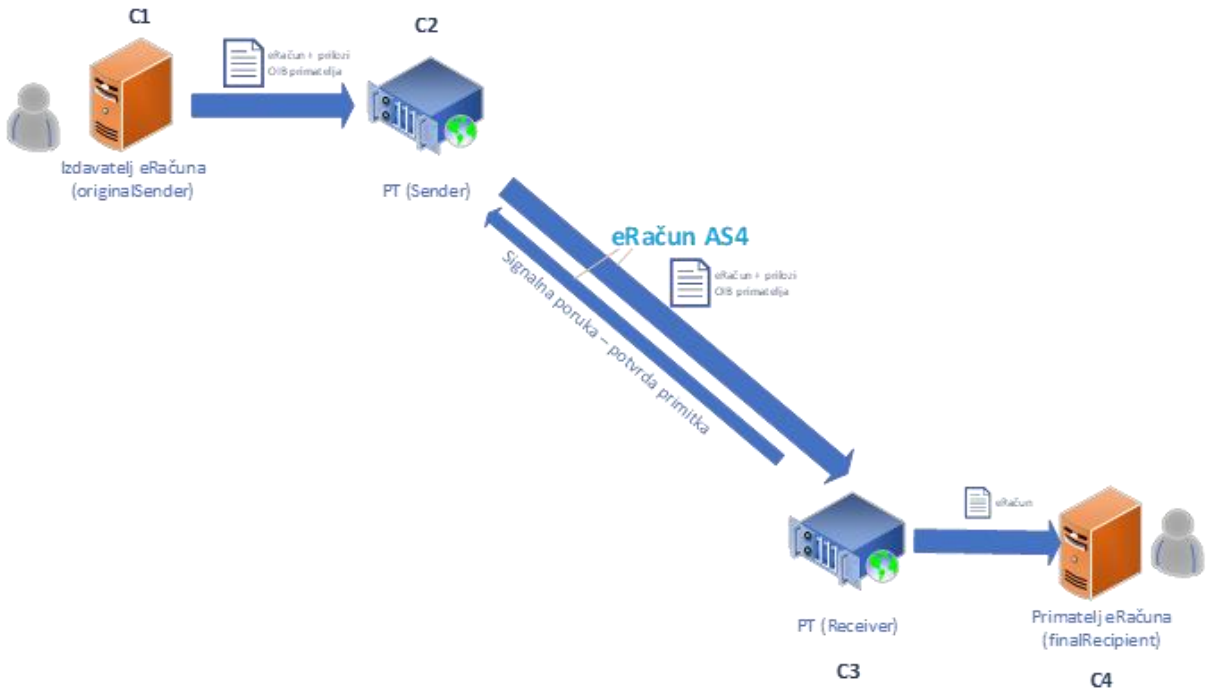
Scenarij razmjene eRačuna podrazumijeva situacije u kojima pristupne točke razmjenjuju poruke u ime drugih strana pa je definiran model razmjene eRačuna koji je baziran na četverokutnoj topologiji (eng. *Four corner topology*) u kojoj postoje četiri uključene strane, od kojih su dvije izvorni izdavatelj i krajnji primatelj eRačuna, a druge dvije strane su pristupne točke koje usmjeravaju poruke od izvornog izdavatelja prema krajnjem primatelju i poruke odgovora (potvrde ili greške) u drugom pravcu.

Specifikacije OASIS ebMS3 i AS4 služe za razmjenu poruka od točke do točke između dva servisa za razmjenu poruka (MSH). Međutim, kako je navedeno u uvodu ovog dokumenta, eRačun AS4 protokol namijenjen je upotrebi u situacijama u kojima pristupne točke razmjenjuju poruke u ime drugih strana. Četiri strane uobičajeno se nazivaju oznakama Cn, pri čemu C označava „kut" i n je jedna od znamenki od 1 do 4:

- C1 je originalni Izdavatelj.
- C2 je pristupna točka koja šalje poruke u ime C1.
- C3 je pristupna točka koja prima poruke u ime C4.
- C4 je krajnji Primatelj.

Budući da se zajednički profil primjenjuje na razmjenu C2-C3, razmjena uključuje AS4 Push slanje od C2 kao inicijatora do C3. Razmjene između C1-C2 i C3-C4 nisu obavezne koristiti AS4 protokol i nisu obuhvaćene ovom specifikacijom.

Atribut pod nazivom **trackingIdentifier** dodaje se poruci kako bi bio identifikator (u proizvoljnom formatu) koji omogućuje praćenje poruka s kraja na kraj u razmjeni s četiri kuta. Njegova vrijednost može se postaviti na vrijednost identifikatora poruke od C1 do C2 na koju se odnosi poruka AS4. To omogućuje praćenje poruka i rješavanje eventualnih problema.



Slika 1. Četverokutna topologija

3.1. ADRESIRANJE, IDENTIFIKACIJA SUDIONIKA, IDENTIFIKATOR ZA PRAĆENJE

Ovim opisanim načinom definira se upotreba sustava eRačun AS4 u četverokutnim razmjenama poruka. Njime se definiraju konvencije za upotrebu zaglavlja poruka ebMS3 i konfiguracija odgovarajućih parametara načina obrade.

U scenarijima u kojima se AS4 upotrebljava za komunikaciju između krajnjih subjekata, **eb:From** i **eb:To** zaglavlja na **eb:usermessage/eb:PartyInfo** identificira se Izdavatelj i Primatelj. Kako bi se olakšala uporaba neizmijenjenih implementacija AS4 poruka i pojednostavnila konfiguracija pružatelja usluga AS4 poruka, **eb:From/eb:PartyId** i **eb:To/eb:PartyId** moraju identificirati unutarnje pristupne točke.

Da bi se mogla preusmjeriti primljena poruka, pristupna točka izdavatelja (C2) mora moći odrediti krajnjeg primatelja (C4). Te su informacije općenito dostupne u strukturiranim porukama. Međutim, korištenje informacija iz strukturiranih poruka pretpostavlja razumijevanje sheme na kojoj se temelji strukturirana poruka. Kako bi se pristupnim točkama omogućila obrada strukturiranih poruka bilo koje vrste, poželjno je usvojiti mehanizam koji je neovisan o određenim shemama. Nadalje, u nekim situacijama može postojati zahtjev za usmjeravanje nestrukturiranih ili šifriranih podataka. Stoga se ovdje upotrebljava mehanizam atributa ebMS3 za identifikaciju C1 i C4. Mehanizam atributa omogućuje korištenje proizvoljnih parova atributa i vrijednosti u AS4 poruci i neovisan je o formatu ili strukturi poruke.

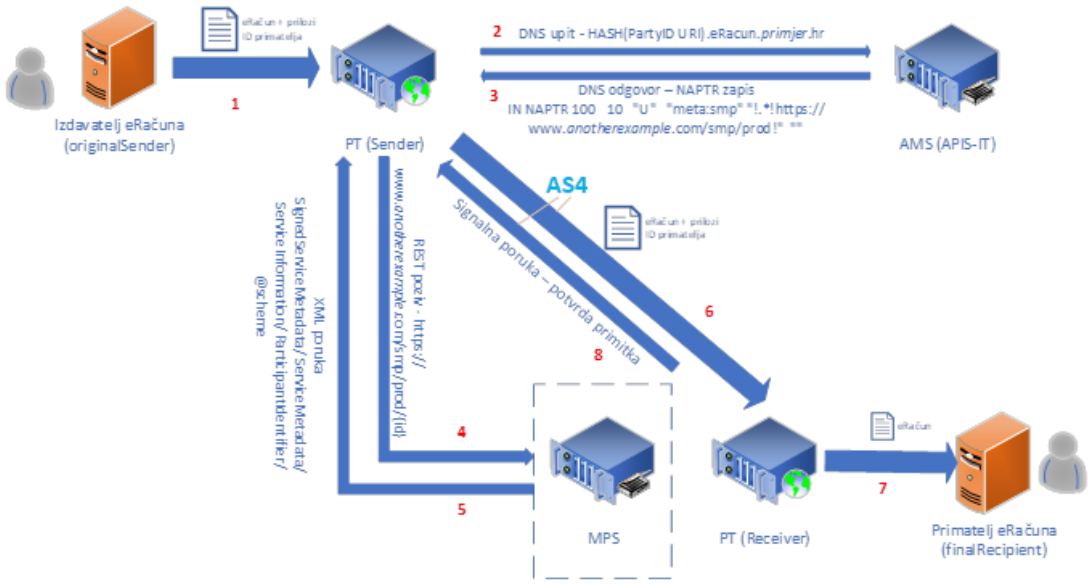
Kada se koristi u topologiji četiri kuta:

- Atribute nazvan **originalSender** mora se dodati poruci koja identificira izvornog izdavatelja (C1)
- Atribut nazvan **finalRecipient** mora se dodati poruci koja identificira stranu konačnog primatelja (C4).

Kao i kod **eb:From/eb:PartyId** i **eb:To/eb:PartyId** zaglavlja, atribut tipa može se koristiti s ova dva svojstva za kategorizaciju tipova identifikatora. Kao identifikacijski sustav i format za adresiranje, oznaka ISO 6523 mora se upotrebljavati za tipove registrirane u normi ISO 6523 i format identifikacijske oznake ebCore trebao bi se upotrebljavati kako je navedeno u [eDelivery-EBCORE].

4. OSNOVNI MODEL RAZMJENE ERAČUNA

Osnovni (pretpostavljeni) mehanizam slanja i primanja eRačuna između pristupnih točaka korištenjem protokola i specifikacija definiranih u ovom dokumentu je dan na sljedećoj slici.



Slika 2. Osnovni model razmjene eRačuna

Osnovni koraci slanja eRačuna između izdavatelja i primatelja:

1. Izdavatelj izdaje eRačun i dostavlja ga do pristupne točke – ili odabranom informacijskom posredniku ili ako ne koristi usluge informacijskog posrednika prosljeđuje račun iz modula/aplikacije u kojem izdaje eRačune u modul/aplikaciju za slanje eRačuna. Način komunikacije i protokoli prijenosa podataka u ovom koraku procesa nisu predmet ove specifikacije. Osim eRačuna koji sadrži sve obavezne elemente i eventualne priloge, podatak koji pristupna točka mora imati da bi mogla proslijediti eRačun je identifikator (ID) krajnjeg primatelja.
2. Pristupna točka Izdavatelja kontaktira AMS servis putem DNS upita formatiranog na definirani način (specificirano u dokumentu Tehnička specifikacija - AMS).
3. AMS servis šalje odgovor na upit u obliku N-APTR zapisa koji sadrži URL adresu metapodatkovnog servisa (MPS) kod kojeg je registriran primatelj eRačuna.
4. Pristupna točka Izdavatelja kontaktira MPS na dobiveni URL putem REST konekcije kojom šalje identifikator primatelja (i opcionalno druge identifikatore) i traži krajnju adresu Primatelja.
5. MPS vraća URL pristupne točke primatelja na koju se može isporučiti eRačun.
6. Pristupna točka izdavatelja kontaktira pristupnu točku primatelja, otvaranjem HTTPS konekcije na dobiveni URL. Nakon uspostave konekcije postavlja se AS4 konekcija prema definiranim parametrima (P-mode), te se šalje eRačun sa prilozima zapakiran u AS4 poruku.
7. Pristupna točka primatelja zaprima AS4 poruku sa eRačunom, te na temelju atributa u zaglavlju poruke (finalRecipient) koja sadrži ID primatelja prosljeđuje poruku do krajnjeg primatelja.
8. Ako je poruka uspješno obrađena i proslijeđena krajnjem primatelju, pristupna točka primatelja šalje potpisanu signalnu poruku s potvrdom primitka pristupnoj točki Izdavatelja. Ako pristupna točka primatelja ne poslužuje navedenog primatelja ili zaprimljeni sadržaj nije sukladan ili obrada zaprimljenog računa nije uspjela zbog greške, pristupnoj točki izdavatelja se šalje poruka o grešci.

5. STANDARDNI AS4 PROFIL ZA RAZMJENU ERAČUNA

Ovaj profil, eRačun-AS4, koristi se kod razmjene eRačuna za prijenos asinkronih poruka između kuta 2 (C2) i kuta 3 (C3) u četverokutnoj topologiji koristeći PKI metodu za potpis AS4 poruke. Profil eRačun-AS4 predstavlja minimalni standard kojeg svaka pristupna točka uključena u procese razmjene eRačuna u RH mora podržati za izdavanje i zaprimanje eRačuna. Sukladno tome, pristupna točka ne smije odbiti zaprimiti eRačun kojeg druga strana u ime izdavatelja eRačuna želi poslati korištenjem eRačun-AS4 profila. Isto tako, prilikom slanja eRačuna pristupna točka ne smije od druge strane koja zaprima eRačun u ime krajnjeg primatelja tražiti profil širi ili drugačiji od eRačun-AS4 profila kao preduvjet za izdavanje eRačuna.

5.1. BAZNA SPECIFIKACIJA

Osnovni tehnički parametri prijenosa za potrebe razmjene eRačuna su u sljedećoj tablici:

Core Messaging	Web Services
Exchange Pattern Bindings	Push
Exchange Patterns	One Way
Internet Transport	HTTP 1.1
Message and Payload Packaging	SOAP 1.2 with attachments
Message Confidentiality	WS-Security 1.1 bez korištenja XML Encryption
Message Correlation	ebMS 3.0 "ConversationId"
Message Identification	ebMS 3.0 "MessageId"
Message Timestamp	ebMS 3.0 "Timestamp" i WS-Security "Timestamp"
Non-Repudiation of Origin	WS-Security 1.1 korištenjem XML Signature (XAdES)
Non-Repudiation of Receipt	Signed Receipt Signal Message
Party Identification	ebMS 3.0 "From" i "To" identifikatori strana u komunikaciji.
Payload Compression	Gzip (**)
Reliable Message	AS4 reception awareness feature for lightweight, interoperable reliable messaging
Routing and Dispatching, SOA integration	Obavezni "Service" i "Action" elementi zaglavlja
Transport Layer Integrity, Sender Authentication, Receiver Authentication and Message Confidentiality (Non-Persistent)	Transport Layer (SSL / TLS) Security

Tablica 2 – Bazna specifikacija

Okvirni pregled izmijenjenih funkcionalnosti u eRačun-AS4 specifikaciji u odnosu na osnovni CEF eDelivery AS4 profil:

Funkcionalnost	eRačun-AS4	CEF eDelivery AS4
Obrazac razmjene (eng. *Exchange Patterns*)	One Way	One Way ili Two Way

Prijenos obrasca razmjene (eng. *Exchange Pattern Bindings*)	Push	Push, Pull i Sync
Povezivanje poruka (eng. *Message Correlation*)	ebMS 3.0 "ConversationId"	ebMS 3.0 "RefToMessageId" i "ConversationId"

Tablica 3 – Pregled funkcionalnosti u eRačun-AS4

Obrazac razmjene (MEP) **One-Way/Push** je jedini koji mora biti podržan od strane svih sudionika u procesu razmjene eRačuna u RH i pretpostavljeni obrazac se koristi u svim prijenosima.

5.2. KONFIGURACIJA SIGURNOSTI U PRIJENOSU – TRANSPORT LAYER SECURITY (TLS)

Pristupne točke koje su dio eRačun mreže ne razmjenjuju informacije povezane s IP adresama i portovima unaprijed za prijenos poruka kako je opisano u [CEFeDeliveryAS4].

U eRačun mreži pristupna točka mora biti konfigurirana u skladu sa sljedećim:

- Pristupna točka primatelja mora podržavati TLS u skladu s odjeljkom 3.2.6. CEF eDelivery AS4 (https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eDelivery+AS4+-+1.15).
- Verzije novije od TLS v1.2 mogu se koristiti nakon međusobnog dogovora putem TLS *handshake* procesa.
- Port 443 se uvijek koristiti za TLS.
- Pristupne točke izdavatelja moraju omogućiti samo izlazne prijenose na portu 443.
- TLS mora koristiti valjani certifikat u skladu s politikom za sigurnost i izdan od strane ovlaštenog izdavatelja (CA) u Republici Hrvatskoj.

5.3. SPORAZUM

Budući da se razmjena poruka između dviju pristupnih točaka u mreži eRačuna temelji na sporazumu **hrAgreement**, parametar **PMode.Agreement** koji se koristi za označavanje poslovnog sporazuma kojim se uređuje razmjena poruka mora imati vrijednost `urn:fdc:eracun.hr:2023:agreements:ap_provider`. Referenca na sporazum je uključena u **eb3:AgreementRef** element ebMS zaglavlja poruke.

5.4. POVRATNA INFORMACIJA U SLUČAJEVIMA NEPOSTOJEĆEG PRIMATELJA ILI NEISPRAVNE AS4 PORUKE

Pristupna točka validira sadržaj korisničke poruke tijekom ebMS obrade, što uključuje provjeru primatelja, identifikacijsku oznaku vrste dokumenta i identifikacijsku oznaku postupka, te provjeru formalne ispravnosti

sadržaja prema propisanoj normi. Ako PT ne pruža krajnjem primatelju uslugu zaprimanja eRačuna ili ako bilo koja od drugih formalnih provjera nije zadovoljena mora generirati i poslati ebMS poruku o pogrešci.

Atribut pogreške kod generirane Error poruke mora biti postavljen na EBMS:0004 (Ostala pogreška), a njegov atribut kritičnosti mora biti postavljen na neuspjeh (*failure*).

Nadalje, atribut errorDetail ima vrijednost ovisno o detektiranoj grešci:

- ERACUN:NOT_SERVICED kako bi se naznačilo da pristupna točka ne pruža uslugu adresiranom primatelju.
- ERACUN:VALIDATION_ERROR kako bi se naznačilo da je došlo do greške prilikom validacije sadržaja.

5.5. IDENTIFIKACIJA SUDIONIKA

P-Mode	Vrijednost
PMode.Initiator.Party	Jedan PartyId sa vrijednosti Subject CNAME iz certifikata pristupne točke, npr. HR11111111111 (u formatu HR<OIB>) Fiksna vrijednost za Party.type: urn:fdc:eRacun.hr:2023:identifiers:ap
PMode.Initiator.Role	Fiksna vrijednost: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator
PMode.Responder.Party	Jedan PartyId sa vrijednosti Subject CNAME iz certifikata pristupne točke, npr. HR11111111111 (u formatu HR<OIB>) Fiksna vrijednost za Party.type: urn:fdc:eRacun.hr:2023:identifiers:ap
PMode.Responder.Role	Fiksna vrijednost: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder

Tablica 4– Identifikacija sudionika

5.6. SERVIS, ULOGA I AKCIJA

Prilikom slanja eRačuna pristupna točka mora definirati PMode prema predloženoj tablici.

P-Mode	Vrijednost

PMode[1].BusinessInfo.Service	Predefinirana vrijednost identifikatora procesa za slanje eRačuna - **hrBillingService**. Vrijednost: `urn:fdc:eracun.hr:2023:processId`
PMode[1].BusinessInfo.Service.type	Predefinirana vrijednost sheme identifikatora procesa za slanje eRačuna. Primjer: cenbii-procid-ubl

PMode[1].BusinessInfo.Action	Predefinirana vrijednost identifikatora tipa dokumenta za eRačun formatirana po slijedećem:
	«scheme id»::«document type id value»
	
	Definirana su dva tipa:
	
	hrBillingInvoiceAction -
	
	`busdox-docid-qns::urn:oasis:names:specification:ubl:schema:xsd:Invoice-2::Invoice##urn:cen.eu:en16931:2017#compliant#urn:fdc:peppol.eu:2017:poacc:billing:3.0::2.1`
	
	hrBillingCreditNoteAction –
	
	`busdox-docid-qns::urn:oasis:names:specification:ubl:schema:xsd:CreditNote-2::CreditNote##urn:cen.eu:en16931:2017#compliant#urn:fdc:peppol.eu:2017:poacc:billing:3.0::2.1`
	
	Napomena: Ne smije se koristiti URL enkodiranje korištenjem znaka „%“ (eng. *URL percent-encoding*).

Tablica 5 – Servis, akcija i uloga

5.7. KORIŠTENJE PKI

Sva komunikacija u mreži eRačuna koristi kvalificirane X.509 certifikate izdane od pouzdanog izdavatelja i taj certifikat mora imati naveden OIB PT-a kao jedan od atributa. Certifikati koji ne udovoljavaju ovim uvjetima se ne smiju koristiti.

P-Mode	Vrijednost
PMode[].Security.X509.Signature.Certificate	Certifikat pristupne točke pošiljatelja

PMode[].Security.X509.Encryption.Certificate	Ne koristi se

Tablica 6 – Korištenje PKI

Zbog dinamičke prirode razmjene certifikata u mreži eRačun, tip „Binary Security Token" se mora upotrebljavati kao tip identifikatora ključa.

Kod razmjene eRačuna ne koristi se enkripcija na nivou AS4 poruke.

5.8. KORIŠTENJE ZADANOG MPC

Koristi se zadani MPC, tj. PMode[1].BusinessInfo.MPC koji se mora postaviti na:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC

5.9. KORIŠTENJE SBDH

Svi prijenosi podataka u mreži eRačuna moraju imati sadržaj zapakiran kao integralni element koristeći SBDH (*Standard Business Document Header*). SBDH je integralni dio XML dokumenta (eRačun) koji je zapakiran u jedan MIME privitak. Nije dozvoljeno korištenje izdvojenog (*eng. Standalone*) SBDH. SBDH element koji sadrži poslovnu poruku mora biti prvi MIME privitak nakon MIME privitka koji sadrži AS4 zaglavlje.

5.9.1. IDENTIFIKATORI SUDIONIKA

Obavezni identifikator primatelja (*sh:Receiver)* u ovojnici poruke mora odgovarati sudioniku koji je registriran u AMS/MPS servisu (tj. C4). Također, identifikator Izdavatelja (*sh:Sender*) je obavezan i označava sudionika C1. Struktura identifikatora mora slijediti pravila definirana u ovom dokumentu. U slučaju da Izdavatelj nije registriran u AMS/MPS-u njegov identifikator mora biti formiran kao i u slučaju da je registriran.

Primjer:

```
<Sender>

 <Identifier Authority="iso6523-actorid-upis">9934:11111111111</Identifier>

</Sender>

<Receiver>

 <Identifier Authority="iso6523-actorid-
upis">0088:0847976000005</Identifier>

</Receiver>
```

5.10. PAKIRANJE PORUKA

Dokumenti koji su dio korisničke poruke ebMS-a mogu biti sadržani u SOAP tijelu ili zasebnim MIME privitcima. Budući da ovaj profil koristi značajku AS4 Compression (vidjeti u nastavku) koja se odnosi samo na sadržaj zapakiran u privitak, pristupna točka mora uključivati sve dokumente i priloge kao MIME privitke.

5.11. PRONALAZAK SPOSOBNOSTI I DINAMIČKO LOCIRANJE

Za pronalaženje pristupnih točaka prema identifikatoru primatelja koristi se kombinacija AMS i MPS servisa (u skladu sa Tehničkim specifikacijama).

Pristupna točka Izdavatelja mora doći do krajnje adrese primatelja i sukladno tome dinamički popuniti vrijednosti u P-Modeu. eRačun koristi AMP i MPS za pronalazak adrese primatelja. Sukladno tome, dinamički se mora popuniti:

P-Mode	Vrijednost
PMode[].Protocol.Address	URL adresa dobivena od MPS servisa

Tablica 7 – Pronalazak sposobnosti i dinamičko lociranje

6. PRILOZI

Prilog 1 – P-Mode parametri

Prilog 2 – Primjer P-Mode XML za Domibus rješenje

Prilog 3 – Shema SBDH ovojnice

Prilog 4 – Upute za instalaciju javno dostupnog Domibus rješenja za AS4 pristupnu točku

6.1. PRILOG 1: P-MODE PARAMETRI

P-Mode parametar	Vrijednost
PMode.ID	eRacun
PMode.Agreement	hrAgreement `urn:fdc:eracun.hr:2023:agreements:ap_provider`

Financira Europska unija NextGenerationEU

PMode.MEP	oneway http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay
PMode.MEPBinding	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push
PMode.Initiator.Party	Unosi se u Pmode za pošiljatelja: Jedan PartyId sa vrijednosti Subject CNAME iz certifikata pristupne točke, npr. HR11111111111_1000000100 (u formatu HR<OIB>) Fiksna vrijednost za partyIdType: `urn:fdc:eRacun.hr:2023:identifiers:ap`
PMode.Initiator.Role	Fiksna vrijednost: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator
PMode.Responder.Party	Unosi se u Pmode za primatelja Jedan PartyId sa vrijednosti Subject CNAME iz certifikata pristupne točke, npr. HR11111111111_1000000100 (u formatu HR<OIB>) Fiksna vrijednost za partyIdType: `urn:fdc:eRacun.hr:2023:identifiers:ap`
PMode.Responder.Role	Fiksna vrijednost: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder
PMode[1].Protocol.Address	Obavezno, https URL primatelja
PMode[1].Protocol.SOAPVersion	1.2
PMode[1].BusinessInfo.Service	Predefinirana vrijednost identifikatora procesa za slanje eRačuna - **hrBillingService**. Vrijednost: `urn:fdc:eracun.hr:2023:processId`
PMode[1].BusinessInfo.Service.type	Ne unosi se

PMode[1].BusinessInfo.Action	Predefinirana vrijednost identifikatora tipa dokumenta za eRačun formatirana po slijedećem: «scheme id»::«document type id value» Definirana su dva tipa: hrBillingInvoiceAction - busdox-docid-qns::urn:oasis:names:specification:ubl:schema:xsd:Invoice-2::Invoice##urn:cen.eu:en16931:2017#compliant#urn:fdc:peppol.eu:2017:poacc:billing:3.0::2.1 hrBillingCreditNoteAction – busdox-docid-qns::urn:oasis:names:specification:ubl:schema:xsd:CreditNote-2::CreditNote##urn:cen.eu:en16931:2017#compliant#urn:fdc:peppol.eu:2017:poacc:billing:3.0::2.1
PMode[].BusinessInfo.MPC	https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/
PMode[].Errorhandling.Report.AsResponse	True
PMode[].Errorhandling.Report.ProcessErrorNotifyConsumer	True
PMode[].ErrorHandling.Report.ProcessErrorNotifyProducer	True
PMode[].Errorhandling.DeliveryFailuresNotifyProducer	True
PMode[].ErrorHandling.Report.MissingReceiptNotifyProducer	True
PMode[].Security.WSSversion	1.1.1
PMode[].Security.X509.Sign	True

PMode[].Security.X509.Signature.Certificate	Certifikat pristupne točke pošiljatelja
PMode[].Security.X509.Signature.HashFunction	https://www.w3.org/TR/xmlenc-core1/
PMode[].Security.X509.Signature.Algorithm	https://www.ietf.org/internet-drafts/draft-eastlake-additional-xmlsec-uris-00.txt
PMode[].Security.X509.Encryption.Encrypt	False
PMode[].Security.PModeAuthorize	False
PMode[].Security.SendReceipt	True
PMode[].Security.SendReceipt.NonRepudiation	True
PMode[].Security.SendReceipt.ReplyPattern	Response
PMode[].PayloadService.CompressionType	application/gzip
PMode[].ReceptionAwareness	True
PMode[].ReceptionAwareness.Retry	True
PMode[].ReceptionAwareness.Retry.Parameters	maxretries=10, period=3000
PMode[].ReceptionAwareness.DuplicateDeteCtion	True
PMode[].ReceptionAwareness.DuplicateDeteCtion	maxsize=10Mb, checkwindow=7D

Tablica 8 Prilog 1: P – Mode parametri

6.2. PRILOG 2: PRIMJER P-MODE XML ZA DOMIBUS RJEŠENJE

```
<?xml version="1.0" encoding="UTF-8"?>
<db:configuration xmlns:db="http://domibus.eu/configuration"
party="porezna-uprava">
      <mpcs>
            <mpc name="defaultMpc" qualifiedName="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC" enabled="true"
default="true" retention_downloaded="0" retention_undownloaded="600"/>
      </mpcs>
      <businessProcesses>
            <roles>
                  <role name="defaultInitiatorRole"
value="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/initiator"/>
                  <role name="defaultResponderRole"
value="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/responder"/>
            </roles>
            <parties>
                  <partyIdTypes>
                        <partyIdType name="partyTypeUrn"
value="urn:fdc:eracun.hr:2023:identifiers:ap"/>
                  </partyIdTypes>
                  <party name=" porezna-uprava "
endpoint="http://localhost:8080/domibus/services/msh" allowChunking="true">
                        <identifier partyId=" porezna-uprava "
partyIdType="partyTypeUrn"/>
                  </party>
            </parties>
            <meps>
                  <mep name="oneway" value="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay"/>
            </meps>
            <properties>
                  <property name="originalSenderProperty"
key="originalSender" datatype="string" required="true"/>
                  <property name="finalRecipientProperty"
key="finalRecipient" datatype="string" required="true"/>
                  <propertySet name="ecodexPropertySet">
                        <propertyRef property="finalRecipientProperty"/>
                        <propertyRef property="originalSenderProperty"/>
                  </propertySet>
            </properties>
            <payloadProfiles>
                  <payload name="businessContentPayload" cid="cid:message"
required="true" mimeType="text/xml"/>
```

```
                <payload name="businessContentAttachment"
cid="cid:attachment" required="false" mimeType="application/octet-stream"/>
                <payloadProfile name="MessageProfile" maxSize="40894464">
                      <attachment name="businessContentPayload"/>
                      <attachment name="businessContentAttachment"/>
                </payloadProfile>
          </payloadProfiles>
          <securities>
                <security name="eDeliveryAS4Policy"
policy="eDeliveryAS4Policy.xml" signatureMethod="RSA_SHA256"/>
                <security name="noSigNoEnc" policy="doNothingPolicy.xml"
signatureMethod="RSA_SHA256"/>
                <security name="signOnly" policy="signOnly.xml"
signatureMethod="RSA_SHA256"/>
          </securities>
          <errorHandlings>
                 <errorHandling name="demoErrorHandling"
errorAsResponse="true" businessErrorNotifyProducer="false"
businessErrorNotifyConsumer="false" deliveryFailureNotifyProducer="false"/>
                 <errorHandling name="notifyErrorHandling"
errorAsResponse="true" businessErrorNotifyProducer="true"
businessErrorNotifyConsumer="true" deliveryFailureNotifyProducer="true"/>
          </errorHandlings>
          <agreements>
                <agreement name="hrAgreement"
value="urn:fdc:eracun.hr:2023:agreements:ap_provider" type=""/>

          </agreements>
          <services>
                <service name="hrBillingService"
value="urn:fdc:eracun.hr:2023:processId" type=""/>
          </services>
          <actions>
                <action name="hrBillingInvoiceAction" value="busdox-
docid-qns::urn:oasis:names:specification:ubl:schema:xsd:Invoice-
2::Invoice##urn:cen.eu:en16931:2017#compliant#urn:fdc:peppol.eu:2017:poacc:
billing:3.0::2.1"/>
                <action name="hrBillingCreditNoteAction" value="busdox-
docid-qns::urn:oasis:names:specification:ubl:schema:xsd:CreditNote-
2::CreditNote##urn:cen.eu:en16931:2017#compliant#urn:fdc:peppol.eu:2017:poa
cc:billing:3.0::2.1"/>
          </actions>
          <as4>
                <receptionAwareness name="receptionAwareness"
retry="12;4;CONSTANT" duplicateDetection="true"/>
                <reliability name="AS4Reliability" nonRepudiation="true"
replyPattern="response"/>
                <reliability name="noReliability" nonRepudiation="false"
replyPattern="response"/>
```

```
            </as4>
            <legConfigurations>
                  <legConfiguration name="hrBillingInvoiceLeg"
service="hrBillingService" action="hrBillingInvoiceAction"
defaultMpc="defaultMpc" reliability="AS4Reliability" security="signOnly"
receptionAwareness="receptionAwareness" propertySet="ecodexPropertySet"
payloadProfile="MessageProfile" errorHandling="demoErrorHandling"
compressPayloads="true"/>
                  <legConfiguration name="hrBillingCreditNoteLeg"
service="hrBillingService" action="hrBillingCreditNoteAction"
defaultMpc="defaultMpc" reliability="AS4Reliability" security="signOnly"
receptionAwareness="receptionAwareness" propertySet="ecodexPropertySet"
payloadProfile="MessageProfile" errorHandling="demoErrorHandling"
compressPayloads="true"/>
                  </legConfigurations>
            <process name="hrInvoiceSendProcess" agreement="hrAgreement"
mep="oneway" binding="push" initiatorRole="defaultInitiatorRole"
responderRole="defaultResponderRole">
                  <initiatorParties>
                        <initiatorParty name="porezna-uprava"/>
                  </initiatorParties>
                  <legs>
                        <leg name="hrBillingInvoiceLeg"/>
                  </legs>
            </process>
            <process name="hrBillingNoteSendProcess"
agreement="hrAgreement" mep="oneway" binding="push"
initiatorRole="defaultInitiatorRole" responderRole="defaultResponderRole">
                  <initiatorParties>
                        <initiatorParty name="porezna-uprava"/>
                  </initiatorParties>
                  <legs>
                        <leg name="hrBillingCreditNoteLeg"/>
                  </legs>
            </process>
            <process name="hrInvoiceReceiveProcess" agreement="hrAgreement"
mep="oneway" binding="push" initiatorRole="defaultInitiatorRole"
responderRole="defaultResponderRole">
                  <responderParties>
                        <responderParty name="porezna-uprava"/>
                  </responderParties>
                  <legs>
                        <leg name="hrBillingInvoiceLeg"/>
                  </legs>
            </process>
            <process name="hrBillingNoteReceiveProcess"
agreement="hrAgreement" mep="oneway" binding="push"
initiatorRole="defaultInitiatorRole" responderRole="defaultResponderRole">
                  <responderParties>
```

```
                <responderParty name="porezna-uprava"/>
            </responderParties>
            <legs>
                <leg name="hrBillingCreditNoteLeg"/>
            </legs>
        </process>
        </businessProcesses>
</db:configuration>
```

6.3. PRILOG 3: SHEMA SBDH OVOJNICE

Element/Attribute	Annotation	
StandardBusinessDocument	Type	StandardBusinessDocument
xs:sequence	Occurrence	1 .. 1
StandardBusinessDocumentHeader	Occurrence Type	1 .. 1 StandardBusinessDocumentHeader
xs:sequence	Occurrence	1 .. 1
HeaderVersion	Occurrence Type Fixed Description	1 .. 1 xs:string 1.0 Always value 1.0
Sender	Occurrence Type	1 .. 1 Partner
xs:sequence	Occurrence	1 .. 1
Identifier	Occurrence Type Description	1 .. 1 PartnerIdentification Use the format XXXX:AAAAAAAA where XXXX is the type of identifer (such as 0088 for GS1 GLN) and AAAAAAAA the actual identifier.
Authority	Type Use Description	xs:string required Use fixed value "iso6523-actorid-upis"
Receiver	Occurrence Type	1 .. 1 Partner
xs:sequence	Occurrence	1 .. 1
Identifier	Occurrence Type Description	1 .. 1 PartnerIdentification Use the format XXXX:AAAAAAAA where XXXX is the type of identifer (such as 0088 for GS1 GLN) and AAAAAAAA the actual identifier.
Authority	Type Use Description	xs:string required Use fixed value "iso6523-actorid-upis"
DocumentIdentification	Occurrence Type	1 .. 1 DocumentIdentification
xs:sequence	Occurrence	1 .. 1
Standard	Occurrence Type Description	1 .. 1 xs:string The standard of the enveloped business message, normally described by use of the XML namespace of the business message root element (such as urn:oasis:names:specification:ubl:schema:xsd:Order-2)
TypeVersion	Occurrence Type Description	1 .. 1 xs:string The version number of the enveloped business message (such as the value "2.1" for OASIS UBL 2.1 or "2.0" for OASIS UBL 2.0)
InstanceIdentifier	Occurrence Type Description	1 .. 1 xs:string An informative unique ID created by the issuer of the envelope. The InstanceIdentifier MUST be unique for each Business Message Envelope being created. This ID is not the same as the ID of the business message (such as the Invoice Number). It is not the same as a transmission Message ID generated by the application sending the message (as defined in AS4). The InstanceIdentifier MUST be globally unique and it is RECOMMENDED to use UUID (such as 118e3040-51d2-11e3-8f96-0800200c9a66)
Type	Occurrence Type Description	1 .. 1 xs:string Message type - mandatory in SBDH. XML local element name of the root-element in the business message.

Slika 3. Prilog 3: Shema SBDH ovojnice

6.4. PRILOG 4: UPUTE ZA INSTALACIJU JAVNO DOSTUPNOG DOMIBUS RJEŠENJA ZA AS4 PRISTUPNU TOČKU

Domibus je javno dostupno rješenje koji pruža funkcionalnosti AS4 pristupne točke a održava ga Europska komisija (Directorate-General for Informatics - DIGIT).

Upute za instalaciju i zahtjevi za Domibus rješenje:

- Dokumentacija i osnovni podaci: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Domibus
- Linkovi na distribuciju:
  - https://ec.europa.eu/digital-building-blocks/artifact/repository/eDelivery/eu/domibus/domibus-msh-distribution/5.1.3/domibus-msh-distribution-5.1.3-tomcat-full.zip
  - https://ec.europa.eu/digital-building-blocks/artifact/repository/eDelivery/eu/domibus/domibus-msh-distribution/5.1.3/domibus-msh-distribution-5.1.3-wildfly-full.zip
  - https://ec.europa.eu/digital-building-blocks/artifact/repository/eDelivery/eu/domibus/domibus-msh-distribution/5.1.3/domibus-msh-distribution-5.1.3-weblogic-war.zip

Link na upute za instalaciju: https://ec.europa.eu/digital-building-blocks/sites/download/attachments/718734654/%28eDelivery%29%28AP%29%28QSG%29%28Domibus%205.1.3%29%287.8%29.pdf?version=1&modificationDate=1712324424129&api=v2

PODRŽANE PLATFORME ZA INSTALACIJU:

- Application servers:
  - WildFly 26.1.x
  - WebLogic 12.2.1.4 (tested version, future versions might work)
  - Apache Tomcat 9.0.x
- Database:
  - MySQL 8 (future versions might work)
  - Oracle 12c R2 and Oracle 19c
- Java:
  - Oracle JDK 8u291+ for WebLogic, Tomcat and WildFly
  - OpenJDK 11.0.11 for WildFly and Tomcat (tested with AdoptOpenJDK 11 version 11.0.9.1+1)