VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

EVIP
e-vročanje SVEV 2.0

Jože Rihtaršič

Vrhovno sodišče Republike Slovenije
Center za informatiko

Predstavitev SVEV 2.0 17. 6. 2015

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

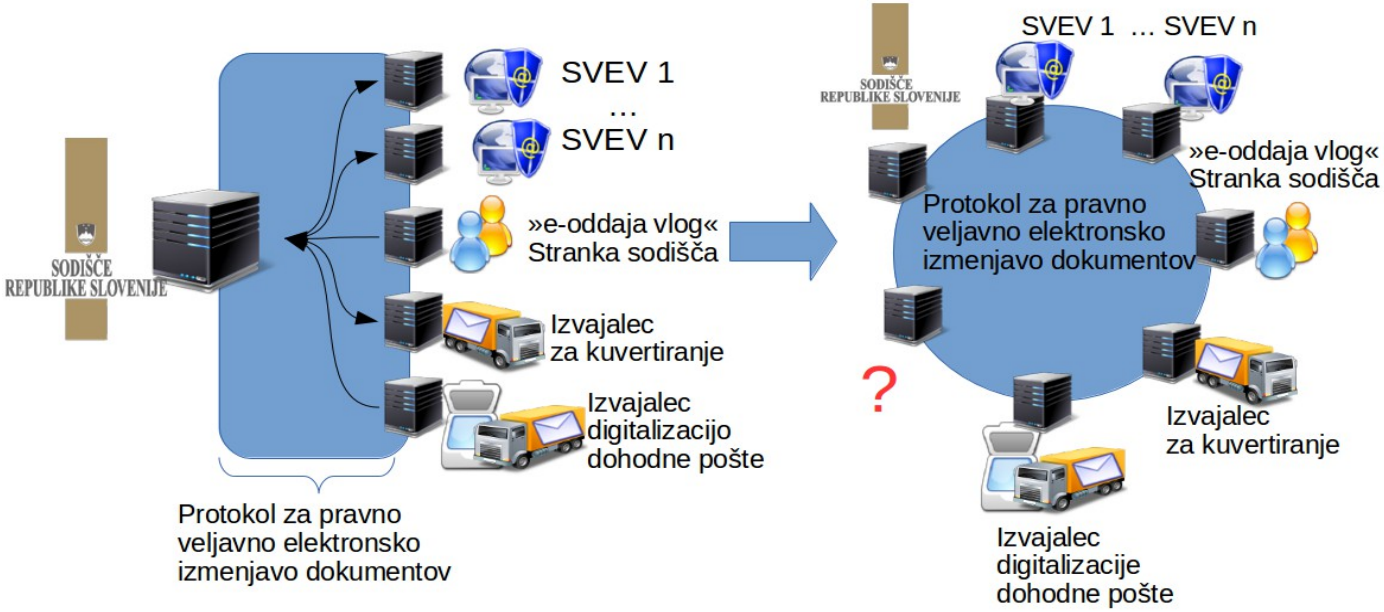
Namen posodobitve SVEV 2.0

- Vedno več namenskih integracij.
  - Različne tehnologije
  - Stroški vzdrževanja
  - Preglednost sistema

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

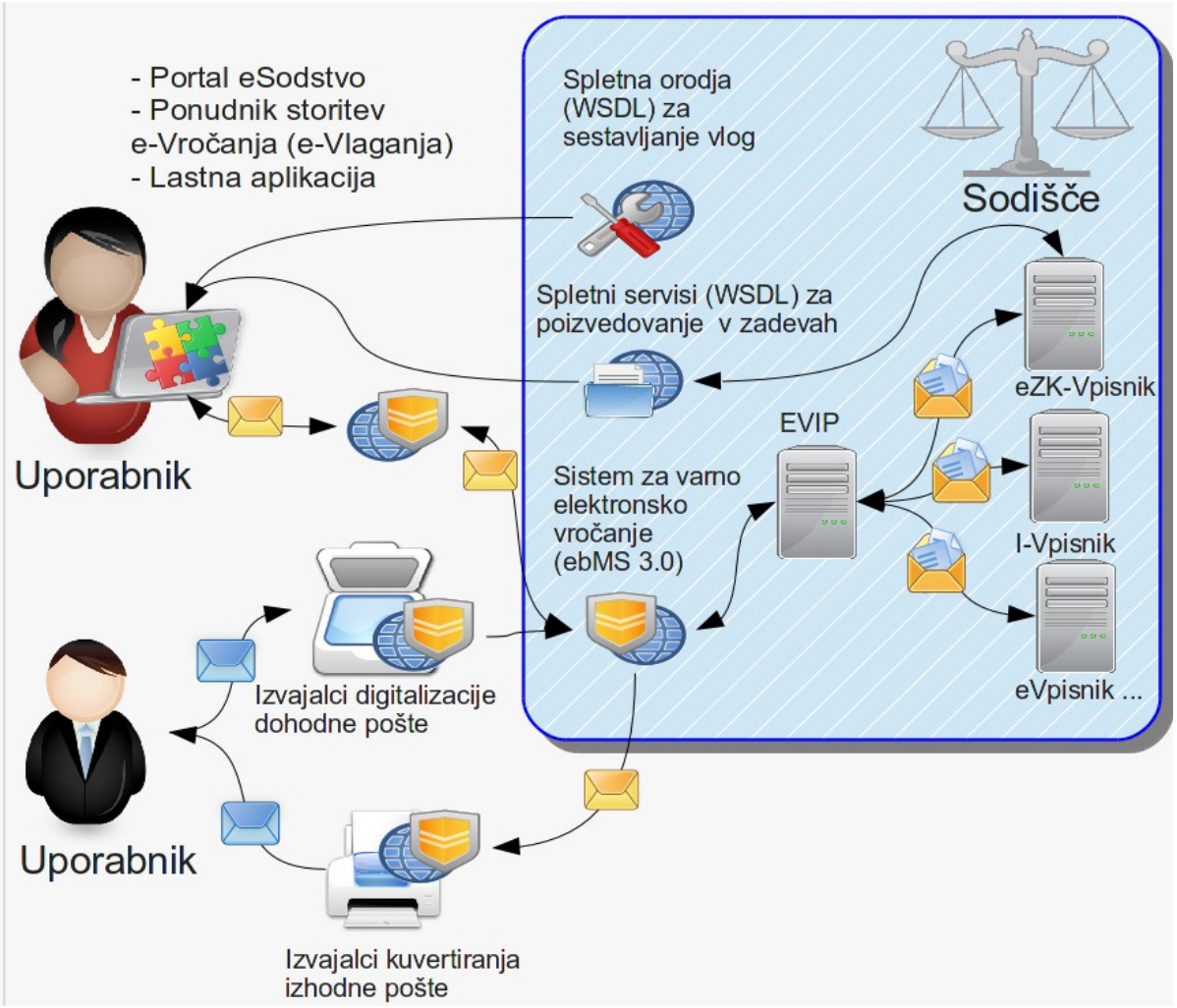
Namen posodobitve SVEV

- Izdelava univerzalnega modula za izmenjavo dokumentov
- Uporaben izven pravosodnega okolja
  - Lažje opravičenje stroškov pri izvajalcih
- Transport neodvisen od vsebine, ki se prenašajo
  - Lažja vpeljava sprememb struktur podatkov, ki se vročajo.



VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

E-vlaganje: OASIS ECF 4.0



VRHOVNO SODIŠČE REPUBLIKE SLOVENIJE

OASIS ebMS 3.0

Prednosti

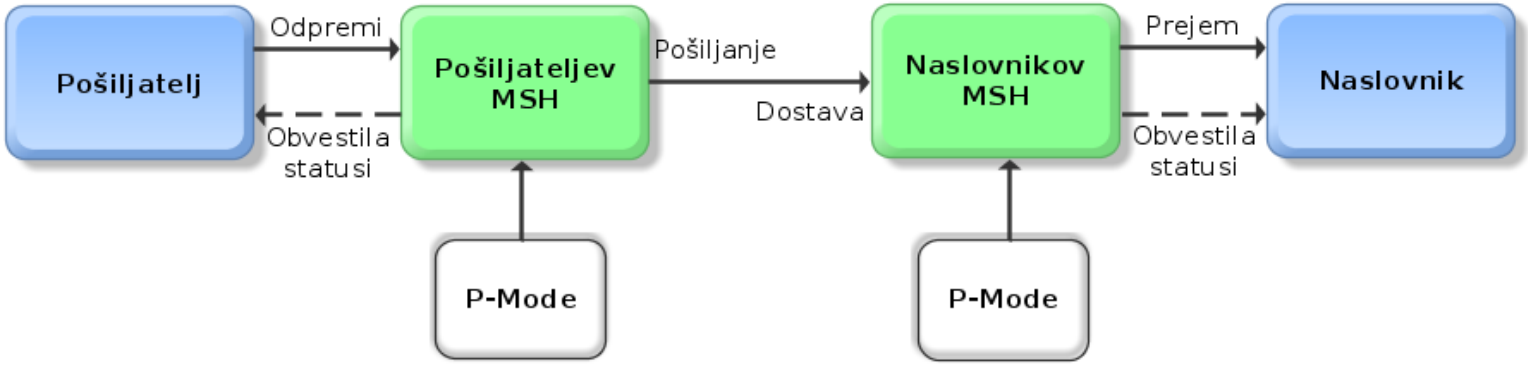
- Odprti/zastonjski standard
- Združuje obstoječe spletne standarde: WS-Security, WS-RM,..
- SOAP s priponkami
- Bogate izkušnje B2B ebMS 2.0
- Vsebina in transportni podatki so ločeni
- Omogoča poslovne transakcije
- Uporabljajo jih zadnji evropski projekti velikih razsežnost (LSP) e-CODEX, e-SENS
- Holodeck-b2b alternativa: WS-Standardi: apache-cxf, axis 2.0, apache-camel)

Slabosti

- Malo odprtih rešitev/tehnologij, ki podpirajo, ta standard.
- Sheme sporočil, niso del opisa servisa (implementacija)

VRHOVNO SODIŠČE REPUBLIKE SLOVENIJE

EbMS 3.0 – MSH (Mesage service handler)

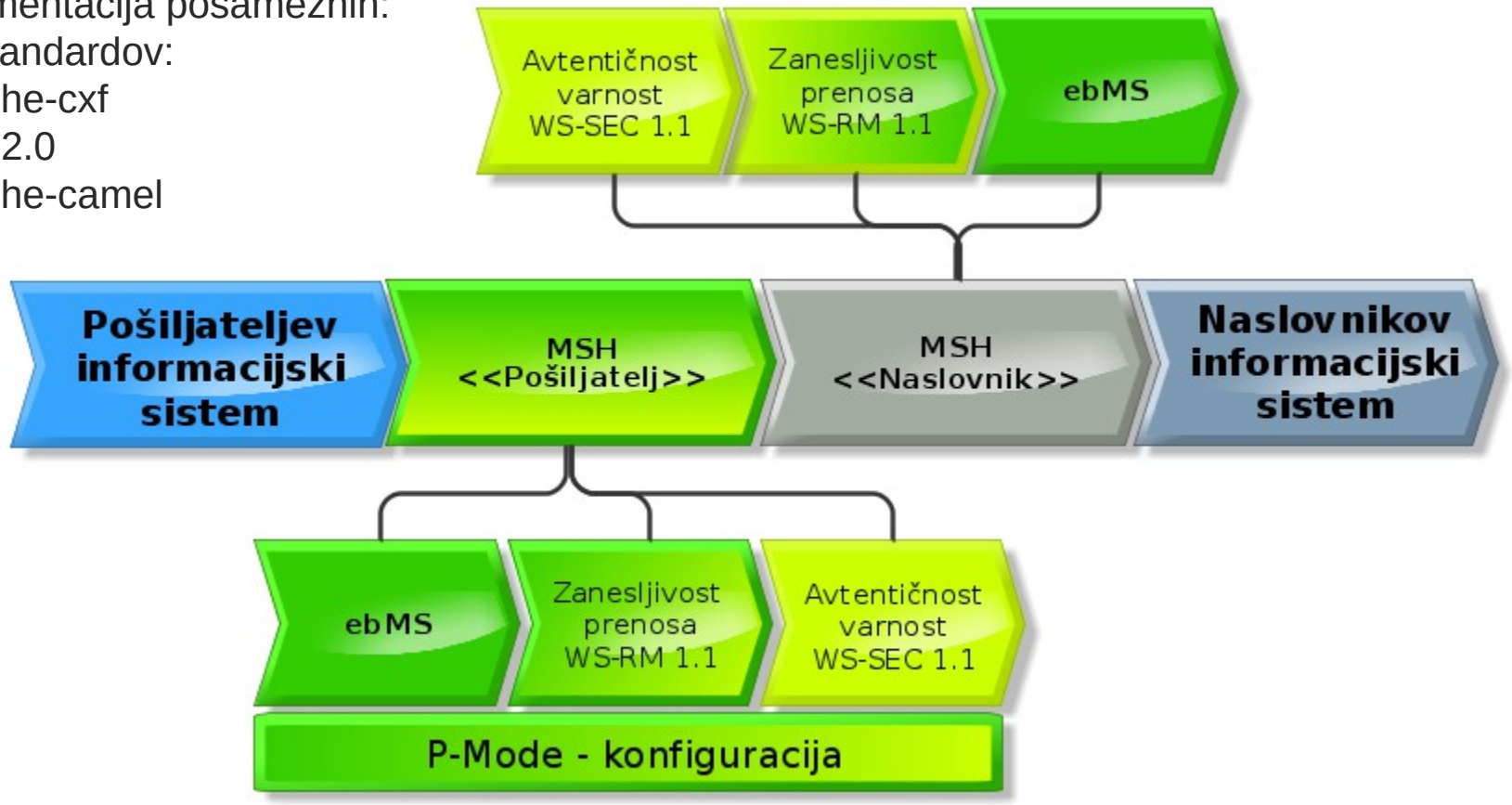


- **splošni parametri**, kot so enolična oznaka konfiguracije, referenca na pogodbo za izmenjavo dokumentov, identifikator naslovnika/prejemnika sporočila ter vloge pri izmenjavi dokumentov;
- **protokol**: določa spodaj ležeči protokol izmenjave (HTTP, SMTP, FTP) ter naslov (URL ali email) prejemnikovega MSH;
- **poslovni kontekst**: določa namen, storitev, akcijo in obliko vsebine;
- **napake**: razdelek določa ravnanje in poročanje v primeru napak pri prenosu;
- **zanesljivost prenosa**: parametri določajo uporabo mehanizmov za zagotavljanje zanesljivosti prenosa;
- **varnost**: parametri določajo nivo varnosti, pravila in certifikate za enkripcijo in podpisovanje sporočil.

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

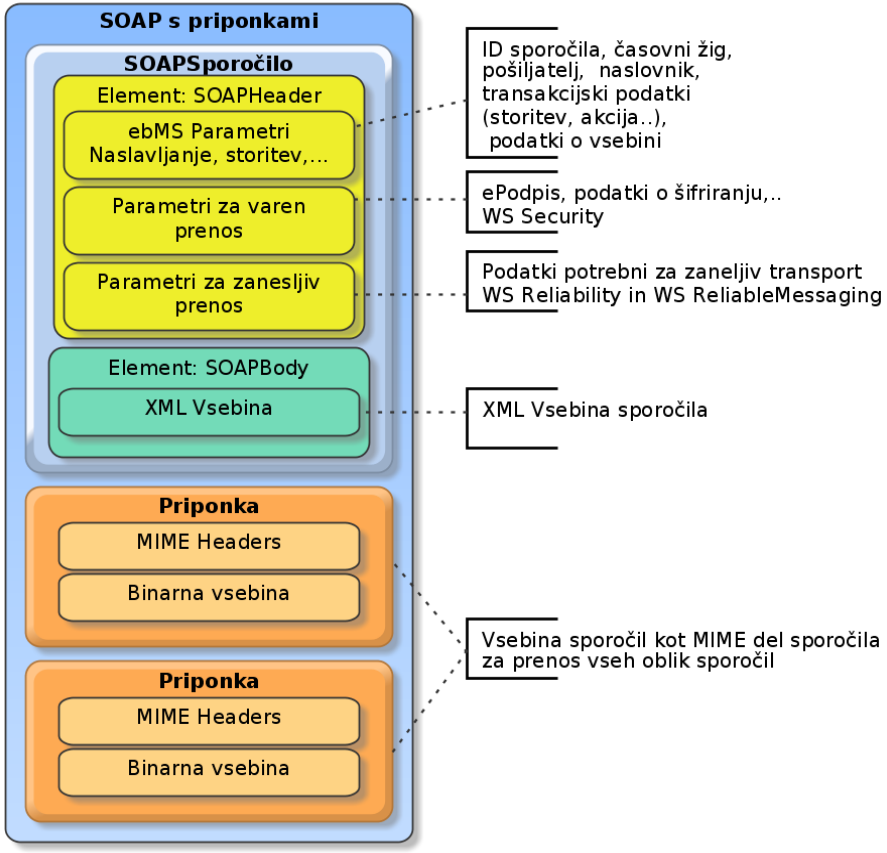
EbMS 3.0 - implementacija

Holodeck-b2b: (OK rešitev)
implementacija posameznih:
WS-standardov:
- apache-cxf
- Axis 2.0
- apache-camel



VRHOVNO SODIŠČE REPUBLIKE SLOVENIJE

EbMS 3.0 pakiranje sporočila



- Vse vsebine so v priponkah: Glava SOAP sporočila vsebuje podpise priponk, podpis sporočila, pošiljatelja, naslovnika, poslovni kontekst,...

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

AS4Receipt

- Potrdilo o prenosu vsebin:
  - Id prejetega sporočila
  - zgostitvene vrednosti prenesenih/prejetih priponk;
  - e-podpis naslovnikovega MSH.

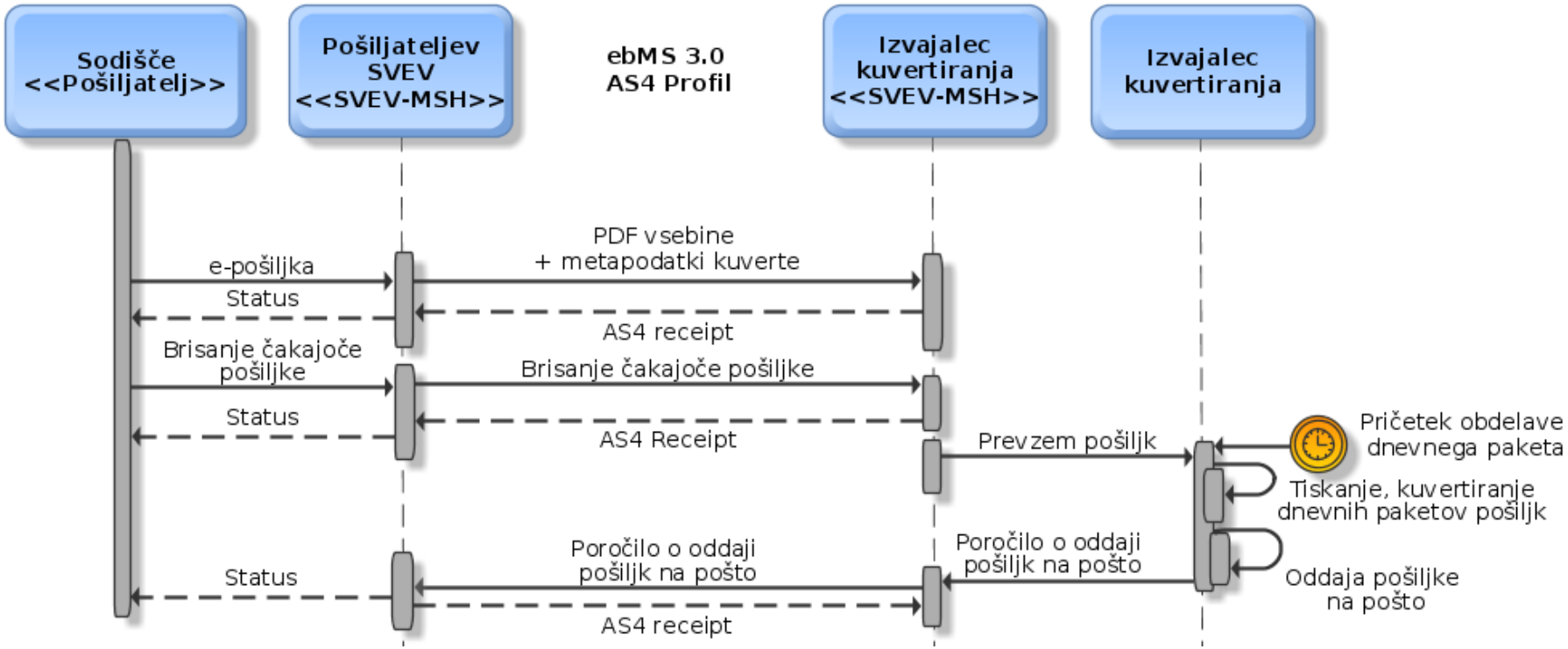
VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Poslovne transakcije

- ebMS 3.0: business transactions: messages are parts of basic choreographies that map to higher-level business exchanges between partners.
  - Nakup: Naročilo -> Potrdilo naročila -> Dobavnica -> Račun
  -
- **Storitev** (ebMS 3.0: Service: Name of the service to which the User message is intended to be delivered)
- **Akcija:** (ebMS 3.0: Action: Name of the action the User message is intended to invoke)
- **Id transakcije:** (ebMS 3.0: ConversationId This element is a string identifying the set of related messages that make up a conversation between Parties.)

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Poslovne transakcije
Storitev tiskanja in kuvertiranja



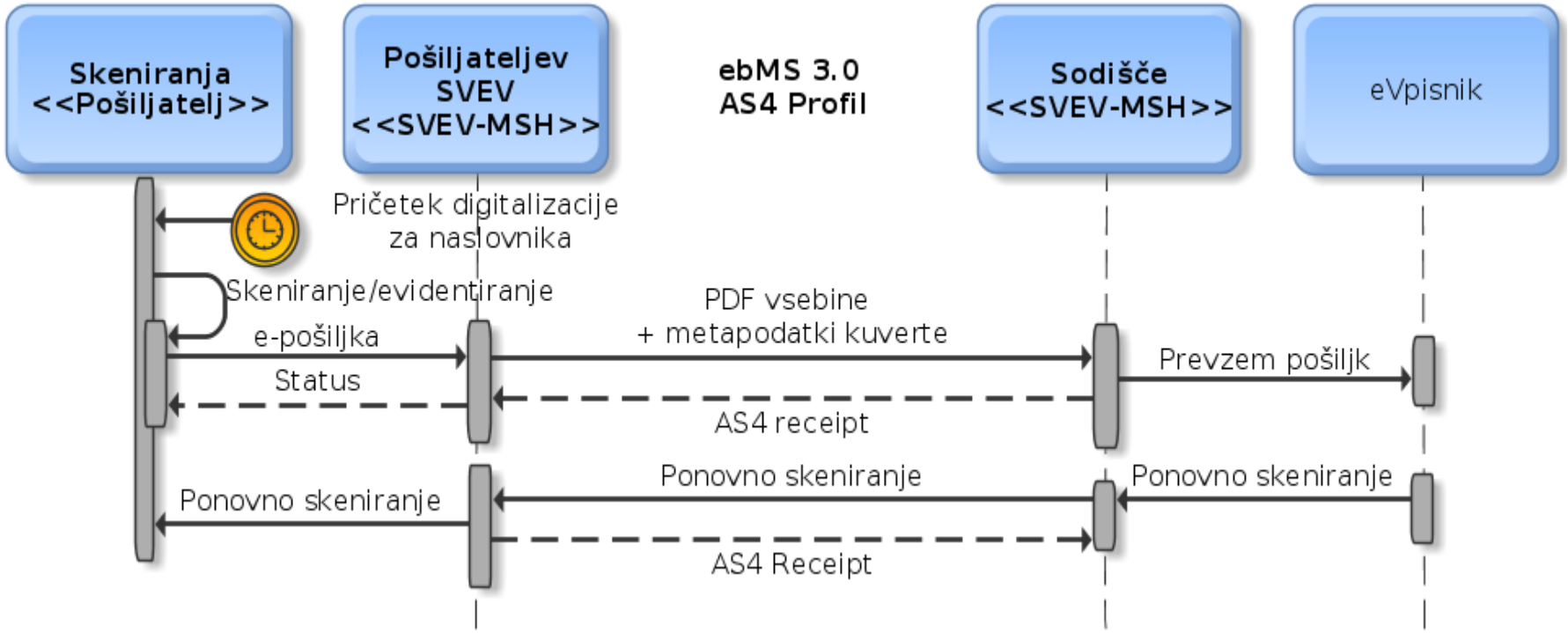
VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Poslovne transakcije
Storitev tiskanja in kuvertiranja

- Storitve:
  - PrintAndEnvelope-LegalZPP
  - PrintAndEnvelope-LegalZPP-Personal
  - PrintAndEnvelope-LegalZUP
  - PrintAndEnvelope-Mail-C5
  - PrintAndEnvelope-RegistredMail-C5
- Akcije:
  - **AddMail** - dodajanje pošiljke v kuvertiranje (Vsebuje: XML - metapodatki kuverte + PDF; Odgovor: AS4Receipt ali napaka)
  - **RemoveMail** – Zahtevek za brisanje pošiljke (AS4Receipt ali napaka – pošiljka je že bila sprocesirana)
  - **MailProcessed** – Sporočanje pošiljatelju o opravljenih storitvah. (AS4Receipt)

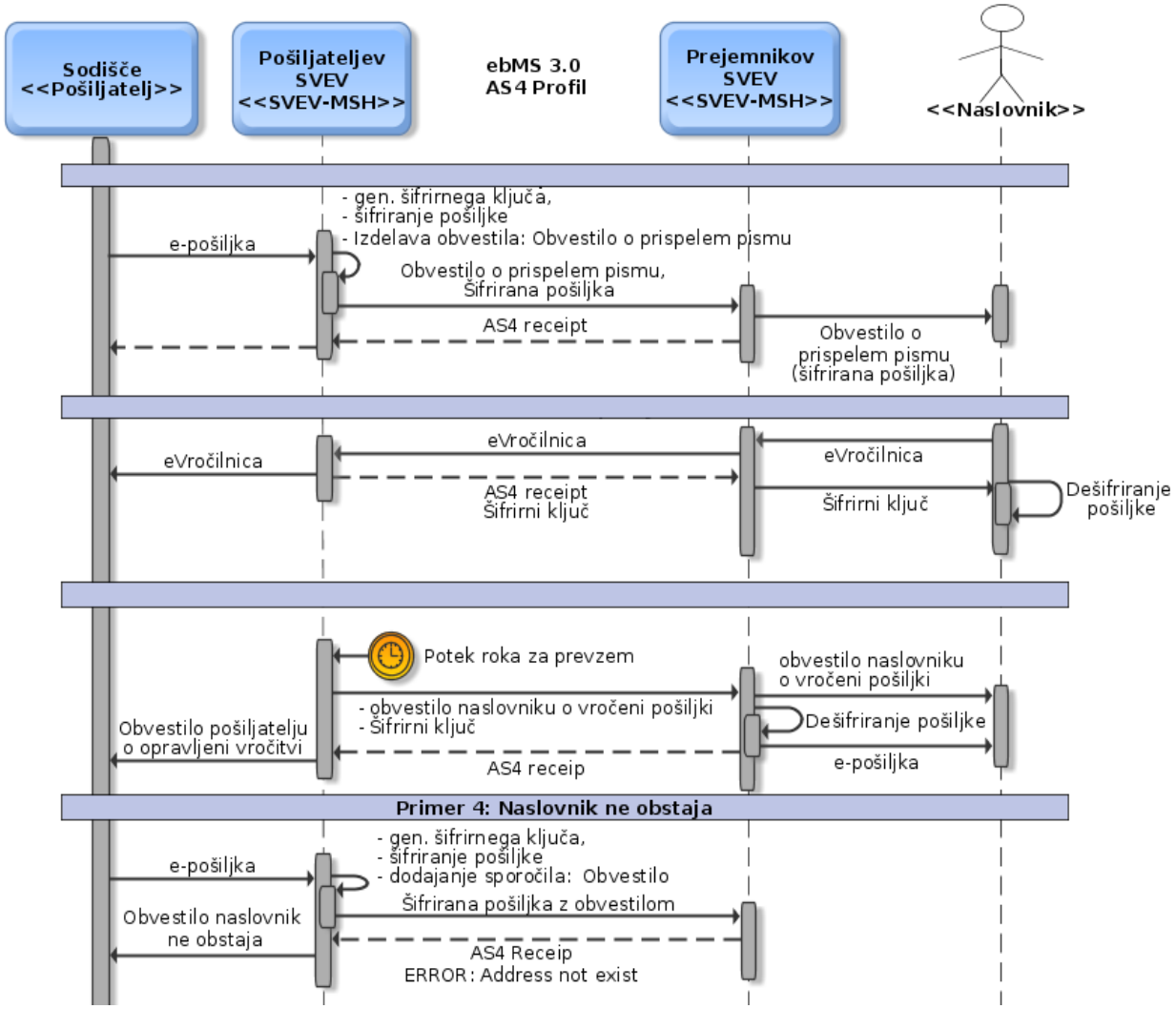
VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Izvajalci digitalizacije



VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Poslovne transakcije: Elektronsko vročanje v e-predal



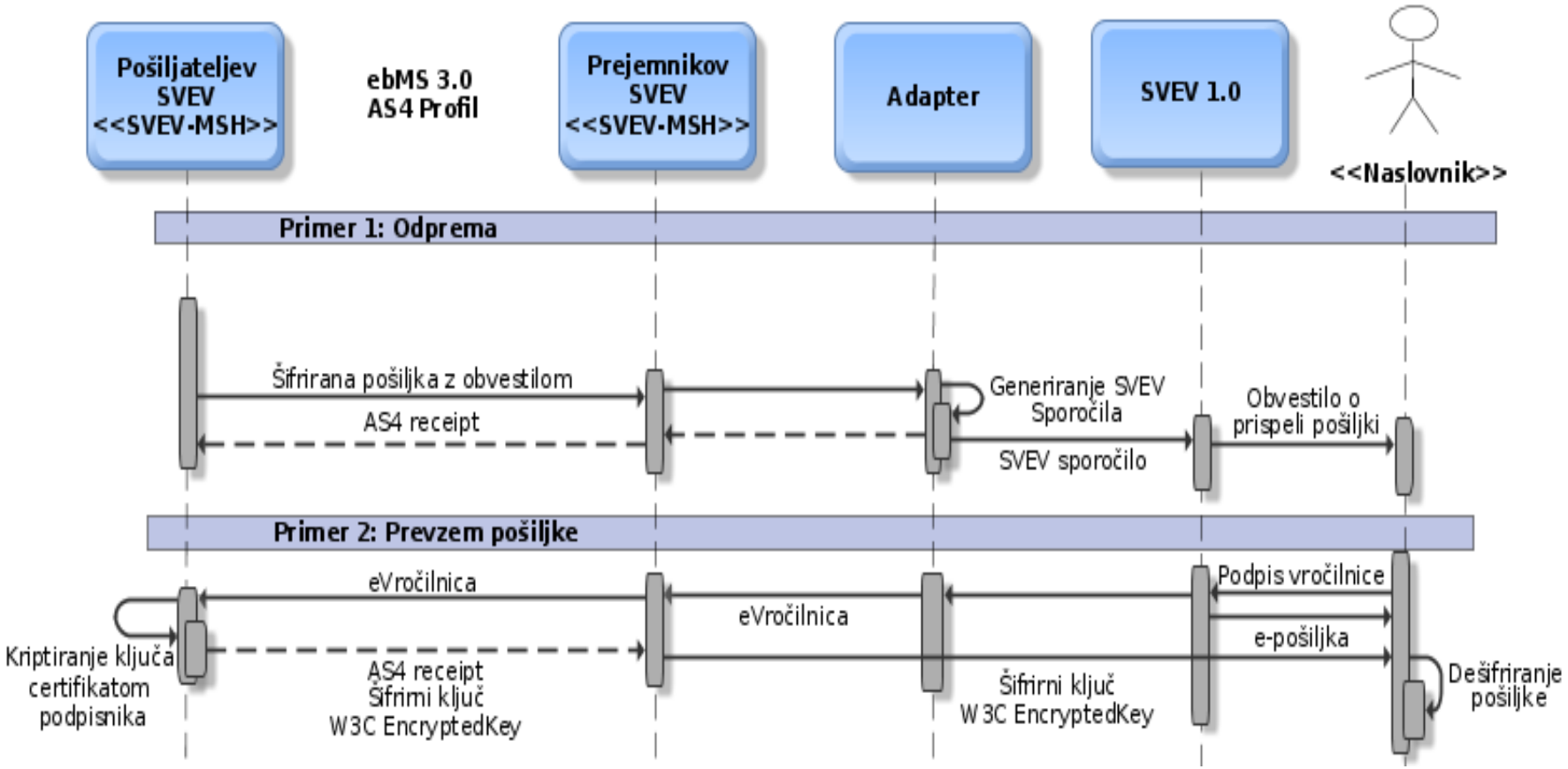
VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Poslovne transakcije: Elektronsko vročanje v e-predal

- Storitve:
  - **LegalZPP** (LegalZUP,LegalZKP,RegistredMail)
- Akcije:
  - **DeliveryNotification**“ proži pošiljateljev MSH za prenos šifriranega sporočila in ustreznega obvestila o prispeli pošti v naslovnikov MSH. Naslovnikov MSH obvestilo tudi posreduje v naslovnikov elektronski predal;
  - **AdviceOfDelivery**“ proži naslovnikov MSH, ki posreduje ustrezno podpisano vročilnico v pošiljateljev MSH in v odgovor prejme ključ za dešifriranje dohodne pošte;
  - „**FictionNotification**“ posreduje pošiljateljev MSH po preteku zakonsko določenega roka od uspešne oddaje pošiljke v naslovnikov MSH. Sporočilo vsebuje obvestilo o opravljeni vročitvi stranki in šifrirni ključ, s katerim naslovnikov MSH dešifrira pošiljko;

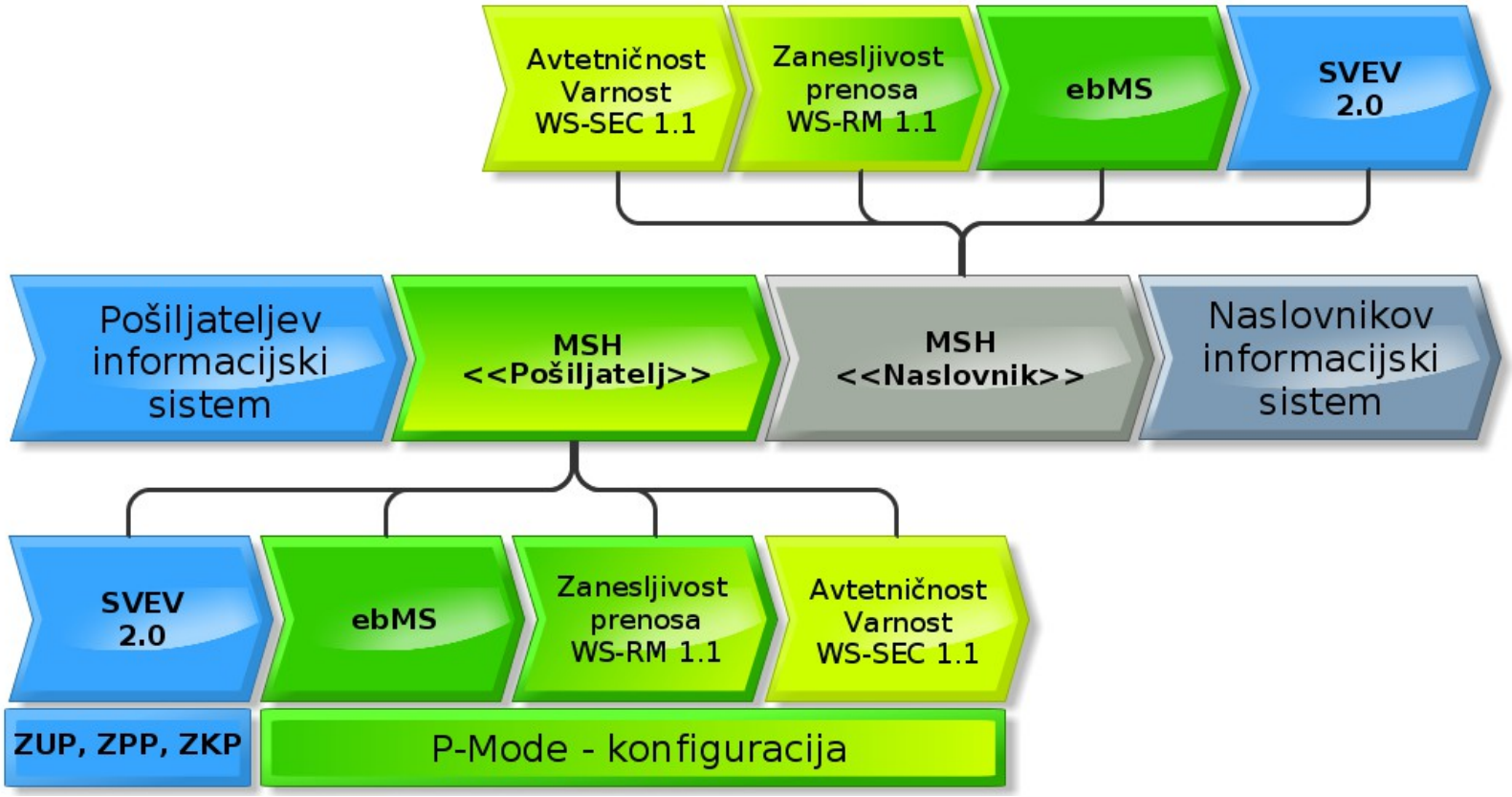
VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Predlog integracije



VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

SVEV 2.0 z uporabo ebMS 3.0



VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

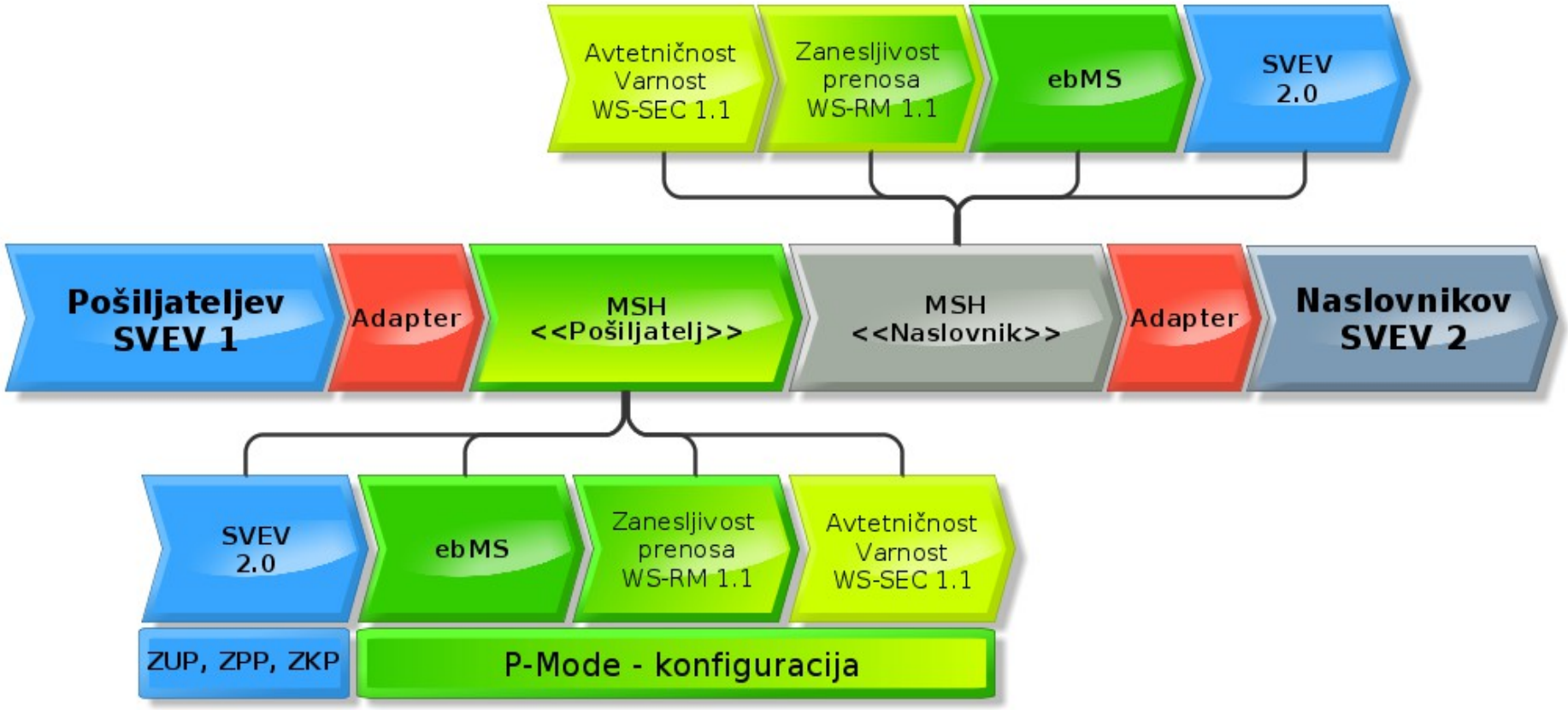
ebMS 3.0 - naslavljanje

```
<ns2:PartyInfo>
  <ns2:From>
    <ns2:PartyId>si-svev:Vesna.Pomlad@moja.posta.si</ns2:PartyId>
    <ns2:Role>si-svev:Sender</ns2:Role>
  </ns2:From>
  <ns2:To>
    <ns2:PartyId>si-svev:Zora.Mrak@vep.si</ns2:PartyId>
    <ns2:Role>si-svev:Receiver</ns2:Role>
  </ns2:To>
</ns2:PartyInfo>
```

- Obdrži se obstoječe SVEV naslove
  - Na domena naslova @moja.posta.si, @vep.si, @svev-sodisce.si, @svev-kro.si se določa URL pošiljateljevega in naslovnikovega MSH-ja.
  -

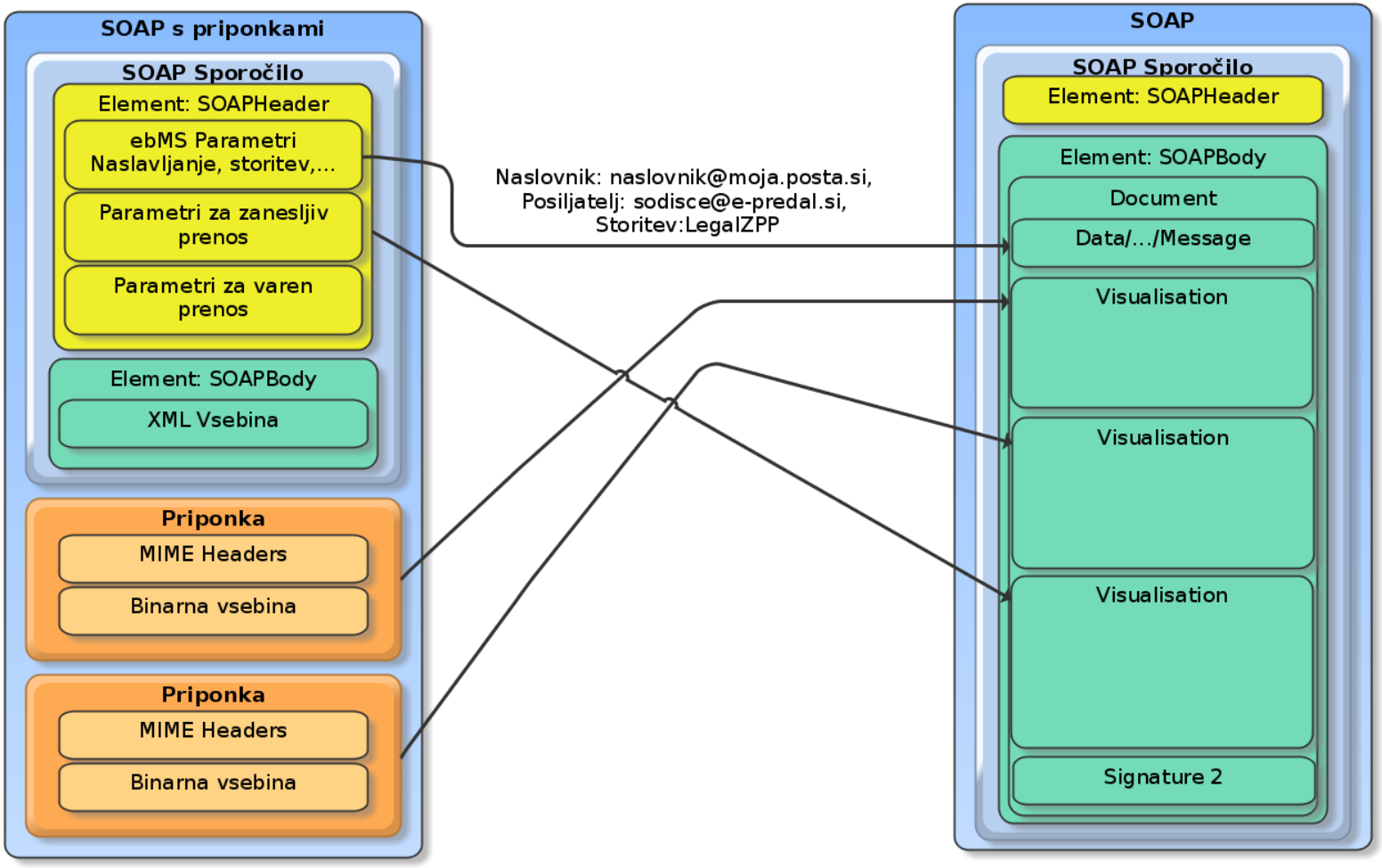
VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Obstoječi SVEV 1.0



VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Preslikava sporočil SVEV 1.0 v SVEV 2.0



VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Transport

- Prenos sporočil poteka preko TLS seje, ki se vzpostavi z obojestransko avtentikacijo (Mutual authentication).
  Standardi:
  TLS + HTTP 1.1 + SOAP 1.2 + WSS 1.1 + SOAP with Attachments

- EbMS 3.0 MEP: One-way / Push

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Zanesljivost

- Odgovor vedno AS4Receipt ali Exception signal.
- V primeru SoapFault ali tcp/http ERROR, pošilatelj sporočilo poskuša ponovno poslati, tako kot to določajo »Retry« nastavitve.

PMode[1].ReceptionAwareness: true

PMode[1].Security.SendReceipt: true;

Pmode[1].Security.SendReceipt.ReplyPattern: response
PMode[1].ReceptionAwareness.Retry: true;

PMode[1].ReceptionAwareness.Retry.Parameters: maxretries=10, period=2000, e*xponentialBackoff=true;*

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Zanesljivost

PMode[1].ReceptionAwareness.DuplicateDetection: true;
PMode[1].ReceptionAwareness.DetectDuplicates.Parameters: 5y

```
<eb:Error origin="reliability" category="delivery"
errorCode="SVEV:0201" severity="warning"
refToMessageInError="23434-345rt34-e343@sender.ebox.si"
shortDescription="First sucessfuly delivery: 2014-07-25T12:19:05">
</eb:Error>
```

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Varnost

- Podpisani so elementi: env:Header/eb3:Messaging in env:Body ter vse SOAP priponke.
  PMode[1].Security.X509.Sign: true
- Lastnosti podpisa:
  PMode[1].Security.X509.Signature.HashFunction: http://www.w3.org/2001/04/xmlenc#sha256
  Pmode[1].Security.X509.Signature.Algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Primer kriptirane priponke

```
<?xml version="1.0" encoding="UTF-8"?>
<ns3:EncryptedData Id="72bft7d60utlf18vihg2qr" Encoding="UTF-8" MimeType="text/plain">
   <ns3:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:RetrievalMethod URI="#EK-1"
Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
   </ds:KeyInfo>
   <ns3:CipherData>

<ns3:CipherValue>rIlCvt//zsatNLyA7gsAJgAmx4b1ptpq4Uet3kS5GpU=</ns3:CipherValue>
   </ns3:CipherData>
</ns3:EncryptedData>
```

VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

Primer ključa

```
<EncryptedKey Id="EK-1" xmlns="http://www.w3.org/2001/04/xmlenc#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:KeyName>Janez Prejemnik</ds:KeyName>
          <ds:X509Data>
                <ds:X509IssuerSerial>
                     <ds:X509IssuerName>CN=msh.e-box-
b.si,OU=test,OU=msh,OU=jrc,OU=si</ds:X509IssuerName>
                          <ds:X509SerialNumber>228884898</ds:X509SerialNumber>
                </ds:X509IssuerSerial>
           </ds:X509Data>
     </ds:KeyInfo>
      <CipherData>
           <CipherValue>YTE3eGoyeg==</CipherValue>
      </CipherData>
      <ReferenceList>
          <DataReference URI="#72bft7d60utlf18vihg2qr"/>
      </ReferenceList>
</EncryptedKey>
```