VRHOVNO SODIŠČE
REPUBLIKE SLOVENIJE

CENTER ZA INFORMATIKO

**E -VLOŽIŠČE**

# Funkcionalne in tehnične zahteve informacijskega sistema za varno elektronsko vročanje v civilnih sodnih postopkih

**2.0**

**OSNUTEK**

# KONTROLA VERZIJ

## ZADNJA VERZIJA:

| | |
|---|---|
| Verzija | 1.1 |
| Datum | 01.08.14 |
| Avtor | Jože Rihtaršič |
| Odgovornost | Bojan Muršec |
| Zaupnost | |
| Datoteka | |

## ZGODOVINA:

| Verzija | Datum | Avtor | Opis |
|---|---|---|---|
| 1.0 | 01.08.14 | Jože Rihtaršič | Dokument kreiran. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## REVIZIJE:

| Revizija | Datum | Avtor | Opis |
|---|---|---|---|
| | | | |

## ZAŠČITA DOKUMENTA

# Kazalo vsebine

# 1 Uvod

## 1.1 Namen

V dokumentu so opisane zahteve, ki jim mora ustrezati informacijski sistem za varno elektronsko vročanje v civilnih sodnih postopkih v skladu s 1. točko drugega odstavka 7. člena Pravilnika o elektronskem poslovanju v civilnih sodnih postopkih (Uradni list RS, št. 64/10; v nadaljnjem besedilu: PEPCSP).

Dokument vsebuje opis aplikacijskih vmesnikov (API) ter XML shem (xsd), ki se uporabljajo za varno elektronsko vročanje. Namenjen je razvijalcem programske opreme ponudnikov storitev varnega elektronskega vročanja.

Pojmi, uporabljeni v dokumentu, imajo pomen, opredeljen v naslednjih določbah Zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 − uradno prečiščeno besedilo in 61/06-ZEPT ) in PEPCSP:

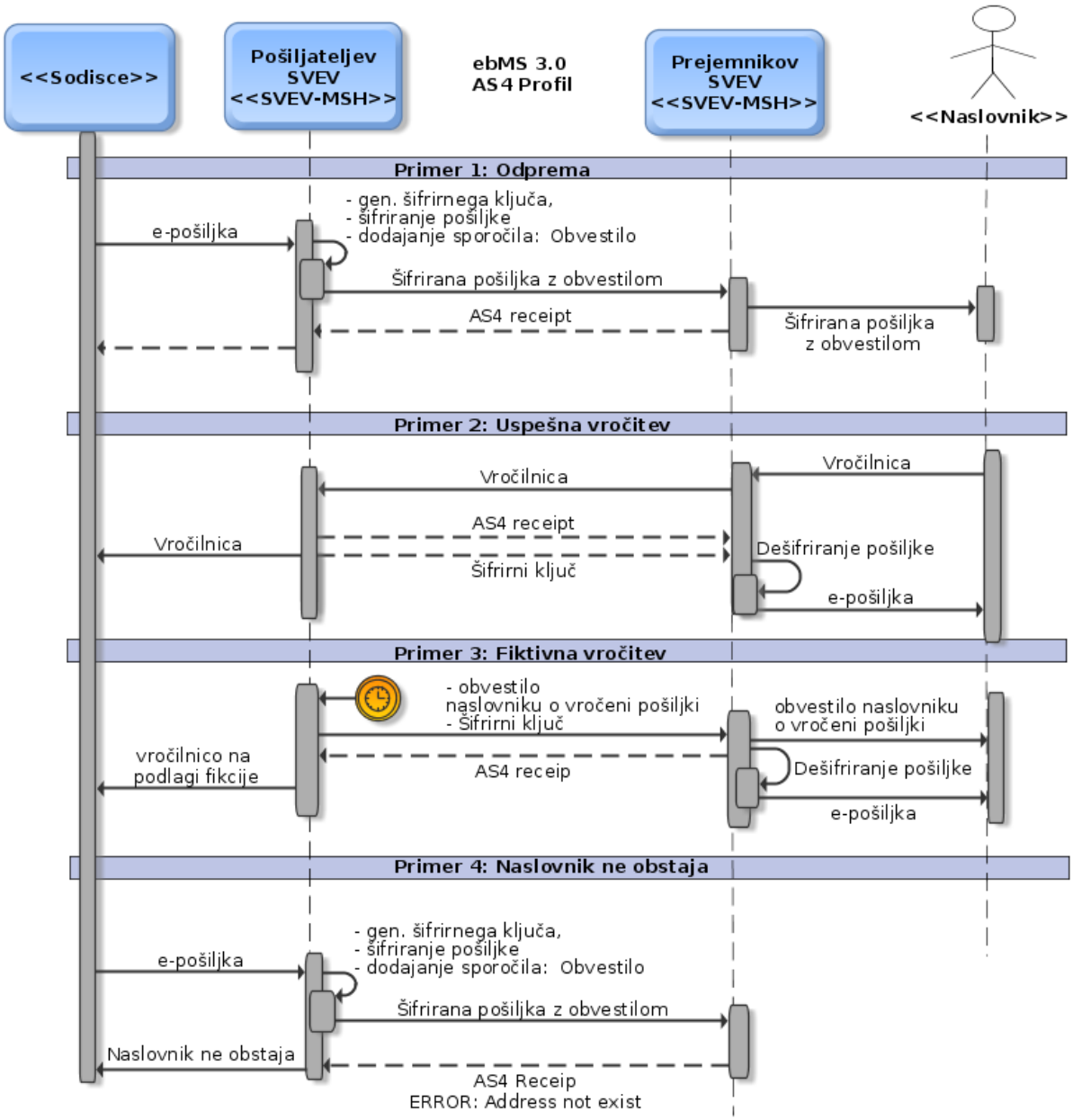
1. ***varen elektronski podpis*** v 4. točki 2. člena ZEPEP.
2. ***časovni žig*** v 5. točki 2. člena ZEPEP.
3. ***kvalificirano potrdilo*** v 19. točki 2. člena ZEPEP.
4. ***elektronska priloga v*** 2. točki prvega odstavka 5. člena PEPCSP.
5. ***odpravek elektronskega sodnega pisanja*** v 4. točki prvega odstavka 6. člena PEPCSP.
6. ***elektronska pošiljka*** (v nadaljevanju: e-pošiljka) v 25. členu PEPCSP.
7. ***obvestilo o prispeli elektronski pošiljki*** v 26. členu PEPCSP.
8. ***elektronska vročilnica*** (v nadaljevanju: vročilnica) v 27. členu PEPCSP.
9. ***potrdilo o opravljeni elektronski vročitvi na podlagi fikcije*** v 28. členu PEPCSP.
10. ***Informacijski sistem za varno elektronsko vročanje*** (v nadaljevanju: SVEV) v drugem odstavku 7. člena PEPCSP.
11. ***Modul e-poštna knjiga*** (v nadaljevanju: ePK) v sedmem odstavku 7. člena PEPCSP.
12. ***Povratnica*** je vročilnica, fikcija ali obvestilo o vrnjeni pošiljki.
13. ***Varen elektronski predal*** (v nadaljevanju: e-predal) v šestem odstavku 7. člena PEPCSP**.**

## 1.2 Struktura dokumenta

V prvem delu je predstavljen postopek vročanja ter možni primeri vročanja, kot so uspešna odprema in vrnjena pošiljka ter uspešna vročitev in fiktivna vročitev. Sledi podrobnejši tehnični opis izvedbe vročanja.

# 2 Elektronsko vročanje v e-predal

V nadaljevanju je opisan postopek vročanja v e-predal ter izmenjava sporočil/dokumentov med SVEV in ePK.




*Slika 1: Primeri vročanja*

**1. Primer: Uspešna vročitev:**
Sodišče izdela e-pošiljko tako, da določi vsebino (sodni odpravek), naslovnika (naslovnikov e-predal) in način vročitve ter pošiljko posreduje v sistem za odpremo (Pošiljateljev SVEV). Pošiljki se določi šifrirni ključ ter se vsebine šifrirajo. Nato se zgenerira: **obvestilo naslovniku o prispeli pošiljki** (glej poglavje: 3.3). Pošiljka se posreduje v prejemnikov SVEV, kjer se z obvestilom dostavi v naslovnikov e-predal.

Naslovnik prevzame e-pošiljko tako, da podpiše **vročilnico** (glej poglavje: 3.4) s kvalificiranim potrdilom naslovnika. Podpisano vročilnico naslovnikov SVEV dostavi v »pošiljateljev SVEV«.

Kot odgovor pošiljateljev SVEV vrne ključ za dešifriranje pošiljke. Naslovnikov SVEV dešifira pošiljko in jo dostavi v e-predal naslovnika (Slika 1 - Uspešna vročitev).

**2. Primer: Fikcija vročitve:**
Primer fikcije vročitve se izvede, če v zakonsko določenem roku naslovnik e-pošiljke ne prevzame. Pošiljateljev SVEV po preteku roka izdela **obvestilo naslovniku o vročeni pošiljki** (glej poglavje: 3.6) ter jo skupaj s šifrirnim ključem dostavi v naslovnikov SVEV. Naslovnikov SVEV dešifrira izvorno pošiljko ter jo skupaj z obvestilom dostavi v naslovnikov predal. Na podlagi potrdila AS4Receipt pošiljateljev SVEV izdela tudi **vročilnico na podlagi fikcije** (glej poglavje: 3.5) in jo dostavi v izvorno aplikacijo (Slika 1 - Fikcija vročitve).

**3. Primer: Naslovnik ne obstaja**
SVEV pri prejemu e-pošiljke preveri, ali naslovnik obstaja. Če naslov v sistemu SVEV ne obstaja/ne obstaja več, vrne napako »Naslovnik ne obstaja«. Pošiljateljev SVEV na podlagi napake izdela **obvestilo o vrnjeni pošiljki** (glej poglavje: 3.2).

# 3 Obvestila v zvezi z vročanjem

V zvezi s posameznimi dejanji v postopku elektronskega vročanja izvajalec storitev varnega elektronskega vročanja pošilja sporočila:

1. obvestilo sodišču ob sprejemu e-pošiljke v SVEV: Sporočilo o potrditvi sprejema,
2. obvestilo sodišču o neobstoju naslova naslovnika ob sprejemu e-pošiljke v SVEV: Obvestilo o vrnjeni pošiljki,
3. obvestilo naslovniku, da je bila e-pošiljka vložena v njegov e-predal: Obvestilo naslovniku o prispeli pošiljki,
4. obvestilo sodišču o opravljeni vročiti, in sicer:
    - če je naslovnik podpisal vročilnico: Obvestilo sodišču o opravljeni vročitvi,
    - če naslovnik v zakonsko določenem času za prevzem e-pošiljke, le-te ne prevzame: vročilnica na podlagi fikcije,
5. obvestilo naslovniku o vročeni e-pošiljki, če naslovnik v zakonsko določenem času za prevzem e-pošiljke, le-te ne prevzame: Obvestilo naslovniku o vročeni pošiljki.

Obvestila morajo biti zapisana v PDF/A obliki.

Oblike obvestil, ki sledijo, služijo zgolj kot primeri.

## 3.1 Sporočilo sodišču o potrditvi sprejema

**SPOROČILO O POTRDITVI SPREJEMA**

**Pošiljatelj**
*< podatki o sodišču>*

**Zadeva : Potrditev sprejema dokumenta v postopek elektronskega vročanja**

Potrjujemo sprejem dokumenta z oznako
*<oznaka e-pošiljke>*

**Naša oznaka**
*<Oznaka SVEV sporočila >*

**Za naslovnika**
*< podatki o naslovniku>*

Potrjujemo, da smo v postopek elektronskega vročanja v sistem *<ponudnik e-predala>* sprejeli navedeno pošiljko, ki jo bomo vročili naslovniku v njegov varen elektronski predal v skladu z ZPP in vam po opravljeni vročitvi posredovali potrdilo – vročilnico.

Storitev : Sporočilo o sprejemu pošiljke v postopek elektronske vročitve po ZPP

Datum opravljene storitve : *<Datum opravljene storitve>*
*<Kraj nastanka obvestila>, <Datum nastanka obvestila>*

## 3.2 Obvestilo o vrnjeni pošiljki

**OBVESTILO O VRNJENI POŠILJKI**

**Pošiljatelj**
*< podatki o sodišču>*

**Zadeva : Naslov pošiljke ne obstaja**

***Naslov: < e-predal naslovnika>***
Varen elektronski predal naslovnika v sistemu <*ponudnik e-predala*> ne obstaja, zato naslovniku poslana poštna pošiljka <*oznaka e-pošiljke*> ni bila vročena.

Storitev : Sporočilo o vrnjeni pošiljki v postopku elektronske vročitve po ZPP

<*Kraj nastanka obvestila*>, <*Datum nastanka obvestila*>

## 3.3 Obvestilo naslovniku o prispeli pošiljki

**OBVESTILO O PRISPELI POŠILJKI**

**Pošiljatelj**
*< podatki o sodišču>*

**Naslovnik**
*< podatki o naslovniku>*

**Zadeva : Obvestilo o prispeli pošiljki in pravni pouk o posledicah neprevzema**

Obveščamo vas, da je v vaš varen elektronski predal dne <*datum posredovanja obvestila*> prispela pošiljka z oznako <*oznaka e-pošiljke*>.
Pošiljko lahko prevzamete v roku 15 dni v vašem varnem elektronskem predalu na naslovu <*naslov s povezavo za dostop*>. Rok za prevzem začne teči od dne <*datum posredovanja obvestila*>. Če v tem roku pošiljke ne boste prevzeli, se bo po sedmem odstavku 141.a člena ZPP s potekom tega roka vročitev štela za opravljeno.

**Naša oznaka**
<*Oznaka SVEV sporočila*>

<*Kraj nastanka obvestila*>, <*Datum nastanka obvestila*>

## 3.4 Obvestilo sodišču o opravljeni vročiti

**VROČILNICA**

**Pošiljatelj**
*< podatki o sodišču>*

**Naslovnik**
*< podatki o naslovniku>*

**Zadeva : Potrjena vročilnica po ZPP**

Naslovnik potrjujem, da sem dne *<datum elektronskega podpisa vročilnice>* sprejel pošiljko z oznako *<oznaka e-pošiljke>*.

To sporočilo je potrdilo o vročitvi pošiljke in opravljeni storitvi.

**Naša oznaka**
*<Oznaka SVEV sporočila>*

Storitev : Elektronska vročitev pošiljke po ZPP

*Datum opravljene storitve : <Datum opravljene storitve>*
*<Kraj nastanka obvestila>, <Datum nastanka obvestila>*

## 3.5 Vsebina vročilnice na podlagi fikcije

**VROČILNICA NA PODLAGI FIKCIJE**

**Pošiljatelj**
*< podatki o sodišču>*

**Naslovnik**
*< podatki o naslovniku>*

**Zadeva : Potrdilo o opravljeni vročitvi na podlagi fikcije po ZPP**

Potrjujemo,

- da je naslovnik pošiljke z oznako *<oznaka e-pošiljke>* dne *<datum posredovanja obvestila>* prejel obvestilo o tej pošiljki s pravnim poukom o posledicah neprevzema v 15 dneh,
- da naslovnik pošiljke v 15 dneh od dneva obvestila o prispeli pošiljki ni prevzel, zato se po sedmem odstavku 141.a člena ZPP šteje, da je bila vročitev opravljena dne *<datum fikcije>,*
- da je bila po poteku 15 dnevnega roka iz sistema *<ponudnik e-predala>* naslovniku pošiljka puščena v njegovem varnem elektronskem predalu in poslano obvestilo, da lahko pisanje prevzame tudi pri *< podatki o sodišču>*.

To sporočilo je potrdilo o vročitvi pošiljke in opravljeni storitvi.

**Naša oznaka**
*<določi ponudnik e-predala>*

Storitev : Elektronska vročitev pošiljke po ZPP

Datum opravljene storitve :*<Datum: ponudnik e-predala>*

| |
|---|
| *<Kraj opravljene storitve>, <Datum nastanka obvestila>* |

## 3.6 Obvestilo naslovniku o vročeni pošiljki

**OBVESTILO O VROČENI POŠILJKI**

**Pošiljatelj**
*< podatki o sodišču>*

**Naslovnik**
*< podatki o naslovniku>*

**Zadeva : Obvestilo o vročeni pošiljki kot posledica neprevzema pošiljke**

Ker pošiljke z oznako *<oznaka e-pošiljke>* niste prevzeli v roku 15 dni, se je po sedmem odstavka 141.a člena ZPP s potekom tega roka vročitev štela za opravljeno dne *<datum fikcije>*. Pošiljka je bila tega dne puščena v vašem varnem elektronskem predalu, lahko pa jo prevzamete tudi pri:*<podatki o sodišču>*.

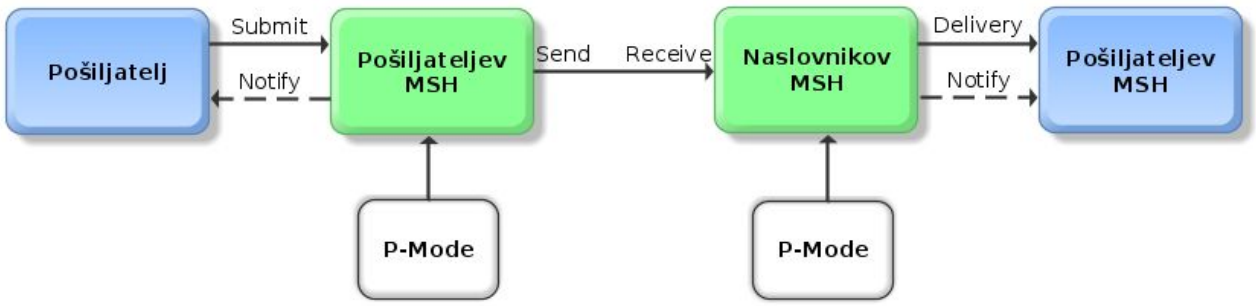
**Naša oznaka**
*<Oznaka SVEV sporočila>*

*<Kraj nastanka obvestila>, <Datum nastanka obvestila>*

# 4 Tehnična izvedba e-vročanja

Tehnična izvedba e-vročanja uporablja protokol AS4, ki temelji na (OASIS) ebMS 3.0. standardu. Prednost standarda ebMS 3.0, pred njegovim prednikom ebMS 2.0 je v tem, da je skladen z »Web Service« standardi. Enostavnost in smotrnost uporabe ebMS 3.0 za namene B2B je v tem, da združuje uveljavljene odprto-kodne web-service standarde za varno in zanesljivo izmenjavo SOAP sporočil (WS-Security, WS-Reliability, WS-ReliableMessaging, SOAP 1.2 with attachments , ...). Zasnova ebMS 3.0 je zasnovan tako, da omogoča prenos različnih mime vsebin.

Osnovni koncept izvajanja ebMS prenosa sporočil temelji na »Messaging Service Handler« (MSH), ki je abstraktno opredeljen kot izvajanje določenih funkcij pri transportu sporočil od pošiljatelja do naslovnika. Način transporta je določen v t.i. Processing Mode (P-Mode) parametrih. P-Mode parametri določajo nivo varnosti (ws-security 1.1), izvedbo robustnosti in zanesljivosti (AS4 Reception Awareness, WS-Reliability, WS-ReliableMessaging ), sporočanje napak prenosa posameznih sporočil itd. Pred pričetkom izvajanja B2B poslovanja po standardu ebMS 3.0 morata pošiljatelj in prejemnik uskladiti p-mode parametre.




*Slika 2: Model sporočanja*

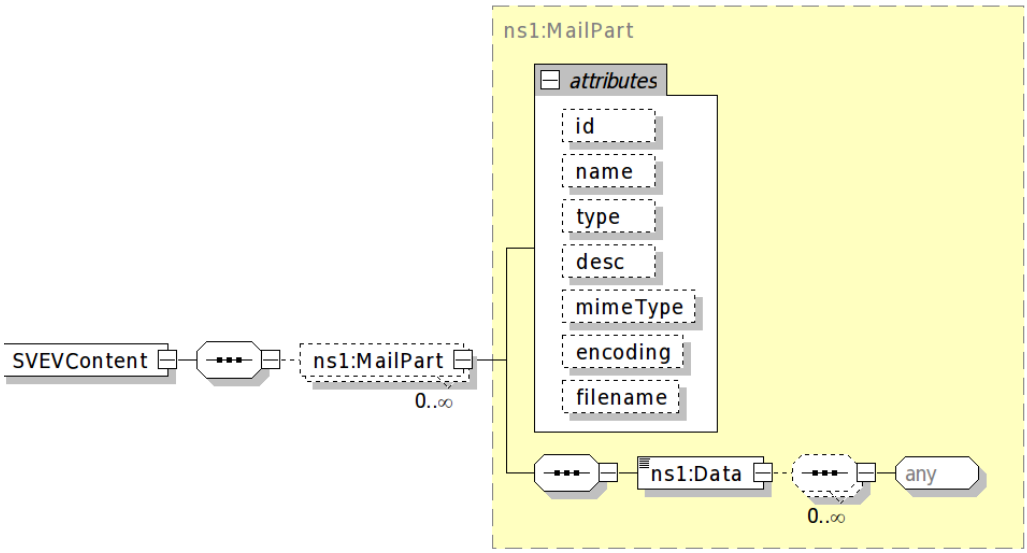
## 4.1 P-Mode konfiguracija

Pred nadaljevanjem je priporočljivo razumevanje specifikacije ebMS 3.0 (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.html) in AS4 (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.html).

V nadajevanju je opisana konfiguracijo P-Mode, ki je uporabljena za namene varnega e-vročanja.

| | |
|---|---|
| Transportni standardi | Prenos sporočil poteka preko TLS seje, ki se vzpostavi z obojestransko avtentikacijo (Mutual authentication).<br><br>TLS + HTTP 1.1 + SOAP 1.2 + WSS 1.1 |
| EbMS 3.0 MEP | One-way / Push |
| Zanesljivost: | Prejemnik sporočil kot odgovor vrača AS4Receipt ali Exception signal. V primeru SoapFault ali tcp/http ERROR, pošilatelj sporočilo poskuša ponovno poslati, tako kot to določajo »Retry« nastavitve. V primeru neuspešnega pošiljanja pošiljateljev MSH vrne pošiljatelju opozorilo o neposlani pošiljki. Prejemnikov MSH mora zaznavati »dvojnike« sporočil in jih eliminirati/ignorirati.<br><br>Nastavitve **PMode**:<br>Vsi »PUSH« klici servisov imajo v odgovoru podpisano potrdilom o prejemu AS4Receipt.<br>**PMode[1].ReceptionAwareness: true**<br>**PMode[1].Security.SendReceipt: true;**<br>**Pmode[1].Security.SendReceipt.ReplyPattern: response**<br><br>V primeru neuspešnega pošiljanja, pošiljatelj poskuša ponovno poslati izvorno sporočilo.<br>**PMode[1].ReceptionAwareness.Retry: true;**<br>Spodnja nastavitev ponovnega pošiljanja služi le kot primer – nastavitve so odvisne od funkcionalnosti aplikacije.<br>**PMode[1].ReceptionAwareness.Retry.Parameters: maxretries=10, period=2000, *exponentialBackoff=true;***<br><br>Prejemnikov MSH mora izločiti vse podvojene pošiljke. Podvojena pošiljka se zaznava na podlagi podatka: **eb:MessageInfo/eb:MessageId.**<br>Odgovor na »podvojeno pošiljko je« AS4Receipt dodatnim ***eb:SignalMessage/eb:Error*** z vrednostmi:<br>• origin: reliability<br>• category: delivery<br>• errorCode: SVEV:0201<br>• severity; warning<br>• refToMessageInError: UUID-23@sender<br>• shortDescription: First sucessfuly delivery: <čas prve dostave sporočila><br><br>Primer;<br>*<eb:Error origin="reliability" category="delivery" errorCode="SVEV:0201" severity="warning" refToMessageInError="UUID-23@sender.ebox.si" shortDescription="First sucessfuly delivery: 2014-07-25T12:19:05">*<br>*</eb:Error>*<br><br>**PMode[1].ReceptionAwareness.DuplicateDetection: true;**<br>Podvojena pošiljka detekcija zaznava za obdobje 5 let (obdobje veljavnosti |

| | |
|---|---|
| | podpisa pošiljke)<br>**PMode[1].ReceptionAwareness.DetectDuplicates.Parameters: 5y** |
| Varnost | Vsa sporočila morajo biti podpisana s pošiljateljevim spletnim certifikatom.<br><br>**PMode[1].Security.X509.Sign: true**<br>Podpisani so elementi: env:Header/eb3:Messaging in env:Body ter vse SOAP priponke.<br><br>eb3: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"/><br>soap: namespace="http://www.w3.org/2003/05/soap-envelope"/><br><br>Lastnosti podpisa:<br>**PMode[1].Security.X509.Signature.HashFunction: http://www.w3.org/2001/04/xmlenc#sha256**<br>**PMode[1].Security.X509.Signature.Algorithm:http://www.w3.org/2001/04/xmldsig-more#rsa-sha512** |
| Oznaka pošiljatelja in prejemnika | Pošiljateljev in naslovnikov predal se označuje z e-predalom, ki je sestavljen iz [naziv]@[domena ponudnika predala]<br>npr: testni.predal@e-box.si<br><br>Poleg predala je obvezen tudi naziv pošiljatelja in prejemnika.<br>Podatka predal in naziv se označuje s tipom:<br>**urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:e-box** za e-predal in<br>**urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:name** za naziv.<br><br>Primer:<br><ns2:To><br><ns2:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:name">Testko Tesnik</ns2:PartyId><br><ns2:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:e-box">testko@e-box-a.si<br></ns2:PartyId><br><ns2:Role>si-svev:receiver</ns2:Role><br></ns2:To> |
| Servisi in akcije | Način vročanja ter posamezno fazo vročanja označujeta podatka v<br>**eb:UserMessage/eb:CollaborationInfo/eb:Service**<br>in<br>**eb:UserMessage/eb:CollaborationInfo/eb:Action**<br><br>V primeru, da je vročanje koreografija izmenjave več sporočil, jih povezuje podatek: **eb:UserMessage/eb:CollaborationInfo/eb:ConversationId**, ki ima vrednost: ***eb:*UserMessage/*eb:MessageInfo/eb:MessageId*** *sporočila, ki je pričel postopek vročanja (**Action: DeliveryNotification**).*<br><br>Sporočila, ki pripadajo postopku vročanja po ZPP imajo v elementu **eb:UserMessage/eb:CollaborationInfo/eb:Service** vrednost:<br>- **LegalDelivery_ZPP**<br><br>V elementu: **eb:UserMessage/eb:CollaborationInfo/eb:Action** so lahko |

| | |
|---|---|
| | naslednje vrednosti:<br>**- DeliveryNotification:**<br>**- AdviceOfDelivery:**<br>**- FictionNotification:**<br><br>Primer:<br><eb:CollaborationInfo><br><eb:AgreementRef pmode="legal-delivery:e-box-a.si">e-box-a.si:e-box-b.si</eb:AgreementRef><br><eb:Service>Delivery_ZPP</eb:Service><br><eb:Action>DeliveryNotification</eb:Action><br><eb:ConversationId>575e09ca-e49f-4ed8-8718-759fe993b4b9</eb:ConversationId><br></eb:CollaborationInfo> |
| Prenos vsebin | Posamezne vsebine se zapišejo v XML obliko kot to določa SVEVContent.xsd.<br>  <br><br>Primer sporočila DeliveryNotification, kjer je kot prva priponka PDF vizualizacija »Obvestilo naslovniku o prispeli pošiljki«, nato sledi šifrirana vsebine.<br><br><?xml version="1.0" encoding="UTF-8"?><br><soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"<br>xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"><br><soap:Header><br><eb:Messaging S11:mustUnderstand="1"><br>...<br><eb:PayloadInfo><br><eb:PartInfo href="#svevMessage-1" /><br><eb:PartInfo href="#content_1" /><br></eb:PayloadInfo><br></eb:Messaging><br></soap:Header><br><soap:Body ><br><ns2:SVEVMail xmlns:ns2="http://jmsh.org/schemas/svevmail" ><br><ns2:MailPart id="svevMessage-1" encoding="base64" mimeType="application/pdf"<br>name="DeliveryNotification"><br><ns2:Data>JVBERi0xLjQKJaqrrK0KNCAwIG9iag ... </ns2:Data><br></ns2:MailPart><br><ns2:MailPart id="content_1" desc="Legal delivery encrypted data" encoding="UTF-8"<br>mimeType="application/xml" name="EncryptedData"><br><ns2:Data><br><ns3:EncryptedData Encoding="UTF-8" MimeType="text/plain"><br><ns3:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/><br><ns4:KeyInfo Id="72bft7d60utlf18vihg2qr"/><br><ns3:CipherData><br><ns3:CipherValue>rIlCvt//zsatNLyA7gsAJgAmx4b1ptpq4Uet3kS5GpU=</ns3:CipherValue><br></ns3:CipherData><br></ns3:EncryptedData><br></ns2:Data> |

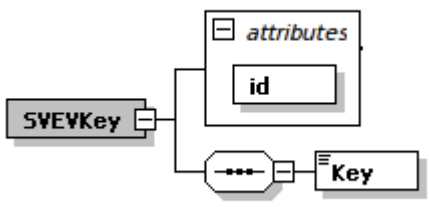
```
            </ns2:MailPart>
        </ns2:SVEVMail>
    </soap:Body>
```

Alternativa uporabi sheme svevmail.xsd je uporaba standarda »SOAP with attachment«, kjer se vsebine dodajo v SOAP request kot »mime part«

```
Content-Type: Multipart/Related; boundary=MIME_boundary; type=text/xml;
                start="<123456@ebox-a.si>"

--MIME_boundary
Content-Type: text/xml; charset=UTF-8
Content-Transfer-Encoding: 8bit
Content-ID: <123456@ebox-a.si>

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope/"
xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/">
   <soap:Header>
      <eb:Messaging S11:mustUnderstand="1">
...
          <eb:PayloadInfo>
             <eb:PartInfo href="#svevMessage-1" />
             <eb:PartInfo href="#content_1" />
          </eb:PayloadInfo>
      </eb:Messaging>
   </soap:Header>
   <soap:Body />
 </soap:Envelope>


--MIME_boundary
Content-Type: application/pdf
Content-Transfer-Encoding: binary
Content-ID: svevMessage-1
...binary »PDF Notification«

--MIME_boundary—
Content-Type: text/xml; charset=UTF-8
Content-Transfer-Encoding: 8bit
Content-ID: content_1

 <ns3:EncryptedData Encoding="UTF-8" MimeType="text/plain">
   <ns3:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
   <ns4:KeyInfo Id="72bft7d60utlf18vihg2qr"/>
   <ns3:CipherData>
      <ns3:CipherValue>rIlCvt//zsatNLyA7gsAJgAmx4b1ptpq4Uet3kS5GpU=</ns3:CipherValue>
   </ns3:CipherData>
</ns3:EncryptedData>

--MIME_boundary—
```

## 4.2 Prenos šifrirnega ključa

Šifrirni ključ naslovnik MSH prejme v odgovoru pri oddaji »Vročilnice« (Action: AdviceOfDelivery) ali ob sprejemu fiktivne vročilnice (Action: FictionNotification). Ključ je shranjen v shemi **svevkey.xsd**, kjer je ***SVEVKey/@id*** enak vrednosti ***EncryptedData/KeyInfo/@Id***




*Slika 3: SVEV key shema*

Primer kritpirane priponke in pripadajočega ključa:
Kriptirana vsebina:

```
<?xml version="1.0" encoding="UTF-8"?>
<ns3:EncryptedData Encoding="UTF-8" MimeType="text/plain">
   <ns3:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
   <ns4:KeyInfo Id="72bft7d60utlf18vihg2qr"/>
   <ns3:CipherData>
      <ns3:CipherValue>rIlCvt//zsatNLyA7gsAJgAmx4b1ptpq4Uet3kS5GpU=</ns3:CipherValue>
   </ns3:CipherData>
</ns3:EncryptedData>
```

Pripadajoči ključ:

```
<?xml version="1.0" encoding="UTF-8"?>
<SVEVKey id="72bft7d60utlf18vihg2qr" xmlns="http://jmsh.org/schemas/legaldelivery"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <Key>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</Key>
</SVEVKey>
```