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	1.2
Datum	08.06.15
Avtor	Jože Rihtaršič
Odgovornost	Bojan Muršec
Zaupnost	/
Datoteka	

ZGODOVINA:

Verzija	Datum	Avtor	Opis
1.0	01.08.14	Jože Rihtaršič	Dokument kreiran.
1.1	03.03.15	Jože Rihtaršič	Spremenjeno besedilo sporočila: - Sporočilo sodišču o potrditvi sprejema - Obvestilo o vrnjeni pošiljki Dodana zahteva v poglavju 3.: podpisana s kvalificiranim potrdilom strežnika, na katerem teče SVEV pošiljatelja oziroma naslovnika.
1.2	08.06.2015	Jože Rihtaršič	Dodan opis asimetričnega šifriranja ključa za dešifriranje pošiljke pri uspešni vročitvi in vročitvi na podlagi fikcije. Spremenjen način pakiranja vsebine. Vsebina se v SOAP sporočilo dodaja kot MIME priponke.

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. ***povratnica*** je vročilnica, fikcija ali obvestilo o vrnjeni pošiljki;
12. ***varen elektronski predal*** (v nadaljevanju: e-predal) v šestem odstavku 7. člena PEPCSP***;***

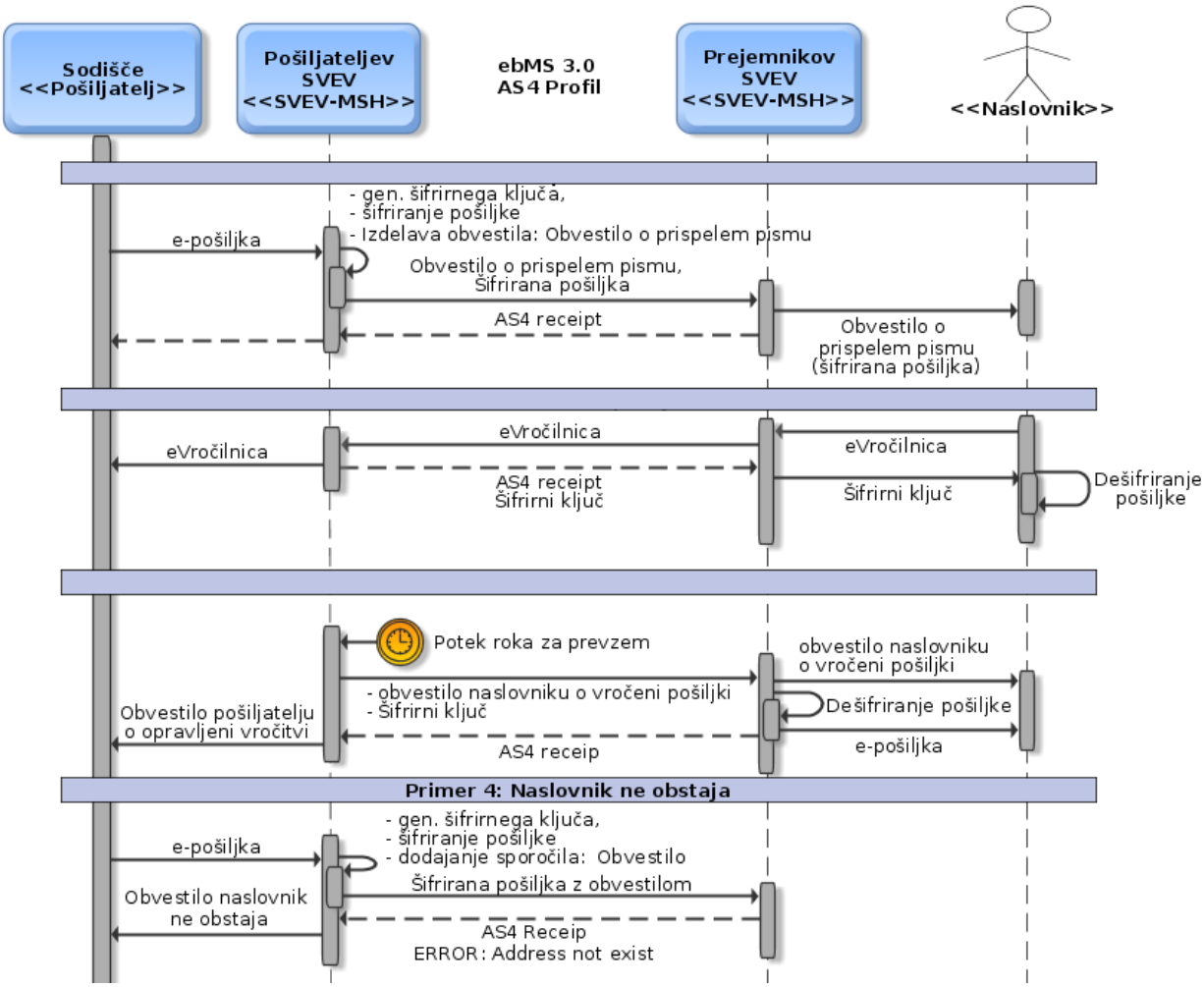
1.2 Struktura dokumenta

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 moduli.

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 s katerim se šifrirajo vsebine. Nato se zgenerira in doda pošiljki: **obvestilo naslovniku o prispeli pošiljki** (glej poglavje: 3.3). Pošiljka se posreduje v prejemnikov SVEV, ki takoj ob prejemu obvestilo s šifriranimi vsebinami dostavi v naslovnikov e-predal. Pošiljateljevem SVEV sistemu pa posreduje elektronsko podpisano potrdilo, ki vsebuje čas prejema in zgostitvene vrednosti prejetih dokumentov (AS4 povratnica). Na podlagi prejetega potrdila, pošiljateljev SVEV po potrebi izdela vizualizacijo „Potrdilo o prejemu“ (glej poglavje:3.1).

Naslovnik prevzame e-pošiljko tako, da podpiše **vročilnico** (glej poglavje: 3.4) s kvalificiranim potrdilom naslovnika. Podpisano vročilnico prejemnikov SVEV dostavi v »pošiljateljev SVEV«. Kot odgovor pošiljateljev SVEV vrne ključ za dešifriranje pošiljke. Ključ je asimetrično šifiriran z javnim ključem podpisnikovega certifikata, ki je sestavni del vročilnice. Naslovnikov SVEV dostavi ključ v e-predal naslovnika in mu nudi orodja za dešifriranje dohodne pošte. (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. Ključ je asimetrično šifriran s prejemnikovim SVEV certifikatom, ki se uporablja za vzpostavitev TLS seje. Prejemnikov SVEV dešifrira izvorno pošiljko ter jo skupaj z obvestilom dostavi v naslovnikov e-predal. Na podlagi potrdila o prejemu pošiljke v vročanje (AS4 receipt) 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 se uporabljajo naslednje vizualizacije sporočil:

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 varni 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 ter morajo biti podpisana s kvalificiranim potrdilom strežnika, na katerem teče SVEV pošiljatelja oziroma naslovnika.

Oblike obvestil, ki sledijo, služijo zgolj kot primeri.

3.1 Sporočilo 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 po Zakonu o pravdnem postopku v sistem *<ponudnik e-predala>* sprejeli navedeno pošiljko, ki jo bomo dostavili v naslovnikov varni elektronski predal. Po opravljeni vročitvi vam bomo posredovali potrdilo o opravljeni elektronski vročitvi.

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 mu na tem naslovu elektronske vročitve pošiljke <*oznaka e-pošiljke*> ni mogoče opraviti.

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*>

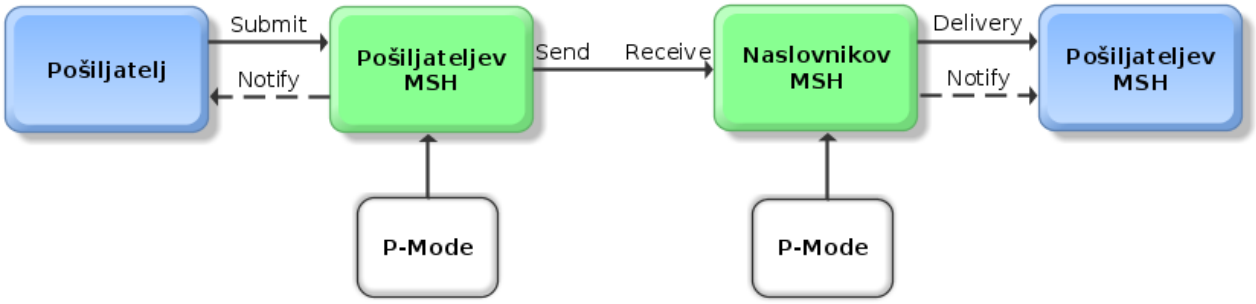
<*Kraj nastanka obvestila*>, <*Datum nastanka obvestila*>

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



vir: OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features

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). TLS + HTTP 1.1 + SOAP 1.2 + WSS 1.1 + SOAP with Attachments
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. Nastavitve **PMode**:

	Vsi »PUSH« klici servisov imajo v odgovoru podpisano potrdilom o prejemu AS4Receipt. **PMode[1].ReceptionAwareness: true** **PMode[1].Security.SendReceipt: true;** **Pmode[1].Security.SendReceipt.ReplyPattern: response** V primeru neuspešnega pošiljanja, pošiljatelj poskuša ponovno poslati izvorno sporočilo. **PMode[1].ReceptionAwareness.Retry: true;** Spodnja nastavitev ponovnega pošiljanja služi le kot primer – nastavitve so odvisne od funkcionalnosti aplikacije. **PMode[1].ReceptionAwareness.Retry.Parameters: maxretries=10, period=2000, e*xponentialBackoff=true;*** Prejemnikov MSH mora izločiti vse podvojene pošiljke. Podvojena pošiljka se zaznava na podlagi podatka: **eb:MessageInfo/eb:MessageId.** Odgovor na »podvojeno pošiljko je« AS4Receipt dodatnim ***eb:SignalMessage/eb:Error*** z vrednostmi: • origin: reliability • category: delivery • errorCode: SVEV:0201 • severity; warning • refToMessageInError: UUID-23@sender • shortDescription: First sucessfuly delivery: <čas prve dostave sporočila> Primer; *<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">* *</eb:Error>* **PMode[1].ReceptionAwareness.DuplicateDetection: true;** Podvojena pošiljka detekcija zaznava za obdobje 5 let (obdobje veljavnosti podpisa pošiljke) **PMode[1].ReceptionAwareness.DetectDuplicates.Parameters: 5y**
Varnost	Vsa sporočila morajo biti podpisana s pošiljateljevim spletnim certifikatom. **PMode[1].Security.X509.Sign: true** Podpisani so elementi: env:Header/eb3:Messaging in env:Body ter vse SOAP priponke. eb3: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"/> soap: namespace="http://www.w3.org/2003/05/soap-envelope"/> 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**
Oznaka pošiljatelja in prejemnika	Pošiljateljev in naslovnikov predal se označuje z e-predalom, ki je sestavljen iz [naziv]@[domena ponudnika predala] npr: testni.predal@e-box.si

	Poleg predala je obvezen tudi naziv pošiljatelja in prejemnika. Podatka predal in naziv se označuje s tipom: **urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:e-box** za e-predal in **urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:name** za naziv. Primer: <ns2:To> <ns2:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:name">Testko Tesnik</ns2:PartyId> <ns2:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-svev:e-box">testko@e-box-a.si</ns2:PartyId> <ns2:Role>si-svev:receiver</ns2:Role> </ns2:To>
Servisi in akcije	Način vročanja ter posamezno fazo vročanja označujeta podatka v **eb:UserMessage/eb:CollaborationInfo/eb:Service** in **eb:UserMessage/eb:CollaborationInfo/eb:Action** 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**).* Sporočila, ki pripadajo postopku vročanja po ZPP imajo v elementu **eb:UserMessage/eb:CollaborationInfo/eb:Service** vrednost: **- LegalDelivery_ZPP** V elementu: **eb:UserMessage/eb:CollaborationInfo/eb:Action** so lahko naslednje vrednosti: **- DeliveryNotification:** **- AdviceOfDelivery:** **- FictionNotification:** Primer: <eb:CollaborationInfo> <eb:AgreementRef pmode="legal-delivery:e-box-a.si">e-box-a.si:e-box-b.si</eb:AgreementRef> <eb:Service>Delivery_ZPP</eb:Service> <eb:Action>DeliveryNotification</eb:Action> <eb:ConversationId>575e09ca-e49f-4ed8-8718-759fe993b4b9</eb:ConversationId> </eb:CollaborationInfo>
Prenos vsebin	Posamezne vsebine se v SOAP sporočilo dodajo na način kot to določa standarda »SOAP with attachment« ------=_Part_1_1083973693.1428143691672 Content-Type: application/soap+xml; charset=utf-8 <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"> ... <ns3:PayloadInfo> <ns3:PartInfo href="cid:42eb013c-0606-4d6b-a84f-d71590d2e758@ebox.test.si"/>

	</ns3:PayloadInfo> </eb:Messaging> </soap:Header> <soap:Body /> </soap:Envelope> ------=_Part_1_1083973693.1428143691672 Content-Type: image/png Content-ID: <42eb013c-0606-4d6b-a84f-d71590d2e758@ebox.test.si> Content-Transfer-Encoding: binary id: 42eb013c-0606-4d6b-a84f-d71590d2e758@ebox.test.si PNG # ### IHDR### ...

4.2 Prenos šifrirnega ključa

Šifrirni ključ prejemnikov MSH prejme v odgovoru pri oddaji »Vročilnice« (Action: AdviceOfDelivery) ali ob sprejemu fiktivne vročilnice (Action: FictionNotification). Vsebine, ki se vročajo so simetrično šifrirane, vendar je ključ za dešifriranje vsebin pri prenosu asimetrično šifriran. V primeru vročilnice, je ključ asimetrično šifriran z javnim ključem s katerim je podpisana vročilnica (javni ključ podpisnika je sestavni del vročilnice). V primeru fikcije vročitve je simetrični ključ šifriran z naslovnikovim SVEV certifikatom, ki se uporablja za vzpostavitev TLS seje. Ključ je shranjen kot določa standard: XML Encryption Syntax and Processing (http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#ref-XML-Schema)

Primer kritpirane priponke in pripadajočega ključa:
Kriptirana vsebina:

```
<?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>
```

Pripadajoči ključ:

```
<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>
```