REPUBLIKA
SLOVENIJA
VRHOVNO
SODIŠČE

CENTER ZA INFORMATIKO

Funkcionalne in tehnične zahteve za e-vlaganje v varni elektronski predal sodišča

Verzija 1.0

EVROPSKA UNIJA
EVROPSKI
SOCIALNI SKLAD

SLOVENSKO
sodstvo 2020

UČINKOVITO
PRAVOSODJE

KONTROLA VERZIJ

ZADNJA VERZIJA:

Verzija	1.0.1
Datum	26. 04. 2024
Pripravil	VSRS CIF
Odgovorna oseba	VSRS CIF (kontakt: Žiga Kosec)
Zaupnost	/
Datoteka	

ZGODOVINA:

Verzija	Datum	Avtor	Opis
0.1	19. 01. 2018	VSRS CIF	Dokument kreiran.
1.0.0	5.05.2022	Žiga Kosec	Začetni dokument dopolnjen.
1.0.1	26.4.2024	Žiga Kosec	Spremenjen potek vlaganja in xml z metapodatki

REVIZIJE:

Revizija	Datum	Avtor	Opis

ZAŠČITA DOKUMENTA

Kazalo vsebine

1. Uvod

1.1. Namen

Namen dokumenta je opisati tehnične zahteve in arhitekturo sistema za elektronsko vlaganje sodstva (odložišče e-sodstvo) ter postopek vlaganja v varne elektronske predale sodstva. Izvedba elektronskega vlaganja temelji na standardu OASIS ebMS 3.0 oz. njegovem profilu eDelivery-AS4.

1.2. Struktura dokumenta

V začetnem delu dokumenta sta kratka opisa namena uporabe standardov OASIS ebMS 3.0 in eDelivery-AS4. Nato sledi opis postopka elektronskega vlaganja. V zadnjem delu je opis tehničnega standarda za prenos sporočil.

1.3. Pojmi uporabljani v dokumentu

Izrazi, uporabljeni v dokumentu, pomenijo:

1. **»IS«** pomeni informacijski sistem,
2. **»kvalificirano potrdilo«** je kvalificirano potrdilo za elektronski podpis, kvalificirano potrdilo za elektronski žig ali kvalificirano potrdilo za avtentikacijo spletišč (5. točka prvega odstavka Zakona o elektronski identifikaciji in storitvah zaupanja),
3. **»varen elektronski predal«** je elektronski naslov uporabnika v informacijskem sistemu za varno elektronsko vročanje, ki ga upravlja izvajalec storitev varnega elektronskega vročanja (četrti odstavek 7. člena Pravilnika o elektronskem poslovanju v civilnih sodnih postopkih in v kazenskem postopku oz. PEPCSPiKP),
4. **»ponudnik storitve elektronskega vlaganja"** pomeni isto kot »izvajalec storitev varnega elektronskega vročanja«, kar pomeni, da informacijski sistem za varno elektronsko vročanje (ali vlaganje) upravlja oseba, ki ima dovoljenje ministra za pravosodje za varno elektronsko vročanje (v nadaljnjem besedilu tudi: IS odprava) (drugi odstavek 7. člena PEPCSPiKP),
5. **»odložišče e-sodstvo«** so spletne storitve informacijskega sistema e-sodstvo, ki omogočajo vlaganje vlog v civilnih sodnih postopkih in kazenskem postopku (v nadaljnem besedilu tudi: IS dostava) (tretji odstavek 2. člena PEPCSPiKP),
6. **»modul e-vpisnik«** je modul za podporo vodenja elektronskega vpisnika v civilnih sodnih postopkih in v kazenskem postopku (3. točka prvega odstavka 2. člena PEPCSPiKP),
7. **»varnostna shema«** je modul informacijskega sistema e-sodstvo, ki omogoča: 1) podeljevanje in odvzemanje pooblastil glede vrste e-opravil, ki so jih upravičene izvajati posamezne podskupine uporabnikov (v nadaljnjem besedilu: upravljanje pooblastil uporabnikov), in

2) podeljevanje in odvzemanje pooblastil administratorjem posamezne skupine ali podskupine uporabnikov (v nadaljnjem besedilu: upravljanje pooblastil administratorjem) (4. člen PEPCSPiKP),

8. **»digitalna vsebina«** so tako sodna pisanja kot strojno berljive datoteke, ki jih pošiljatelj želi vročiti naslovniku,
9. **»elektronska pošiljka«** je skupek digitalnih vsebin z določenim pošiljateljem, naslovnikom in postopkom vročanja,
10. **»elektronsko sporočilo«** so vsa elektronska sporočila (elektronska pošiljka, napake, ...), ki jih v postopku elektronskega vročanja izmenjata IS odprava in IS dostava.
11. **»uporabniški agent«** je IS, s pomočjo katerega uporabnik pripravi vlogo in prične postopek oddaje elektronske vloge na sodišče.

2. Uporaba odprto-kodnih standardov pri elektronskem vlaganju

Elektronska izmenjava podatkov med podjetji in organizacijami ni novost v modernem poslovanju. Znano je, da elektronsko poslovanje prinaša mnogo prednosti, vendar se manj govori o tem, da postaja vzdrževanje integracij z naraščanjem števila e-storitev in števila partnerjev, s katerimi poslujemo po elektronski poti, vedno večji strošek ter vedno večji arhitekturni in produkcijski zalogaj. Vrhovno sodišče RS pričakuje povečanje e-poslovanja sodišč z različnimi strankami, kot so: odvetniki, tožilci, notarji, banke, zavarovalnice... Večina večjih strank ima lastne informacijske sisteme, zato komunikacija preko portalov ni tako učinkovita kot možnost neposredne integracije informacijskih sistemov.

Eden izmed informacijskih izzivov Vrhovnega sodišča RS je izbira primerne arhitekture, tehnologij in standardov za e-poslovanje, ki bi omogočalo dinamično dodajanje/spreminjanje storitev ali partnerjev brez programiranja. Pri tem je smiselno iskati rešitve, ki so splošno sprejete, cenovno dostopne in preproste za uporabo. Poleg tega je smotrno upoštevati smernice Evropske komisije, ki so se oblikovale pri vzpostavljanju enotnega digitalnega trga Evrope. Za ta namen je bilo v preteklosti izdelanih kar nekaj projektov, v katerih so sodelovali strokovnjaki, gospodarstveniki in predstavniki javnega sektorja iz večjega števila članic EU. Cilj projektov je bil izdelava infrastrukture za čezmejno elektronsko poslovanje na področju javnega naročanja, zdravstva, javne uprave. Kot najprimernejši standard za elektronsko izmenjavo podatkov in dokumentov se je uveljavil standard OASIS ebMS 3.0 oz. njegov profil eDelivery-AS4.

2.1. Standard ebMS 3.0 in njegov profil eDelivery-AS4

Standard ebMS 3.0 predpisuje komunikacijsko nevtralen mehanizem, ki temelji na SOAP sporočilih in rešuje tehnična vprašanja glede naslavljanja, varnosti, zanesljivosti prenosa, preverjanja avtentičnosti sporočil itd. Osnovni koncept komunikacije oziroma vročanja temelji na implementaciji transportnega modula, t. im. »Messaging Service Handler« (v

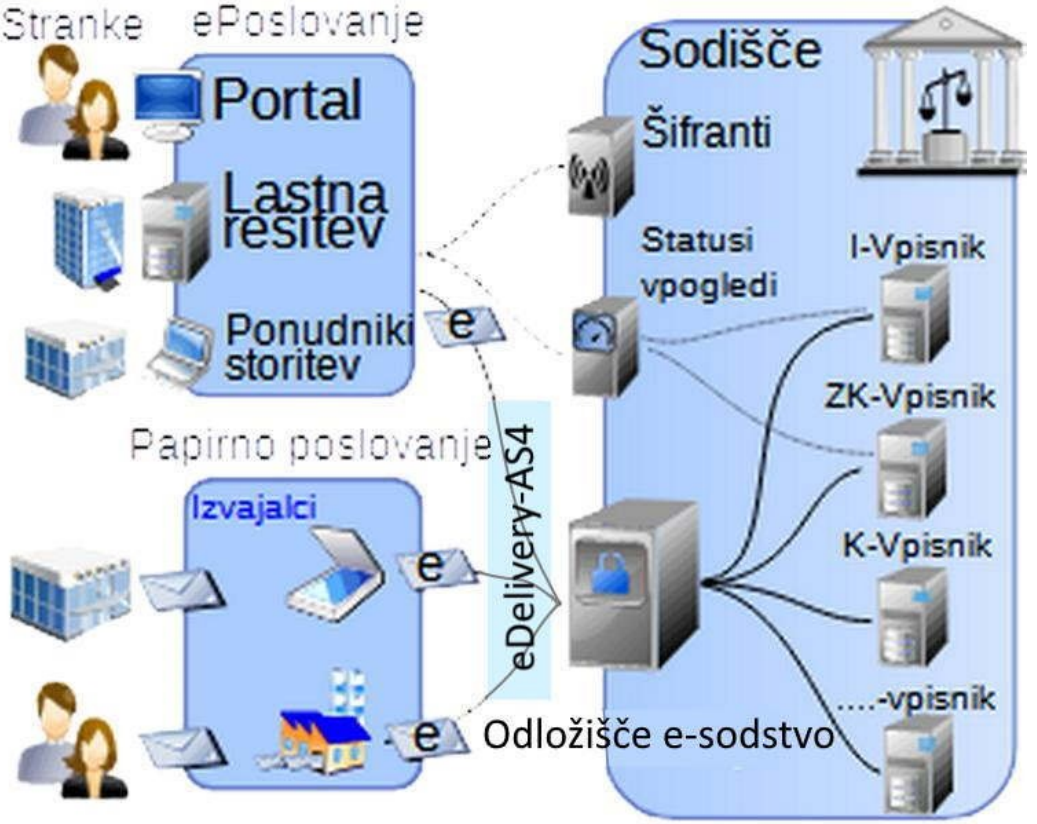
nadaljevanju MSH). Par MSH modulov izvaja transport sporočil med prejemnikom in naslovnikom na varen in zanesljiv način .

Standard predpisuje nabor parametrov, to so t. im. P-Mode parametri (angl. *Processing Mode*), s katerimi lahko določamo nivo in parametre varnosti in zanesljivosti transporta med MSH moduli, ter način naslavljanja in preverjanja tipov priponk v sporočilu. Parametri omogočajo izdelavo univerzalnega MSH modula za izdelavo novih integracij in poslovnih koreografij izmenjave sporočil brez poseganja v programsko kodo MSH modula. Parametri P-Mode so razporejeni v šest vsebinsko povezanih kategorij:

- **splošni parametri:** 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.

S ciljem izdelave enotnega digitalnega trga Evrope se je oblikoval profil uporabe standarda ebMS 3.0 za prenos sporočil: eDelivery-AS4, ki je upoštevan v tehničnih specifikacijah elektronskega vlaganja.

3. Elektronsko vlaganje



Slika 1: Arhitektura sistema za elektronsko vlaganje

3.1. Vsebine elektronskega vlaganja

V elektronski obliki se na sodišče vlagajo vsebine v PDF obliki, ki so namenjene ročni interpretaciji in obdelavi.

PDF-ji morajo ustrezati naslednjim pogojem:
- morajo biti skladni s PDF/A
- morajo biti črno-beli
- ločljivost mora biti med 240dpi in 300 dpi
- velikost posameznih dokumentov ne sme biti večja od 15mb
- skupna velikost pošiljke ne sme biti večja od 100mb
- vodilni dokument (vloga) mora biti digitalno podpisan s strani vlagatelja

Zraven mora biti obvezno priložena tudi xml datoteka z metapodatki (t.j. podatki o pošiljki), ki omogočajo nadaljnjo avtomatsko krmiljenje pošiljke znotraj sistema e-sodstva. To xml datoteko se uporabi tudi za časovno žigosanje pošiljke.

V njej so navedeni naslednji podatki (za podrobnosti glej 4.4):
- sodišče, ki obravnava zadevo
- opravilna številka zadeve (v primeru obstoječe zadeve) *ali* pravno področje (v primeru nove zadeve)
- seznam vloženih pdf dokumentov (z zgostitvenimi vrednostmi le-teh), pri čemer je označeno, kateri dokument je vodilen in kaj so priloge (če so).
- če se vlaga preko ponudnika storitev elektronskega vlaganja, je lahko v xml datoteki prisoten tudi časovno žigosan digitalni podpis (v tem primeru se datum časovnega žiga šteje za datum oddaje)

3.2. Akterji

- **Vlagatelj/Uporabnik**: Stranka sodišča, ki želi oddati elektronsko vlogo.
- **Uporabniški agent** (V nadaljevanju tudi: UA): Aplikacija/sistem, sestavljen iz komponent programske in/ali strojne opreme, s pomočjo katere uporabnik pripravi vlogo in prične postopek oddaje elektronske vloge na sodišče. UA je lahko:
    - **Ponudnik storitve elektronskega vlaganja**: komercialni ponudniki sistema za e-vlaganje tržijo spletne storitve za izdelavo in urejanje eVlog ter njihovo vlaganje na sodišče.
    - **Rešitev „po meri“ oz. lastna rešitev**: stranke sodišča nadgradijo lastne zaledne informacijske sisteme za sestavljanje in vlaganje eVlog na sodišče.
- **Odložišče e-sodstvo**: spletne storitve informacijskega sistema e-sodstvo, ki omogočajo vlaganje vlog v civilnih sodnih postopkih in kazenskem postopku.
- **eVpisnik**: Sistem/modul za podporo vodenja elektronskega spisa v posamezni vrsti sodnega postopka.
- **Ponudnik storitve časovnega žigosanja**: Izdajatelj kvalificiranih elektronskih časovnih žigov. UA in odložišče e-sodstvo lahko uporabljata različne ponudnike izdajateljev kvalificiranih elektronskih časovnih žigov.

3.3. Postopek odddaje

- **Korak 1**: Uporabnik s pomočjo uporabniškega agenta sestavi elektronsko vlogo (v nadaljevanju: eVloga).
- **Korak 2**: Pred oddajo je priporočena kontrola datotek za pošiljanje[1]. Preveriti je treba, če:
    - je PDF glavnega dokumenta (vloge) podpisan in podpis veljaven
    - dokumenti so tipa PDF ali xml
    - PDF-ji so skladni s PDF/A
    - PDF-ji so črno beli, ločljivost PDF-jev je med 240dpi in 300dpi[2]
    - posamezni dokumenti ne presegajo velikost 15mb

1 Oddajanje je možno tudi brez predhodne kontrole, vendar je v interesu vlagatelja, da se ga čim prej opozori na morebitno neustreznost vloge.

2 S tem se se preprečuje preveliko velikost PDF dokumentov.

- skupna velikost vseh dokumentov ne presega velikost 100MB

- **Korak 3**: Nato UA izdela ustrezno spremljajočo XML datoteko z metapodatki pošiljke. Zanjo mora od vlagatelja pridobiti naslednje podatke:
  - sodišče, ki (naj) obravnava zadevo [iz šifranta]
  - opravilno številko zadeve [ustreznega formata] ali pa pravno podpodročje [iz šifranta]
  - kateri od priloženih dokumentov je vodilni (vloga)
- **Koraki 4-6**: (ti koraki so priporočeni, a nenujni, za ponudnike storitev elektronskega vlaganja, niso pa dovoljeni za rešitve "po meri"[3]) UA elektronsko podpiše XML datoteko in podpis časovno žigosa z uporabo storitve izdajatelja kvalificiranih elektronskih časovnih žigov. Časovno žigosano eVlogo mora UA samodejno in v najkrajšem možnem času oddati na sodišče (odložišče e-sodstvo).[4] Vloga se šteje za oddano na sodišče z datumom časovnega žiga.
- **Koraka 7-8**: UA pošlje vlogo preko svojega MSH v odložišče e-sodstvo.
- **Koraki 9-11**: Odložišče e-sodstvo v odgovoru "Uporabniškemu agentu" (preko njegovega MSH) vrne AS4 potrdilo o prejemu, UA pa vlagatelja obvesti, da je bila vloga sprejeta.
- **Korak 12**: Ob prejemu vloge odložišče e-sodstvo izvede *kontrolo tehnične ustreznosti* pošiljke.

  Pošiljka je tehnično neustrezna, če:
  - ne vsebuje obvezne xml datoteke z metapodatki pošiljke
  - xml datoteka z metapodatki ne vsebuje obveznih podatkov: šifre sodišča, opravilne številke ali šifre pravnega podpodročja, seznama dokumentov (kjer je natanko eden označen kot 'jeVodilni')
  - xml datoteka z metapodatki vsebuje obvezne podatke, vendar niso veljavni (format šifre sodišča, format opravilne številke, format šifre pravnega podpodročja, zgostitvene vrednosti iz seznama dokumentov ne ustrezajo priloženim dokumentom, neustrezen časovni žig, če ta prisoten)
  - priponke niso tipa PDF ali xml
  - PDF-ji niso skladni s PDF/A
  - PDF glavnega dokumenta(vloge) ni podpisan ali pa je podpis neveljaven
  - PDF-ji niso črno beli, ločljivost PDF-jev ni med 240dpi in 300dpi
  - priloge pošiljke presegajo velikost 15mb
  - skupna velikost pošiljke presega velikost 100MB

  Tudi tehnično neustrezno pošiljko sodstvo sprejme (je na tej točki ne zavrne), če jo je le zmožno sprejeti. Tako pošiljko se opremi z zabeležbo o pomanjkljivostih[5]. Vkolikor ni dovolj ustreznih podatkov za usmeritev vloge na ustrezno sodišče in vpisnik,

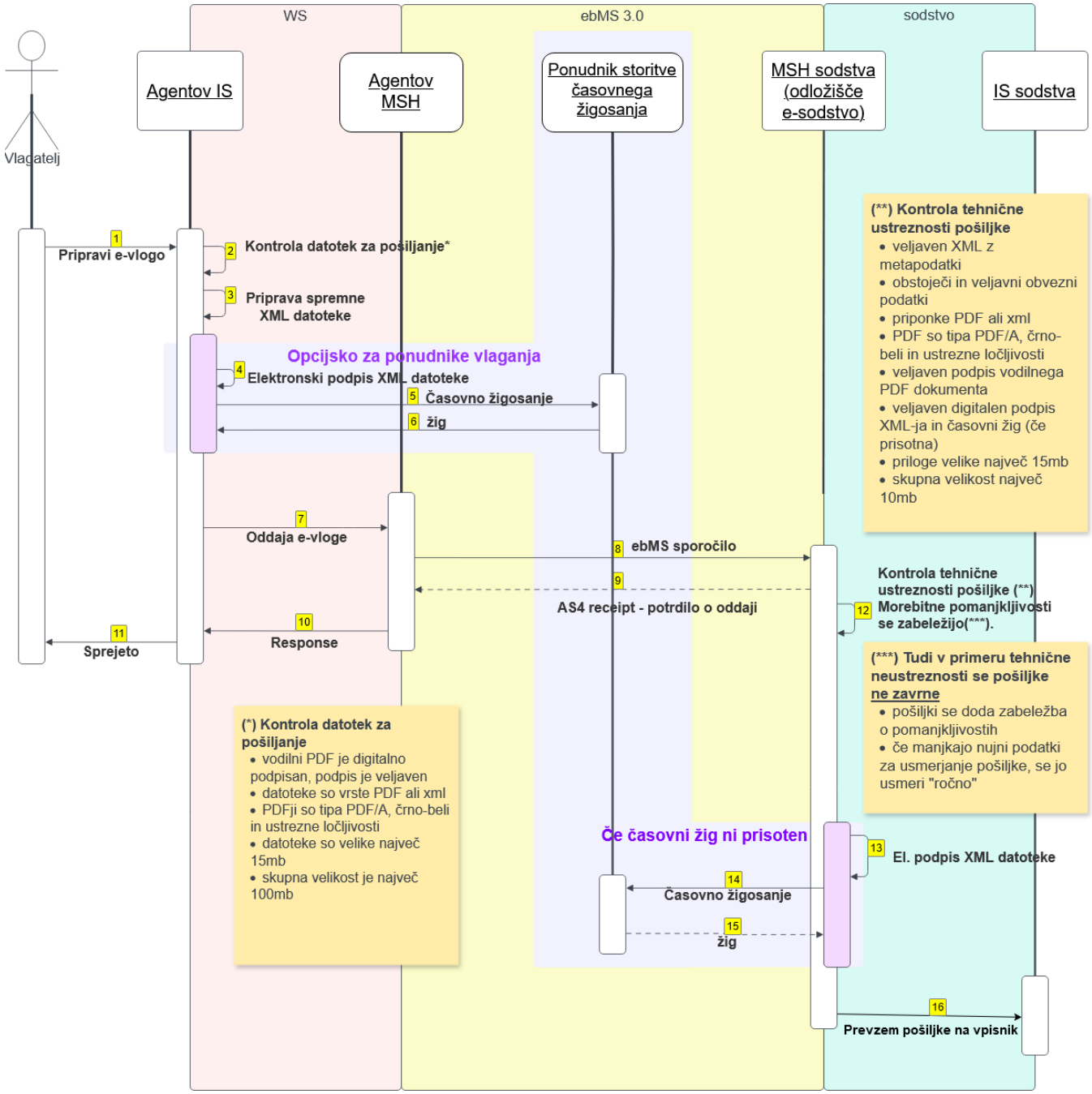
3 Zakon ne dovoljuje časovnega žigosanja rešitvam "po meri", temveč zgolj uradnim ponudnikom elektronskega vlaganja.

4 Časovno žigosana vloga mora biti oddana na sodišče v razumnem roku. V primeru daljšega zadrževanja vloge pri ponudniku storitve elektronskega vlaganja je ponudnik lahko sankcioniran. Kazni bodo določene v pogodbi, ki jo ponudnik sklene s sodiščem.

5 Vloga se morebitno zavrne šele kasneje po vsebinski obravnavi. Namen avtomatskih kontrol (pred in po oddaji) pa je, da se na dolgi rok čimbolj zmanjša število vlog, ki so tehnično neustrezne in potrebujejo ročno obravnavo.

administrator odložišča e-sodstvo vlogo ročno usmeri.

- **Koraki 13-15**: Če vloga ne vsebuje časovnega žiga (ali ni oddana od ponudnika vlaganja) odložišče e-sodstvo elektronsko podpiše xml z metapodatki in podpis časovno žigosa z uporabo storitve izdajatelja kvalificiranih elektronskih časovnih žigov. V tem primeru se vloga šteje za oddano z datumom tega časovnega žiga.
- **Korak 16**: Odložišče e-sodstvo pošlje vlogo v ustrezen eVpisnik (glede na podatke v XML datoteki z metapodatki).

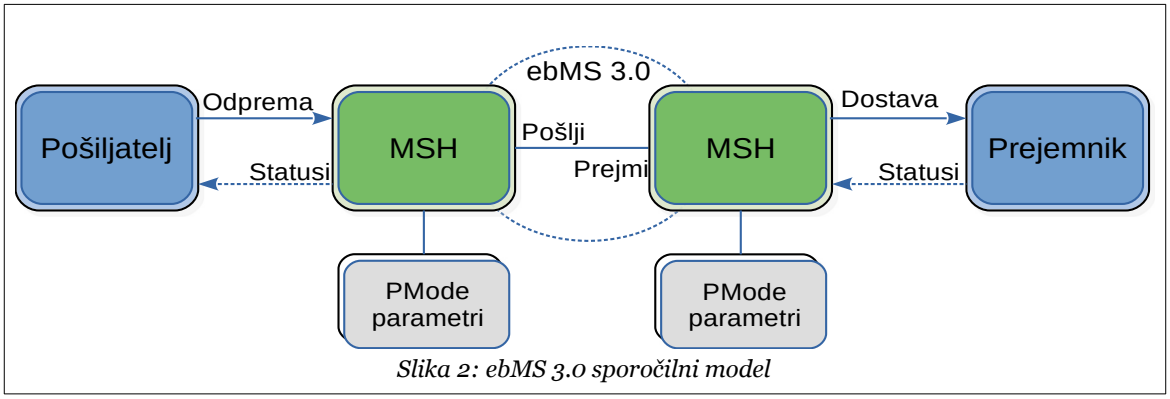


Slika 2: Postopek elektronskega vlaganja na sodišče

4. Tehnična izvedba e-vlaganja

Pri izbiri standarda za zagotavljanje varnosti in zanesljivosti prenosa sporočil je Vrhovno sodišče RS iskalo rešitve, ki bi bile splošno sprejete, cenovno dostopne in preproste za uporabo tudi izven konkretne situacije. Takšne rešitve bi omogočile večjo konkurenco in manjše stroške integracije informacijskih sistemov. Poleg tega je smotrno upoštevati tudi napore Evropske komisije pri vzpostavitvi enotnega digitalnega trga. S tem namenom Evropska komisija promovira profil ebMS 3.0 imenovan **eDelivery AS4**. Tehnična izvedba prenosa elektronskega vročanja temelji na tem profilu in ga dopolnjuje za potrebe elektronskega vlaganja (uporaba TLS, dodatne kode napak, ...)

OASIS ebMS 3.0 (ebXML Messaging Service) standard izhaja iz družine standardov ebXML (Electronic Business using eXtensible Markup Language), ki jih razvija organizacija OASIS (Organization for the Advancement of Structured Information Standards) v sodelovanju z organizacijo UN/CEFACT z namenom zagotovitve moderne, na XML temelječe odprte infrastrukture, ki bi omogočila globalno elektronsko poslovanje na interoperabilen, varen in konsistenten način.



Slika 2: ebMS 3.0 sporočilni model

Kot že rečeno, standard ebMS 3.0 predpisuje komunikacijsko nevtralen mehanizem, ki z uporabo SOAP sporočil in WS-* standardov rešuje tehnična vprašanja glede naslavljanja, varnosti, zanesljivosti prenosa, preverjanja avtentičnosti sporočil itd. Osnovni koncept komunikacije oziroma vročanja temelji na implementaciji transportnega modula, t.i. »Messaging Service Handler« (v nadaljevanju MSH). Par MSH modulov izvaja transport sporočil med prejemnikom in naslovnikom na varen in zanesljiv način kot je določeno v t. im. PMode parametrih (*ang. processing mode parameters).*

Storitev elektronskega vlaganja je implementirana kot koreografija izmenjave sporočil na standardu OASIS ebMS 3.0.

Ker gre za izmenjavo sporočil med dvema MSH, bomo zavoljo enostavnejše terminologije v nadaljevanju vlagateljev MSH (vlagateljev IS za varno elektronsko vlaganje) imenovali "IS odprava", prejemnikov MSH (IS odložišča e-sodstva) pa "IS dostava".

4.1. Reference

Oznaka	Referenca	Opis
OASIS-ebMS3.0	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.html	OASIS ebMS 3.0 standard
OASIS-AS4	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.html	OASIS AS4 profil standarda ebMS 3.0.
eDelivery-AS4	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4	eDelivery AS4 profil uporabe specifikacij OASIS eBMS3 in OASIS AS4.
OASIS-ebCorePartyId	http://docs.oasis-open.org/ebcore/PartyIdType/v1.0/PartyIdType-1.0.html	OASIS ebCore PartyId standard.
eDelivery-ebCorePartyId	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+ebCore+Party+ID	eDelivery ebCore PartyId profil.

4.2. Povzetek ebMS 3.0 parametri

Naslednja tabela povzema nastavitve PMode parametrov za prenos elektronskih sporočil med IS odprava in IS dostava.

Transportni standardi:	
Prenos sporočil poteka preko TLS seje (HTTPS). TLS + HTTP 1.1 + SOAP 1.2 + WSS 1.1.1 + SOAP with Attachments	
PMode[].Protocol.Address	Obvezen, HTTPS URL naslov prejemnika.
PMode[].Protocol.SOAPVersion	1.2
PMode.MEP	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
Zanesljivost:	
V primeru uspešnega prejema sporočila (ebMS 3.0: UserMessage), naslovnikov MSH vrača signalno sporočilo AS4Receipt (glej: OASIS-AS4) ali Exception signal (glej: OASIS-ebMS3.0). V primeru SoapFault ali tcp/http ERROR, pošiljateljev MSH sporočilo poskuša ponovno poslati, tako kot to določajo »Retry«	

nastavitve. V primeru neuspešnega pošiljanja pošiljateljev MSH vrne pošiljatelju opozorilo o neodposlani pošiljki. Naslovnikov MSH mora zaznavati »dvojnike« sporočil in jih eliminirati/ignorirati.	
PMode[].ReceptionAwareness	True
PMode[].Security.SendReceipt	True
PMode[].Security.SendReceipt.NonRepudiation	True
Pmode[1].Security.SendReceipt.ReplyPattern	response
PMode[].ReceptionAwareness.Retry	True (v primeru neuspešnega pošiljanja, pošiljatelj poskuša ponovno poslati izvorno sporočilo)
PMode[].ReceptionAwareness.Retry.Parameters	Spodnja nastavitev ponovnega pošiljanja služi le kot primer – nastavitve so odvisne od funkcionalnosti aplikacije. Pošiljatelj mora pošiljko poslati vsaj 5x v roku enega dneva. maxretries=10, period=2000, e*xponentialBackoff=true;*
PMode[].ReceptionAwareness.DuplicateDetection	True
PMode[].ReceptionAwareness.DetectDuplicates.Parameters	Naslovnikov sistem mora prepoznati že prejeto poročilo vsaj v roku 6 mesecev.
Varnost	
IS odprava in IS dostava zagotavljata varnost prenosa sporočila preko interneta. Vsa sporočila morajo biti podpisana s pošiljateljevem (MSH) digitalnim potrdilom in priponke šifrirane z naslovnikovim (MSH) digitalnim potrdilom. Kljub temu, da je prenos preko HTTPS, se šifriranje vsebin zahteva zaradi skladnosti z eDelivery-AS4 profilom[6].	
PMode[].Security.X509.Sign	True (Podpisovanje sporočila na nivoju transporta med IS odprava in IS dostava)
PMode[].Security.X509.Signature.Certificate	Pošiljka mora biti podpisana s certifikatom IS (pošiljateljev MSH). Podpisane so vse priponke, ter elementa ***env:Body*** in ***ebms:Messaging*** v SOAP ovojnici.
PMode[].Security.X509.Signature.HashFunction	http://www.w3.org/2001/04/xmlenc#sha256
PMode[].Security.X509.Signature.Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
PMode[].Security.X509.Encryption.Encrypt	True (Šifriranje na nivoju transporta med IS Odprava in IS Dostava)

6 Se pa sam standard AS4 razvija, tako da zna priti do sprememb, da šifriranje ne bo več obvezno, ampak zgolj opcijsko.

PMode[].Security.X509.Encryption.Certificate	Vse priponke so šifrirane z uporabo certifikata IS Dostava (naslovnikov MSH).
PMode[].Security.X509.Encryption.Algorithm	http://www.w3.org/2009/xmlenc11#aes128-gcm
PMode[].Security.X509.Encryption.MinimalStrength	128
Vsebine in velikost sporočil	
Sistem mora sprejeti sporočila do skupne velikosti 100MB, posamezne priponke pa so lahko velike 15mb. Propustnost programske opreme mora zagotavljati zaporedni sprejem (z odgovorom) vsaj treh e-pošiljk (v velikosti 100kB) v eni sekundi. Posamezne vsebine se v SOAP sporočilo dodajo kot priponke na način, kot to določa standard »SOAP with attachment« Primer: ------=_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: application/pdf Content-ID: <42eb013c-0606-4d6b-a84f-d71590d2e758@ebox.test.si> Content-Transfer-Encoding: binary id: 42eb013c-0606-4d6b-a84f-d71590d2e758@ebox.test.si %PDF 1.4 # ###...	
PMode[].PayloadService.CompressionType	application/gzip
Metapodatki sporočila	
PMode[].BusinessInfo. Properties	Zaradi uporabe 4-vogalnega naslavljanja pošiljke vsebujejo naslednja parametra:

Parameter	Obvezen	Opis
originalSender	D	Oznaka varnega elektronskega naslova izvornega pošiljatelja pošiljke.

	<table><tr><td>finalRecipient</td><td>D</td><td>Oznaka varnega elektronskega naslova končnega prejemnika pošiljke.</td></tr></table> V prehodnem obdobju imajo zaradi kompatibilnosti z že obstoječimi rešitvami lahko pošiljke, poslane na sodišče, naslednje opcijske parametre (za namen avtomatskega usmerjanja): <table><tr><th>Parameter</th><th>Obvezen</th><th>Opis</th></tr><tr><td>SodiSif</td><td>N</td><td>Šifra sodišča, kateremu se pošilja pošiljko (Glej 5.1 šifrant sodišč).</td></tr><tr><td>OpravilnaSt</td><td>N</td><td>Opravilna številka zadeve, za katero je bila pošiljka narejena. Opravilna številka zajema: kratico vpisnika, zaporedno št. in leto. Kratica vpisnika mora biti nujno iz šifranta kratic vpisnikov (glej 5.3) Vsi trije podatki morajo biti nujno zapisani v naslednjem formatu: med kratico vpisnika in zaporedno št. je enojni presledek, med zaporedno št. in letom pa desna poševnica, Torej: [kraticaVpisnika] [zaporednaŠt]/[leto] Npr: VL 1121/2010 K 21321/2011</td></tr></table>
Metapodatki vsebin / priponk	Poleg metapodatkov, ki jih določa standard AS4, lahko opisi priponk dodatno vsebujejo naslednje metapodatke: <table><tr><td>Podatek</td><td>Opis</td></tr><tr><td>Name</td><td>Opis/naziv priponke</td></tr><tr><td>Filename</td><td>Naziv datoteke.</td></tr></table>
Naslovi varnih elektronskih predalov in vloge (ang, role)	
V elementih **ebms:From/ebms:PartyId** in **ebms:To/ebms:PartyId sta** identifikatorja IS Odprave in IS Dostave, in ne naslova varnih elektronskih predalov originalnega pošiljatelja in končnega prejemnika. (Za podrobnosti glej poglavje: Naslavljanje sporočil (topologija štirih vogalov))	
PMode.Initiator.Role	Rola je določena v opisu posamezne storitve. IS Odprava in IS Dostava pri sestavljanju ebMS 3.0 sporočila prevzemata vloge originalnega pošiljatelja in končnega prejemnika, za katerega izvajata storitev elektronske vročitve e-pošiljke. V primeru odprave e-pošiljke je rola: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator

PMode.Responder.Role	Rola je določena v opisu posamezne storitve. IS Odprava in IS Dostava pri sestavljanju ebMS 3.0 sporočila prevzemata vloge originalnega pošiljatelja in končnega prejemnika, za katerega izvajata prenos sporočila. V primeru pošiljanja e-vročilnice je rola: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder
PMode.Initiator.Party	Oznaka IS Odprave ali IS Dostave, ki prične MEP prenos sporočila (userMessage).
PMode.Responder.Party	Oznaka IS Odprave ali IS Dostave prejemnika sporočila (userMessage).
Oznake storitev in akcij	
Način vročanja ter posamezno fazo vročanja označujeta podatka v **UserMessage/CollaborationInfo/Service** in **UserMessage/CollaborationInfo/Action** Elektronsko vročanje je koreografija izmenjave več sporočil, ki jih povezuje podatek: **UserMessage/CollaborationInfo/ConversationId**. Tako imajo sporočila, ki se izmenjajo pri elektronski vročitvi, vedno vrednost iz sporočila, ki je pričel postopek vročanja Sporočila, ki pripadajo postopku vlaganja imajo v elementu **UserMessage/CollaborationInfo/Service** vrednost: – **CourtFiling** V elementu: **UserMessage/CollaborationInfo/Action** so lahko naslednje vrednosti: **- ServeFiling**: Oddaja vloge na sodišče, Primer: <CollaborationInfo> <Service>CourtFiling</Service> <Action>ServeFiling</Action> <ConversationId>575e09ca-e49f-4ed8-8718-759fe993b4b9@b2g.sodisce.si</ConversationId> </CollaborationInfo>	
PMode[].BusinessInfo.Service	**CourtFiling**: postopek vlaganja v odložišče e-sodstvo
PMode[].BusinessInfo.Action	**ServeFiling**: oddaja vloge na sodišče,

4.3. *Naslavljanje sporočil (topologija štirih vogalov)*

Z namenom zagotavljanja skladnosti s profilom eDelivery-AS4 (objavljen na straneh evropske komisije) je zahtevana implementacija topologije s štirimi vogali (ang. *four corner topology*).

Slika 3: štiri vogalna topologija

Takšna topologija opredeljuje štiri namesto dveh informacijskih sistemov/udeležencev za izmenjavo sporočila. Dva udeleženca sta prvotni stranki v elektronski dostavi sporočila: pošiljatelj in naslovnik. Druge dve stranki sta t.i. dostopni točki, ki prenašata sporočila od prvotnega pošiljatelja do končnega prejemnika na varen in zanesljiv način. Štirje udeleženci so običajno označeni z oznakami Cn, kjer C pomeni "kot" (*ang. corner*) in n ena od števk od 1 do 4:

- C1 je pošiljatelj sporočila. C1 izdela sporočilo tako, da določi vsebine, naslovnika in ostale vsebinske parametre sporočila (primer: vlagatelj).
- C2 je dostopna točka, ki posreduje sporočilo za C1 (primer: IS odprava oz. vlagateljev IS za varno elektronsko vlaganje). C2 sestavi ebMS 3.0 skladno obliko sporočila, določi točko C3, ter na varni in zanesljiv način posreduje sporočilo točki C3.
- C3 je dostopna točka, ki sprejme sporočilo za C4 (primer: IS dostava oz. odložišče e-sodstvo). C3 preveri veljavnost prejetega sporočila za C4 in tako sodeluje pri prenosu sporočila med C2 in C4.
- C4 je končni prejemnik/naslovnik sporočila, ki prevzame sporočilo iz točke C3 (primer: eVpisnik sodstva).

EDelivery-AS4 specifikacija za določanje izvornega pošiljatelja (pošiljateljevega naslova) in končnega prejemnika (prejemnikovega naslova) uporablja ebMS 3.0 parametra **originalSender** in **finalRecipient** (ki se nahajata znotraj elementa eb:MessageProperties):

- Parameter z nazivom **originalSender** določa naslov varnega elektronskega predala izvornega pošiljatelja pošiljke (C1).
- Parameter **finalRecipient** določa naslov varnega elektronskega predala končnega naslovnika pošiljke (C4).

Elementa **From/PartyId** in **To/PartyId** (ki se nahajata znotraj elementa eb:PartyInfo) določata dostopni točki C2 in C3, preko katerih poteka prenos sporočila.

Identifikatorji naslovov udeležencev so skladni ebCoreId in uporabljajo atribut **type**. Za naslavljanje C2 in C3 se za type uporablja oznaka **urn:oasis:names:tc:ebcore:partyid-type:unregistered**. V primeru, da ima udeleženec registrirano tudi ISO 6523 oznako, se lahko uporabi tudi ta.

Primer:

```
<PartyInfo>
   <From>
      <PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered">msh.odprava.si</PartyId>
      <Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator</Role>
   </From>
   <To>
      <PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered">msh.dostava.com</PartyId>
      <Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder</Role>
   </To>
</PartyInfo>

<MessageProperties>
   <Property name="originalSender">janez.posiljatelj@msh.odprava.si</Property>
   <Property name="finalRecipient">martin.prejemnik@msh.dostava.com</Property>
</MessageProperties>
```

4.4. Xml datoteka z metapodatki pošiljke

Pošiljka mora obvezno vsebovati xml priponko z metapodatki. V njej se nahajajo:
- podatki, na podlagi katerih se lahko pošiljka avtomatsko usmerja znotraj sistemov sodstva:
  - šifra sodišča,
  - opravilna številka zadeve *ali* šifra pravnega podpodročja[7],
- seznam pdf datotek in njihovih zgostitvenih vrednosti,
- (neobvezno) časovno žigosan digitalni podpis ponudnika varnega elektronskega vlaganja.

Datoteka mora biti ustrezno poimenovana, njeno ime se mora začeti z "VlogaMetapodatki".
Primer: *VlogaMetapodatki1456784.xml*

Xml datoteka mora imeti naslednjo strukturo elementov in atributov:
(atributi so označeni z @; neobvezni elementi/atributi so znotraj oklepajev)

- elektronskaOvojnica
  - posiljka
    - (@id)
    - zadeva
      - @opravilnaStevilka*
      - sodisce
        - @sifra
      - pravnoPodpodrocje
        - @id*
    - dokumenti
      - dokument
        - @jeVodilni
        - @imeDatoteke
        - @hash
        - (@hashAlgoritem)
        - (@opomba)
  - (Signature)

(* obvezen je en ali drug podatek)

V primeru, če ponudnik varnega elektronskega vročanja xml datoteko tudi digitalno podpiše in ta podpis časovno žigosa, naj:

- se podpisuje vsebina elementa *posiljka*
- bo digitalni podpis v skladu s standardom za XML digitalne podpise: https://www.w3.org/TR/xmldsig-core/
- digitalni podpis se vstavi v element Signature
- se časovni žig zgleduje po standardu XAdes-T: https://www.w3.org/TR/XAdES/#Syntax_for_XAdES_T_form

7 Pravna podpodročja so npr. gospodarsko, pravdno, nepravdno podpodročje.

Vkolikor ponudnik varnega elektronskega vročanja xml datoteke elektronsko ne podpiše in časovno žigosa, digitalni podpis (s certifikatom strežnika IS odložiče e-sodstvo) in časovni žig priskrbi IS odložišče e-sodstvo.

4.4.1. Primer xml datoteke z metapodatki

Ime datoteke: VlogaMetapodatki1234.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:elektronskaOvojnica
      xmlns:ns1="http://sodisce.si/sheme/skupno/v1"
      xmlns:ns2="http://sodisce.si/sheme/skupno/izmenjave/v1"
      xmlns:ns3="http://sodisce.si/sheme/skupno/skupno/v1">
   <ns2:posiljka>
      <ns2:zadeva opravilnaStevilka="K 1/2023">
         <ns3:sodisce sifra="S23"/>
         <ns3:pravnoPodpodrocje id="178"/>
      </ns2:zadeva>
      <ns2:dokumenti>
         <ns2:dokument jeVodilni="true" imeDatoteke="pritožba.pdf" hash="fe73281db675ec53e..." />
         <ns2:dokument jeVodilni="false" imeDatoteke="priloga.pdf" hash="773afe0a4393925435..."/>
      </ns2:dokumenti>
   </ns2:posiljka>
</ns1:elektronskaOvojnica>
```

4.4.2. Podrobnejši opis strukture xml datoteke z metapodatki.

Uporabljeni namespace-i in sheme[8]:
xmlns:ns1="http://sodisce.si/sheme/skupno/v1"
xmlns:ns2="http://sodisce.si/sheme/skupno/izmenjave/v1"
xmlns:ns3="http://sodisce.si/sheme/skupno/skupno/v1"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

ELEMENT ali ATRIBUT	OBV.	OPIS	PRIMER VREDNOSTI	TIP PODATKA
elektronskaOvojnica	D	Korenski element	/	ns2:ElektronskaOvojnicaTip
elektronskaOvojnica/**posiljka**	D	Element, ki vsebuje podelemente s podatki o posiljki	/	ns2:ElektronskaPosiljkaTip
elektronskaOvojnica/posiljka/**@id**	N	Neobvezen id elementa - uporabno za digitalni podpis	24073	xs:ID
elektronskaOvojnica/posiljka/**zadeva**	D	Element, ki vsebuje podelemente s podatki o zadevi	/	ns3:ZadevaTip
elektronskaOvojnica/posiljka/zadeva/ **@opravilnaStevilka**	D*[9]	Opravilna številka zadeve, za katero je bila pošiljka narejena. Opravilna številka zajema: kratico vpisnika, zaporedno št. in leto. Kratica vpisnika mora biti nujno iz šifranta vpisnikov (glej 5.3) Vsi trije podatki morajo biti nujno zapisani v naslednjem formatu: med kratico vpisnika in zaporedno št. je enojni presledek, med zaporedno št. in letom pa desna poševnica,	VL 1121/2020 K 21321/2023 *Format:* [kraticaVpisnika] [zaporednaŠt]/[leto]	xs:string
elektronskaOvojnica/posiljka/zadeva/ **sodisce**	D	Element, ki vsebuje podatke o sodišču, kateremu se pošilja vlogo	/	ns3:SifrantTip
elektronskaOvojnica/posiljka/zadeva/ sodisce/**@sif**	D	Šifra sodišča, kateremu se pošilja vlogo (glej 5.1 šifrant sodišč).	S21 S59	xs:string
elektronskaOvojnica/posiljka/zadeva/ **pravnoPodpodrocje**	N	Element, ki vsebuje podatke o pravnem podpodročju zadeve	/	ns3:SifrantTip
elektronskaOvojnica/posiljka/zadeva/ pravnoPodpodrocje/**@id**	D*[10]	Če se vloga nanaša na novo, še neobstoječo zadevo, je namesto opravilne številke zadeve treba tu vnesti šifro pravnega podpodročje zadeve (iz šifranta pravnih področij, glej 5.4).	27	xs:string
elektronskaOvojnica/posiljka/zadeva/ **dokumenti**	D	Seznam vloženih dokumentov	/	ns2:ElektronskiDokumentSeznamTip
elektronskaOvojnica/posiljka/zadeva/ dokumenti/**dokument**	D	Posamezen dokument s seznama vloženih dokumentov	/	ns2:ElektronskiDokumentTip
elektronskaOvojnica/posiljka/zadeva/ dokumenti/dokument/**@jeVodilni**	D	Indikator, ali je dokument vodilni (za vodilni dokument uporabi 'true', za priloge 'false')	true false	xs:boolean
elektronskaOvojnica/posiljka/zadeva/ dokumenti/dokument/**@imeDatoteke**	N	Ime datoteke (s končnico vred)	Vloga za začetek postopka.pdf	xs:string
elektronskaOvojnica/posiljka/zadeva/ dokumenti/dokument/**@hash**	D	Hash (zgostitvena vrednost) dokumenta, zapisan v heksadecimalni obliki.	0fbb34624c786eeb3f5174 3465beaa61f5a974f395f0 2885d23edde2b8058123	xs:string
elektronskaOvojnica/posiljka/zadeva/ dokumenti/dokument/	N	Izbrani algoritem za izračun hash-a dokumenta[11]	http://www.w3.org/ 2009/xmldsig11#dsa-	xs:anyURI

8 Specifikacijam so priložene xsd sheme, ki opisujejo skupno strukturo vhodnih in izhodnih xml datotek sodišča (trenutno verzije 1.1.1). Čeprav so te sheme precej širše, en del njih opisuje tudi zgoraj predpisani xml metapodatkov datoteke za vlaganje. Izhodiščna xsd datoteka je SkupnoElementi.xsd ("http://sodisce.si/sheme/skupno/v1"), le-ta potem uvozi druge xsd datoteke.

9 Obvezen je eden od elementov: ali opravilnaStevilka ali PravnoPodrocje. Prvega uporabimo v primeru že obstoječe zadeve, drugega v primeru nove zadeve.

10 Glej prejšnjo opombo.

@hashAlgoritem		(če element odsoten, se izračuna po SHA-256 algoritmu)	sha256	
elektronskaOvojnica/posiljka/zadeva/dokumenti/dokument/**@opomba**	N	Morebitna opomba.	Opomba je neobvezna.	xs:string
elektronskaOvojnica/**Signature**	N	Digitalni podpis Strukturo elementa predpisuje shema za xml podpise: https://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd	/	ds:SignatureType

5. Tabele in šifranti

5.1. Šifrant sodišč

Najnovejši šifrant je objavljen na spletnih straneh sodišča:
https://www.sodisce.si/sodna_uprava/e_poslovanje/

5.2. Šifrant e-predalov sodstva

e-predal	Opis
odlozisce.e-sodstvo@b2g.sodisce.si	Enoten varni elektronski predal za vlaganje v odložišče e-sodstvo

Nadaljne usmerjanje v VEP-e posameznih vpisnikov poteka na podlagi vsebine xml datoteke z metapodatki pošiljke.

5.3. Šifrant vpisnikov

Najnovejši šifrant je objavljen na spletnih straneh sodišča:
https://www.sodisce.si/sodna_uprava/e_poslovanje/

5.4. Šifrant pravnih podpodročij, za katere je omogočeno elektronsko vlaganje

Najnovejši šifrant bo objavljen na spletnih straneh sodišča:
https://www.sodisce.si/sodna_uprava/e_poslovanje/

11 Privzeto se za izračun hash-a dokumenta uporablja SHA-256 algoritem (v tem primeru je ta atribut neobvezen), vendar bo v prihodnosti zaradi varnosti to predvidoma potrebno zamenjati z drugimi, tako da se bo s tem elementom lahko določilo izbrano metodo za izračun hash-a dokumenta.

5.5. Šifrant napak

Za prenos sporočil se uporablja shema in zapis napak, kot jih predvideva standard ebMS 3.0 (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.html; glej razdelek: 6 Packaging of ebMS Errors) in profil AS4 (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html; glej razdelek: 3.6 Additional Features Errors).

Šifra napake	**Kratek opis**	**Tip napake (Severity)**	**Katergorija napake**	**Opis**
SVEV:0202	ReceiverNotExists	*failure*	*content*	Naslovnik ne obstaja
SVEV: 0203	MessageInvalid	*failure*	*content*	Pošiljka ni tehnično ustrezna