



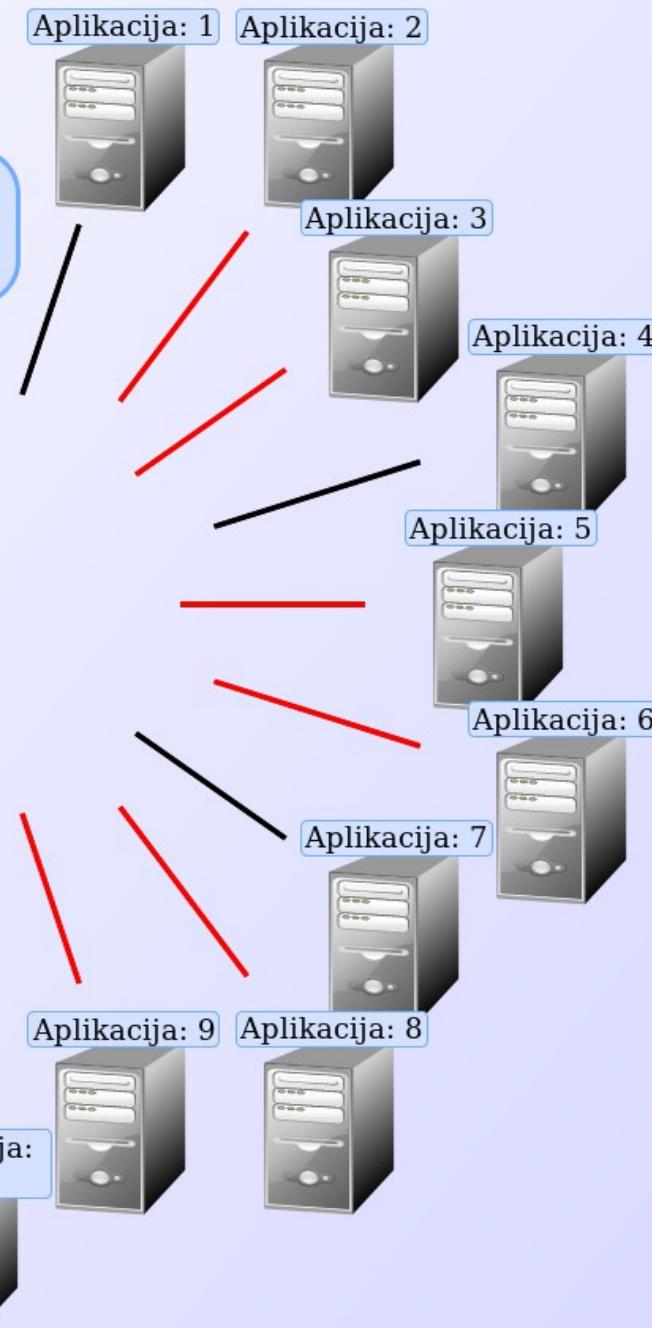
# L Laurentius

Uporaba standarda OASIS - ebMS 3.0  
(ESENS-AS4) za elektronsko poslovanje  
s sodiščem

Konferenca JavaSi'17

Jože Rihtaršič, 16. 10. 2017

Poslovni proces 1  
Aplikacija 1



1. Spreminjanje poslovnih procesov (nove storitve)
2. Nadgrajevanje aplikacij (kvalitetnejše vsebine)
3. Spreminjanje vsebine sporočil
4. Nove tehnologije
5. Menjavanje partnerjev
6. Novi trendi partnerjev



# Cilji elektronskega poslovanje na sodišču

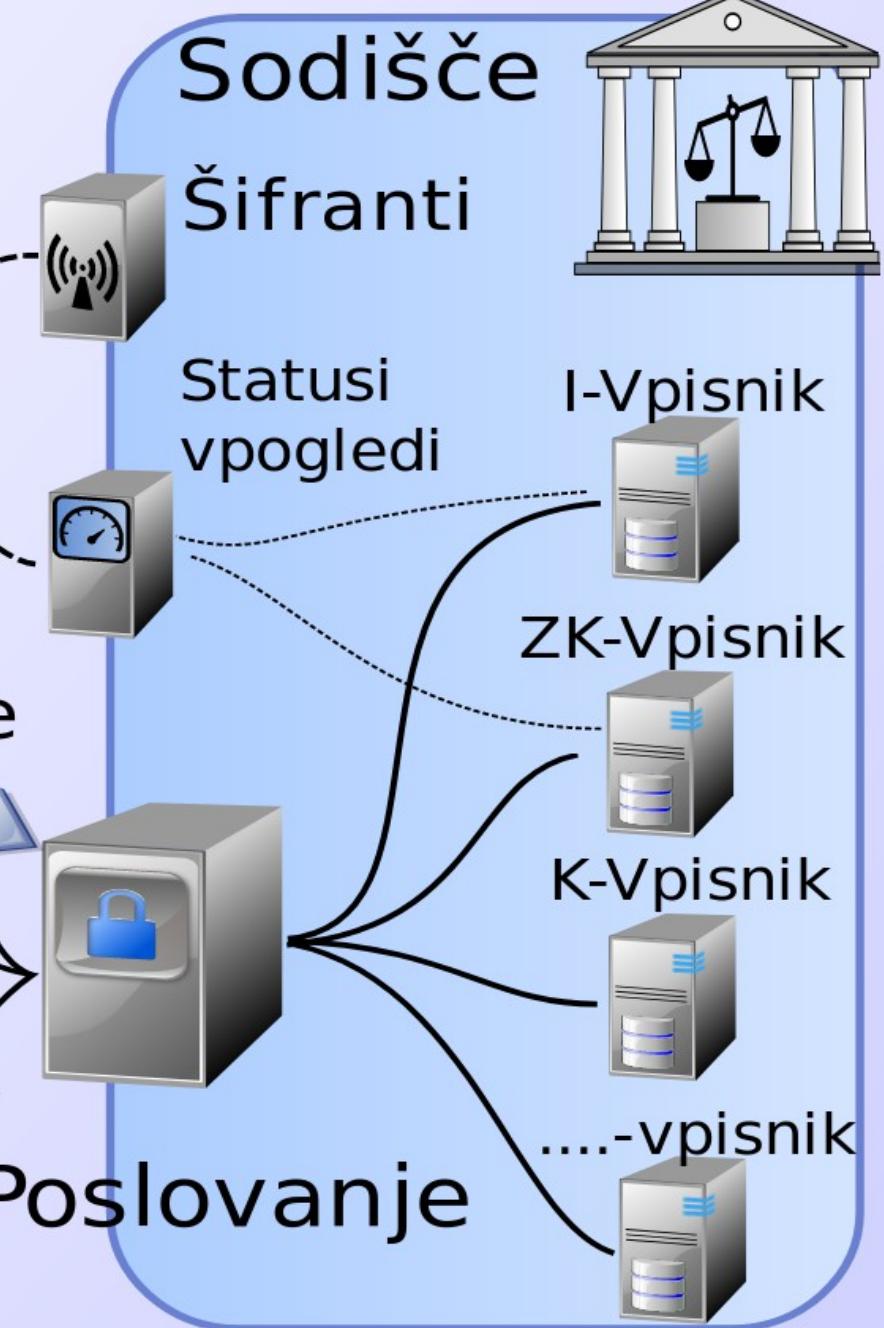
## Stranke ePoslovanje



## Papirno poslovanje



## ePoslovanje

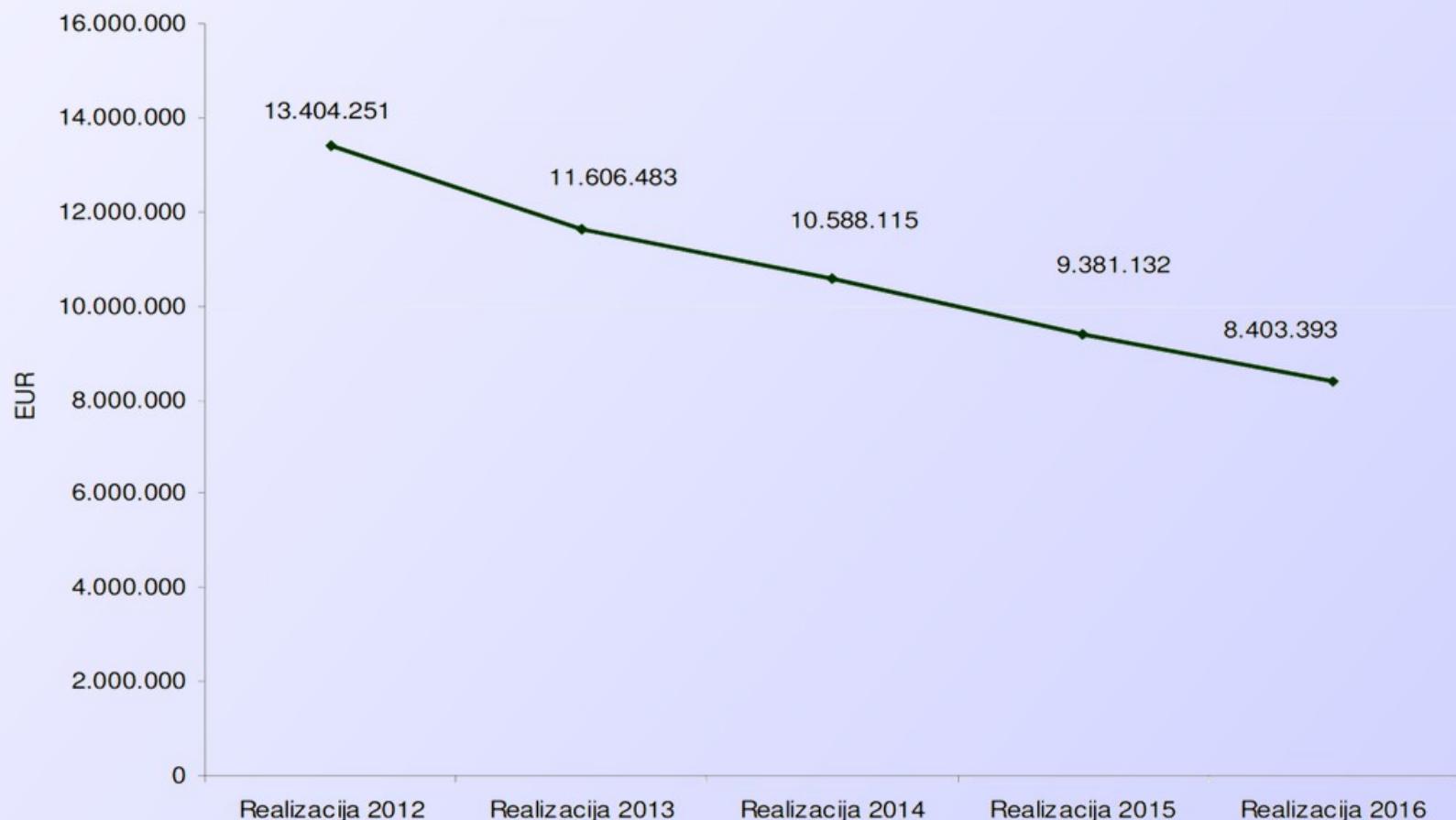


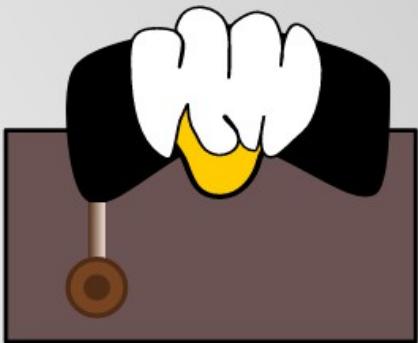


# Izhodna in dohodna pošta

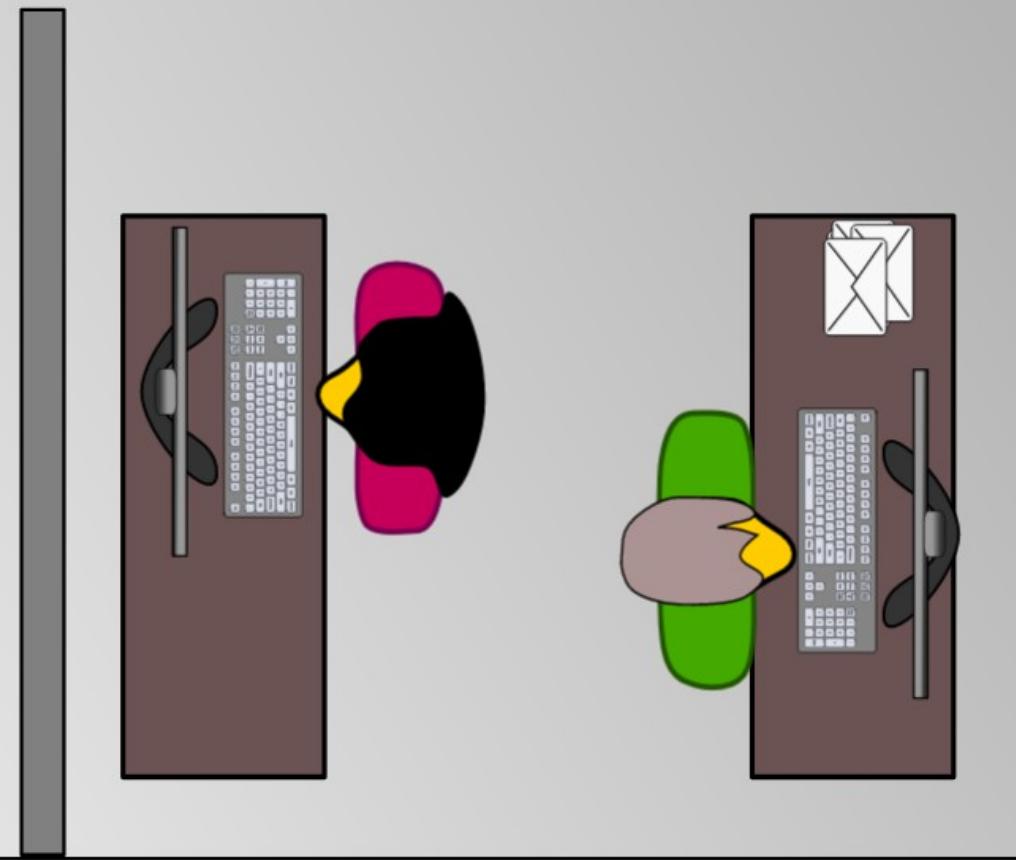
Slovenska sodišča imajo na leto v delu cca 1 milijon zadev:

- več kot 2 milijoni vlog (dohodna pošta);
- več kot 6 milijonov izhodnih pošiljk;
- do leta 2013 strošek poštnih storitev cca 12 milijonov EUR.





- **eVpisnik + podpora orodja** - elektronsko vodenje zadev;
- **eSpis** - listine v elektronski obliki.





eOveritve

SU vpisnik

eINS vpisnik

K vpisnik

T vpisnik

eZK vpisnik

PUND vpisnik

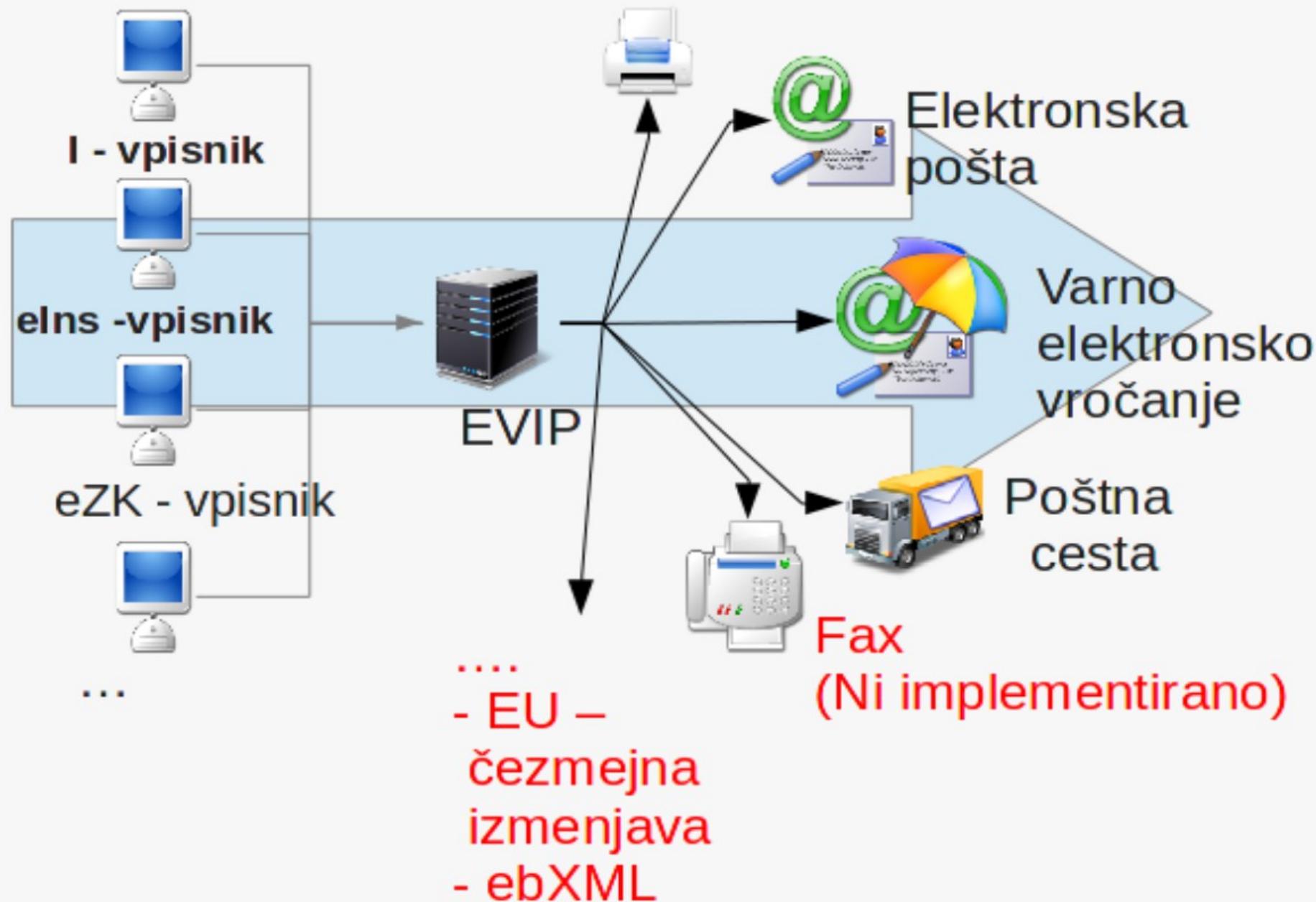
PRS vpisnik

SRG vpisnik





## Lokalna odprema





# Postopki vročanja/ način odpreme

Postopek vročitve / način odpreme	Lokalna odprema	Strojno kuvertiranje	e-vročanje
Navadno (C5 – bela kuverta)	✓	✓	✓ (email)
Priporočeno (C5 – bela kuverta)	✓	o	
Priporočeno - tujina (C5 – bela kuverta)	✓	o	
Priporočeno s povratnico (Slovenija CN 07)	✓		
Priporočeno s povratnico (tujina CN 07)	✓		
Paket	✓	✓	
Paket s povratnico	✓	✓	
OBR. SR. 38	✓		
OBR. SR. 39	✓		
ZPP navadno	✓	✓	V pripravi
ZPP osebno	✓	✓	✓ (SVEV)
ZKP navadno	✓		
ZKP osebno	✓		
ZSReg	✓		
ZFPPIPP	✓		
ZUP	✓	o	

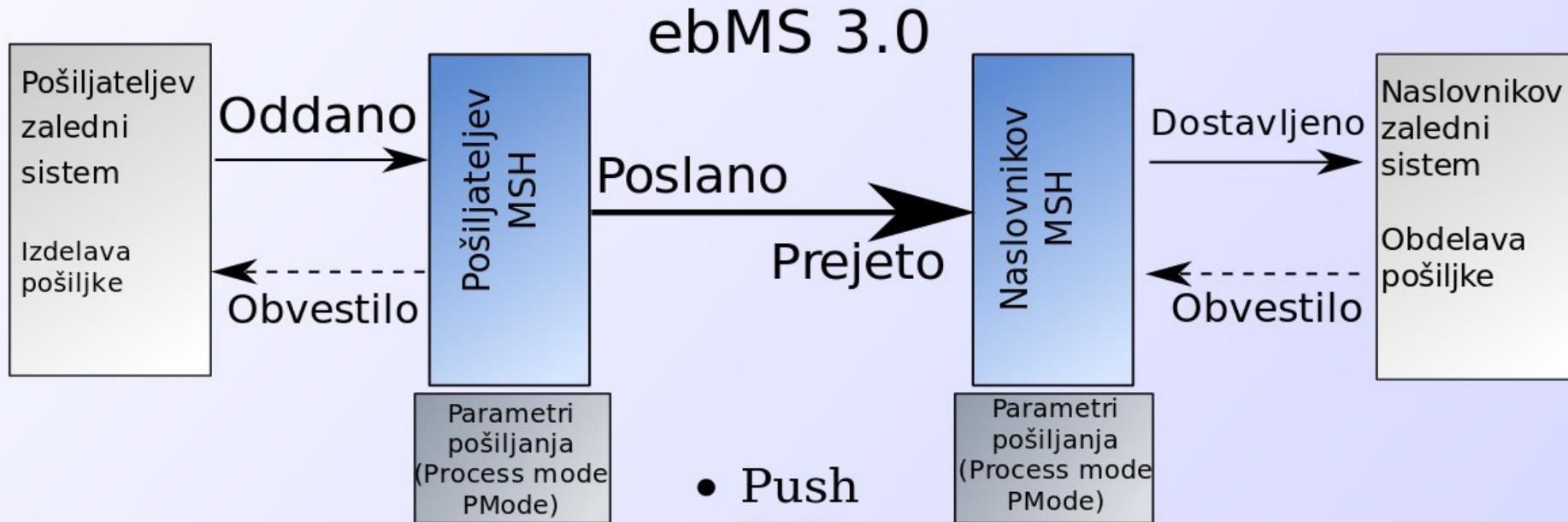


## Integracije:

- izdelava integracije: 5.000 - 50.000 eur
- različne tehnologije: ftp, pgp, https, wsdl, rest, smtp, jms
- različni standardi (standardi po meri)
- vzdrževanje
- nadgrajevanje (vsebina)

## Skupne prvine transporta sporočil:

- zagotavljanje pristnosti sporočil
- identifikacija pošiljatelja
- varnost prenosa sporočil
- zanesljivost prenosa sporočil
- dokazljivost prenosa
- vročanje različnih oblik datotek
- parametrizirano nastavljanje različnih koreografij izmenjave sporočil
- enostavno dodajanje in spremiščanje novih uporabnikov in izvajalcev storitev
- uporaba odprtih standardov in tehnologij
- avtomatizacija sprejema/pošiljanja



- Naslovnik
- Pošiljatelj
- Storitev
- Akcija
- Vsebine (XML, PDF, DOC, ...)

- Push
- Pull
- Sync
- Preveri
- (Šifriraj)
- Podpiši
- Pošlji
- Preveri
- (Dešifriraj)
- Sprejmi
- Prevzemi
- Procesiraj



**Poslovni kontekst:** določa namen, storitev, akcijo in obliko vsebine.

Urejanje storitev

Id	
PrintAndEnvelope-C5	
Naziv:	PrintAndEnvelope-C5
Initiator role:	ServiceRequestor
Executor role:	ServiceProvider
SED parametri:	<input type="button" value="x"/>

Diagram illustrating the business context (PMode) for the service PrintAndEnvelope-C5. It shows the interaction between the Initiator and Executor.

The Initiator sends two messages to the Executor:

- AddMail
- RemoveMail

The Executor returns one message to the Initiator:

- ServiceStatusNotification

Akcia

Akcija	Proženje	Tip sporočila
AddMail	initiator	userMessage
envelope_data (application/xml) concatenated_content (application/pdf)		
RemoveMail	initiator	signalMessage
ServiceStatusNotification	executor	userMessage

Potrdi  Prekliči



**Poslovni kontekst:** storitev skupaj z enolično oznako določa poslovno transakcijo. Lahko vsebuje več Akcij (izmenjave sporočil).

**Urejanje storitev**

**Id**  
PrintAndEnvelope-C5

Naziv: PrintAndEnvelope-C5 Tip storitve: http://laurentius.si/meps

Initiator role: ServiceRequestor Executor role: ServiceProvider

SED parametri:

**Akcija**

	Akcija	Proženje	Tip sporočila
1	AddMail	initiator	userMessage
	envelope_data (application/xml) concatenated_content (application/pdf)		
2	RemoveMail	initiator	signalMessage
3	ServiceStatusNotification	executor	userMessage

**Diagram**

```
sequenceDiagram
    participant Initiator
    participant Executor
    Initiator->>Executor: AddMail
    Executor-->>Initiator: RemoveMail
    Initiator-->>Executor: ServiceStatusNotification
```

**Buttons at the bottom:**

Potrdi  Prekliči



# PMode parametri

**Profil varnosti:** parametri določajo nivo varnosti, metodo podpisa in šifriranja in elemente/priponke za podpis/šifriranje.

**PMode nastavitev varnosti**

**PMode varnost:**

ID:	enc_att_and_sign_v1
Verzija:	1.1

**Podpisovanje in šifriranje sporočila**

<input checked="" type="checkbox"/> Podpis sporočila	<input checked="" type="checkbox"/> Šifriranje sporočila
Algoritem: RSA-SHA256	Algoritem: AES128-GCM
Zgostitvena funkcija: SHA256	
Identifikacija ključa: IssuerSerial	Identifikacija ključa: IssuerSerial
Podpiši priponke: <input type="checkbox"/>	Šifriraj priponke: <input type="checkbox"/>

**SOAP sporočilo**

<input type="button" value="Dodaj"/> <input type="button" value="Uredi"/> <input type="button" value="Izbriši"/>
XPath
env:Header/eb3: Messaging
env:Body

**SOAP sporočilo**

<input type="button" value="Dodaj"/> <input type="button" value="Uredi"/> <input type="button" value="Izbriši"/>
XPath
No records found.



# PMode parametri

**Profil zanesljivosti:** parametri določajo uporabo mehanizmov za zagotavljanje zanesljivosti prenosa.

**PMode zanesljivost**

<b>PMode zanesljivost:</b>
ID: AS4ReceiptResponse
Način odgovora: response
Tip povratnice: AS4Receipt
<b>Ponovno pošiljanje:</b>
Št. poskusov: 3
Množenje periode: 3
Perioda: 5678
<b>Zaznava dvojnikov:</b>
Obdobje zaznave: P1Y
Odstrani dvojnik: <input checked="" type="checkbox"/>
<b>Potrdi</b> <b>Prekliči</b>

# PMode parametri

**eIdentitete:** parametri določajo partnerjeve značilnosti:  
digitalna potrdila, URL naslovi, domena, ...

Urejanje e-identitet partnerjev

<b>Identiteta</b>	<b>Transport</b>				
<b>Identiteta</b>					
ID:	mb-laurentius	Domena:	mb-laurentius.si	<input checked="" type="checkbox"/> Aktiven:	<input type="checkbox"/> Lokalna identiteta:
<b>Certifikati za lokalno identiteto</b>					
Podpisni ključ:	<input type="button" value=""/>	Dešifrirni ključ:	<input type="button" value=""/>		
<b>Certifikati zaupanja</b>					
Cert. podpisa:	<input type="button" value="test-laurentius"/>	Cert. šifriranja:	<input type="button" value=""/>		
<b>Identiteta</b>					
 Dodaj	 Izbriši				
Oznaka	Vir				
urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-shev:name	name				
urn:oasis:names:tc:ebcore:partyid-type:unregistered:si-shev:sed-box	address				
<input checked="" type="checkbox"/> Potrdi <input type="checkbox"/> Preklici					



# PMode parametri

**PMode:** združeni profili v konkretno storitev.

**PModes**

ID	ZPP-legal
Id:	LegalDelivery_ZPP (SVEV:LegalDelivery_ZPP)
Lokalna identiteta:	court-laurentius
Local party def. transport:	default
<input checked="" type="checkbox"/> Initiator role: Sender	
<input checked="" type="checkbox"/> Executor role: Receiver	

**Partnerji**

	Partner	Def. transport
1	mb-laurentius	default
2	mju	default
3	court-laurentius	default
4	bankakoper	default
5	kro	default
6	podpora	default
7	nlb	default
8	dbs	default
9	abanka	default
10	test-sodisce	default
11	MinistrstvoPravosodje	default

**MEP**

Initiator role	MEP	MEP channel binding	MEP akcije
Sender	OneWay	Push	DeliveryNotification,
Receiver	TwoWay	Sync	AdviceOfDelivery,EncryptedKey,
Sender	TwoWay	Sync	FictionNotification,

**Potrdi** **Prekliči**



# PMode parametri

**PMode:** določanje prenos posameznega sporočila/akcije.

PMode MEP dialog

Initiator role: Sender

MEP: OneWay      MEP channel binding: Push

**First leg**

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

**Fore channel**

Akcija: DeliveryNotification      Varnost id: sign\_sha256      ReceptionAwareness: AS4ReceiptResponse

**Back channel**

Akcija:      Varnost id: sign\_sha256

The diagram illustrates the configuration of a PMode MEP dialog. At the top, the initiator role is set to 'Sender' and the MEP is 'OneWay'. The binding is 'Push'. Below this, the 'First leg' is defined with an MPC pointing to a specific URL. The 'Fore channel' section shows the configuration for the forward message exchange, while the 'Back channel' section shows the configuration for the return message exchange, indicated by a dashed line.



# Oblika sporočila ebMS 3.0

## SOAP s priponkami

### SOAP Sporočilo

Element: SOAPHeader

ebMS Parametri  
Naslavljanje, storitev,...

Parametri za zanesljiv  
prenos

Parametri za varen  
prenos

Element: SOAPBody

XML Vsebina

### Priponka

MIME Headers

Binarna vsebina

### Priponka

MIME Headers

Binarna vsebina

ID sporočila, časovni žig,  
pošiljatelj, naslovnik,  
transakcijski podatki  
(storitev, akcija...),  
podatki o vsebini

ePodpis, podatki o šifriranju,...  
WS Security

Podatki, potrebni za zanesljiv transport  
WS Reliability in WS ReliableMessaging

XML Vsebina sporočila

Vsebina sporočil kot MIME del sporočila  
za prenos vseh oblik sporočil



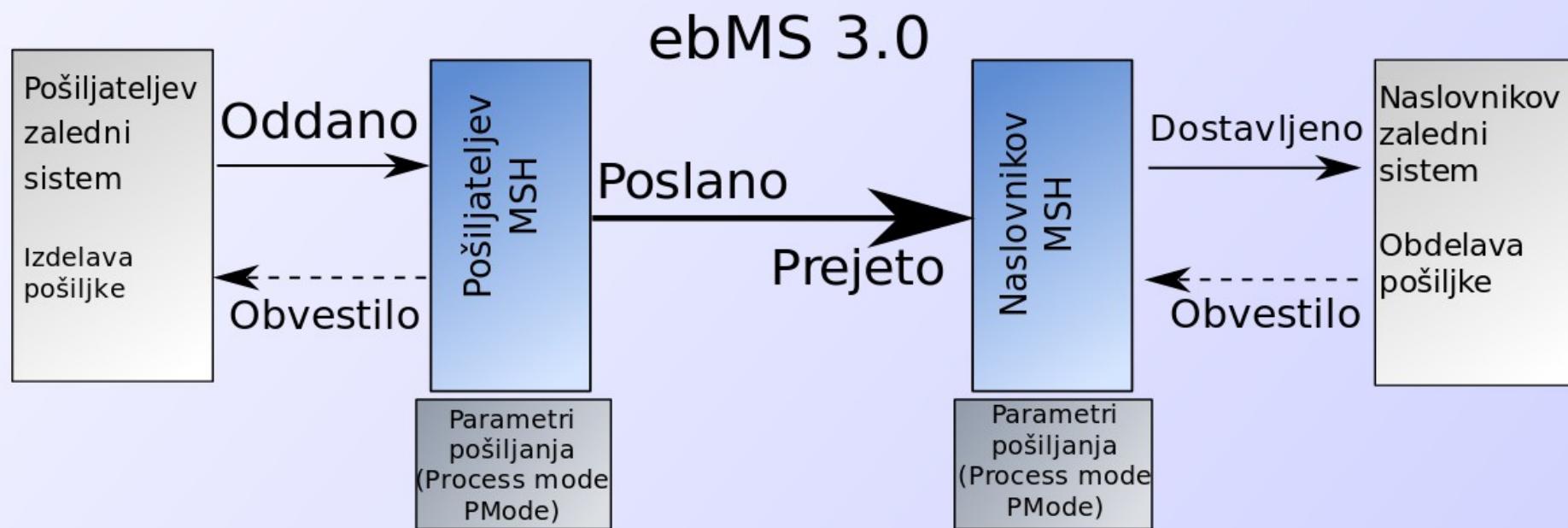
- Implementacija gradnika MSH z namenom spodbujanja (in zmanjševanja začetnih stroškov strankam) pri uporabi protokola ebMS 3.0;
- Skladna rešitev z evropskimi smernicami (eCODEX, eSENS, Skupni digitalni trg);
- Nastal v sodelovanju z Združenjem bank Slovenije;
- Prenos dobrih praks iz gostodarstva na sodišče. Izvajalec programiranja je sodišče, naročnik nekaterih funkcionanih zahtev (integracije, nadzor, zanesljivost) članice ZBS;
- Odprta koda z licenco EUPL (varnost zagotavljajo tehnični mehanizmi in ne skrivanje kode);
- Splošno uporabni programi, ki se razvijejo na sodišču so na voljo tudi državljanom;
- Ime je v spomin Lovrencu Koširju (1804-1879), ki je eden izmed inovatorjev poštne znamke.





# Avtomatizacija sprejema/pošiljanja sporočil

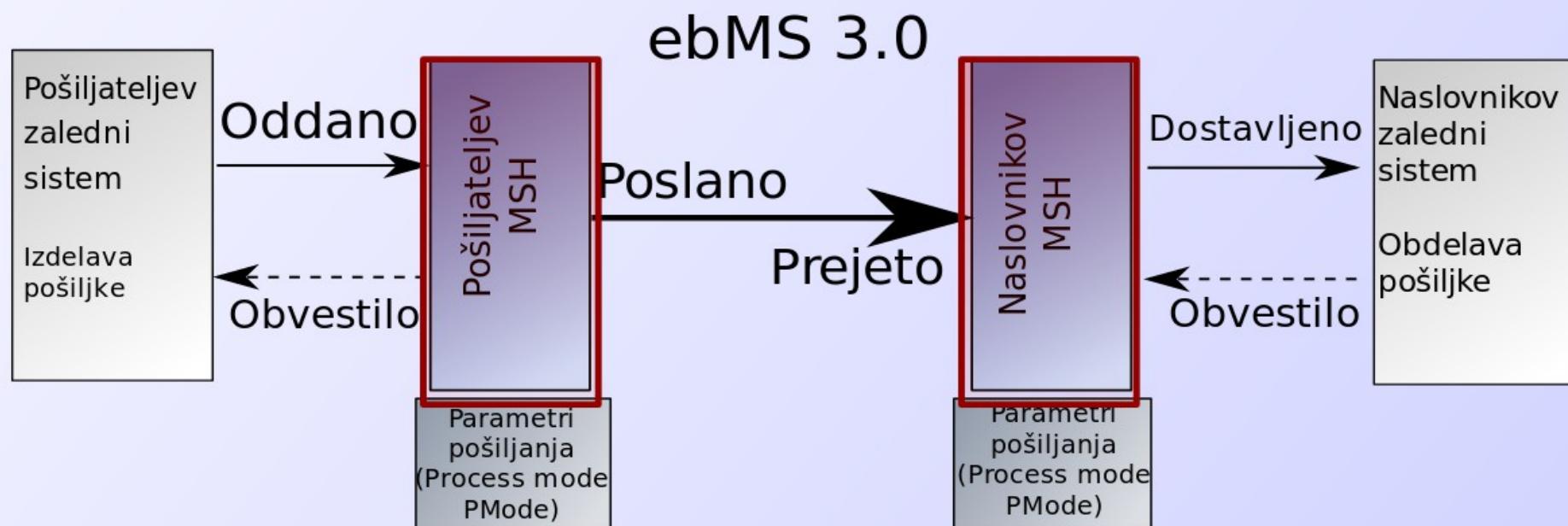
**Dodatki:** namen dodatkov je avtomatizacija obdelave sprejetih in poslanih pošiljk.



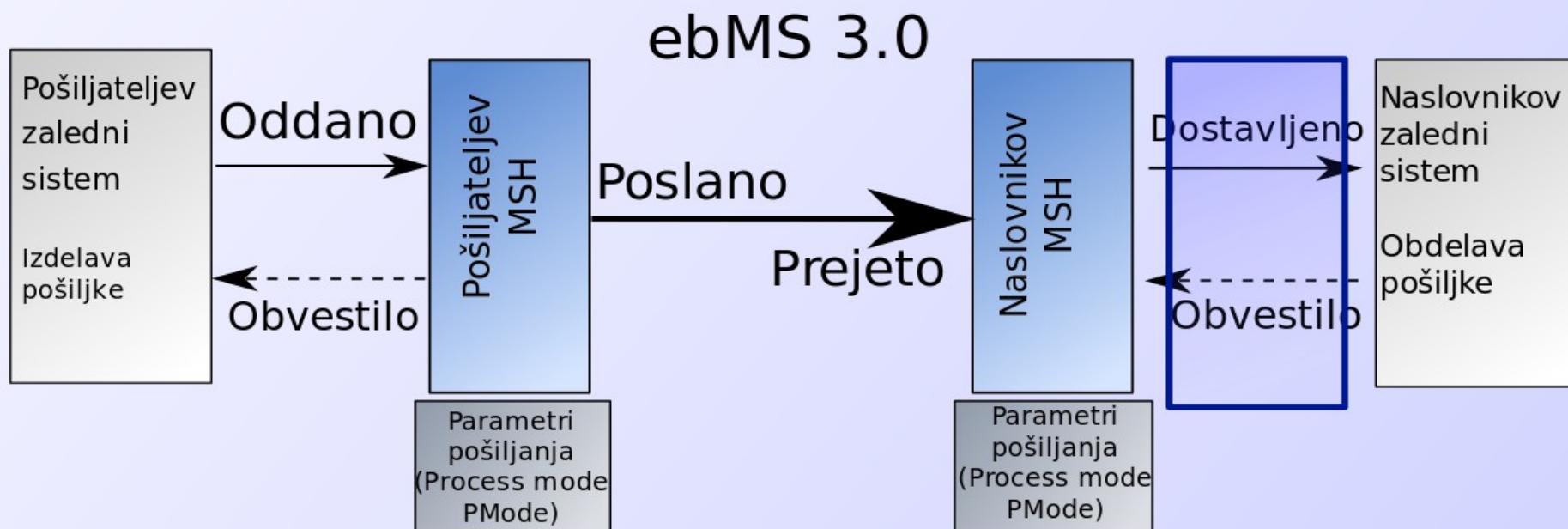


# Avtomatizacija sprejema/pošiljanja sporočil

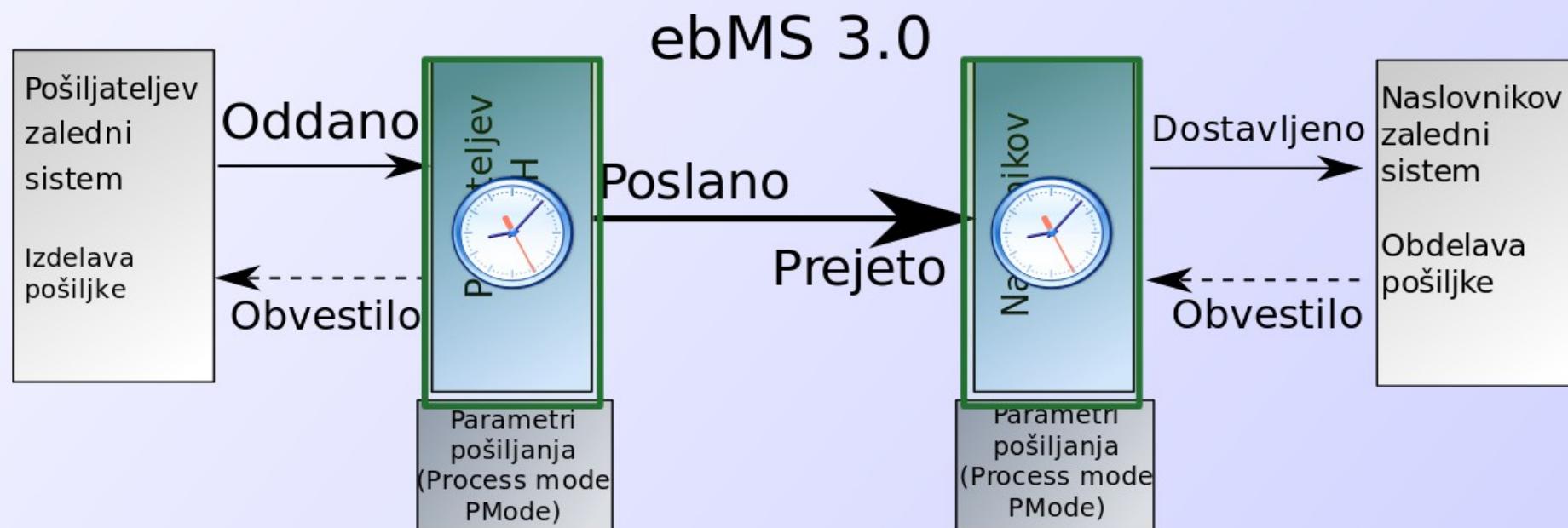
**Prestrezniki:** namen prestreznikov je preoblikovanje sporočil pri pošiljanju in implementacija dodatnih kontrol pred dokončnim prejemom sporočil.

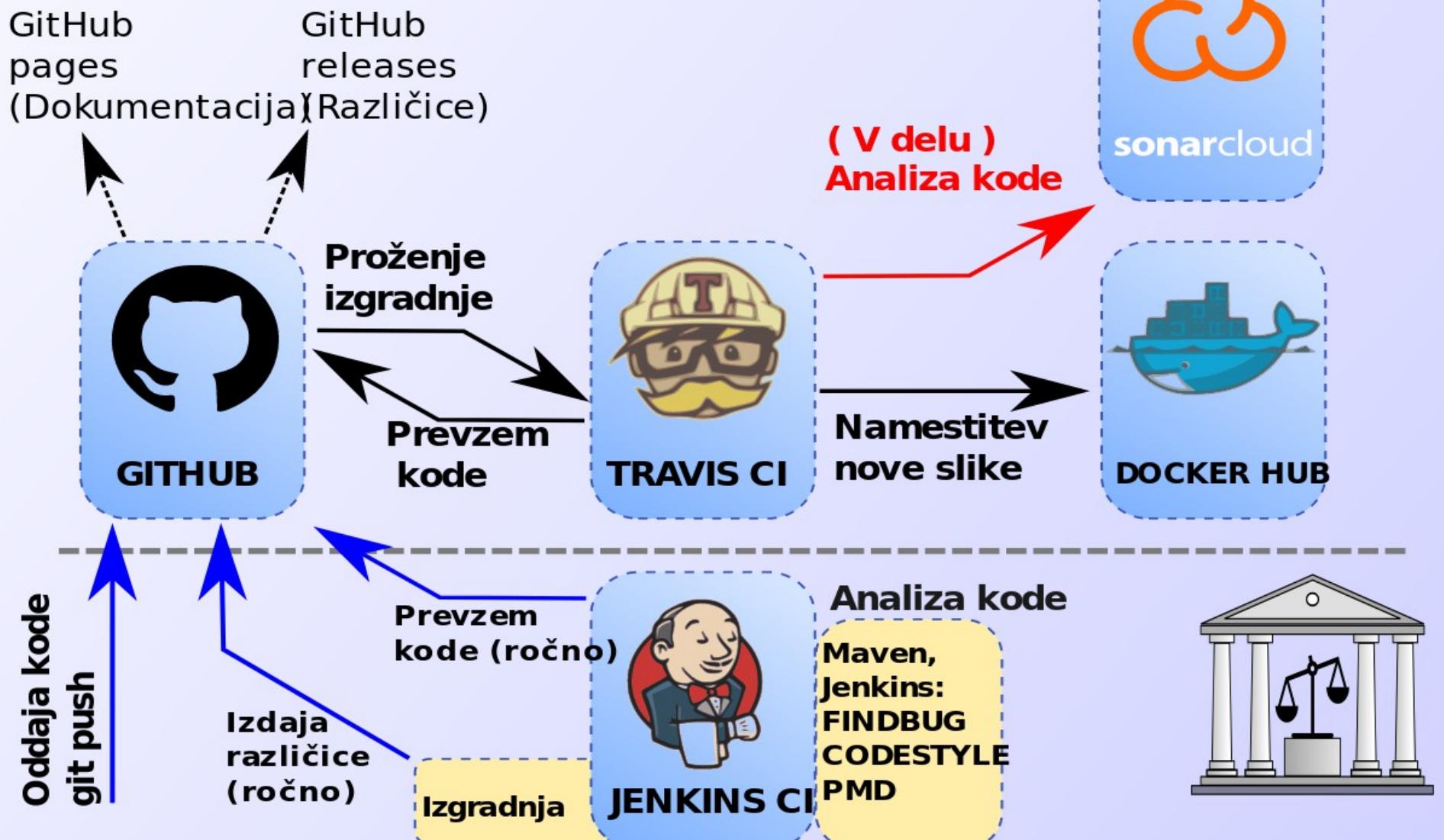


**Procesi dohodne pošte:** namen 'processorjev' je avtomatizacija izvoza in procesiranja dohodne pošte (xslt, izvoz, zagon zunanjih procesov, ...).



**Koledar opravil:** nastavljanje koledarjev za izvajanje časovnih opravila (Poročila, pošiljanje preko datotečnega sistema, ...).

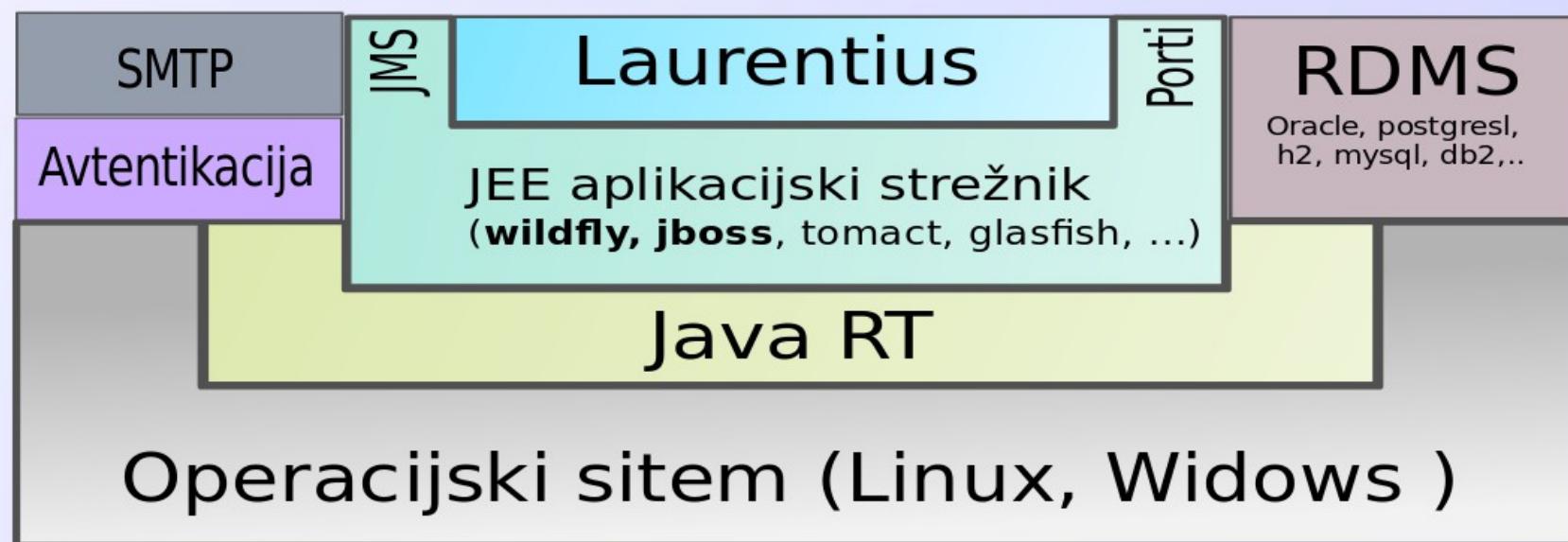




Prilagajanju okolju, ki ga ima uporabnik pod nadzorom:

- **Operacijski sistem:** Linux OS, Windows OS
- **Podatkovna baza:** oracle, postgreSQL, mysql, db2, derby,...
- **Aplikacijski strežnik:** *wildfly, jboss, weblogic, tomcat, ...*
- **Nastavljeni porti:** (Aplikacijski strežnik)
- **OS servis:** Zagon kot linux/windos servis
- ...

Postavitev več konfiguracij (testno, šolsko, proizvodnjsko okolje)





# Hvala za pozornost

- **Laurentius (koda):** <https://vsrscif.github.io/Laurentius/>
- **Laurentius (dokumentacija):** <https://vsrscif.github.io/Laurentius/>
- **Dockerhub (docker run --net=host -p 8080:8080 -p 9990:9990 -it jrihtarsic/laurentius):** <https://hub.docker.com/r/jrihtarsic/laurentius/>
- **ebMS 3.0:** [http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms\\_core-3.0-spec-cs-02.html](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html)
- **eSENS-AS4 rešitve:** <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+AS4+conformant+solutions>