**NOV UVOZNI NADZORNI SISTEM**

**(ICS2)**

**5. izdaja, SEPT 2023**

**Zgodovina dokumenta**

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzija** | **Datum** | **Avtor** | **Kratek opis sprememb** |
| **1.izdaja** | OKTOBER 2019 | DS za ICS2 |  |
| **2. izdaja** | FEBRUAR 2021 | DS za ICS2 | Posodobitev tehnične specifikacije za komunikacijo z STI ter dodana tehnična specifikacija za komunikacijo med gospodarskim subjektom in NES |
| **3.izdaja** | JUNIJ 2021 | DS za ICS2 | Posodobitev shem Ctypes.xsd, IE3QS2.xsd ter IE3SN5.xsd v komunikaciji med gospodarskim subjektom in NES |
| **4. izdaja** | MAJ 2023 | DS za ICS2 | Dodana vsebina za potrebe R2 NES. |
| **5. izdaja** | SEPTEMBER 2023 | DS za ICS2 | Posodobitve shem za IE3RS8 za potrebe R2 NES |

**KAZALO**

[1 Uvod 4](#_Toc138063494)

[2 Namen in cilji ICS2 4](#_Toc138063495)

[2.1 Časovni okvir uvedbe ICS2 5](#_Toc138063496)

[3 Pregled osnovnih komponent ICS2 5](#_Toc138063497)

[3.1 Sistemi gospodarskega subjekta 6](#_Toc138063498)

[3.2 UUM&DS 6](#_Toc138063499)

[3.3 STI - skupni vmesnik za gospodarske subjekte 6](#_Toc138063500)

[3.4 CR - Skupno skladišče 6](#_Toc138063501)

[3.5 CCN2 6](#_Toc138063502)

[3.6 NES – Nacionalni sistem nadzora uvoza 7](#_Toc138063503)

[4 Funkcijska in tehnična dokumentacija 7](#_Toc138063504)

[5 Poslovni proces 9](#_Toc138063505)

[5.1 Proces predložitve blaga NES – poštne pošiljke v okviru letalskega prometa 9](#_Toc138063506)

[5.1.1 Poslovni proces NES 9](#_Toc138063507)

[5.1.2 Sporočila za komunikacijo med sistemom deklaranta in sistemom NES 9](#_Toc138063508)

[5.2 Proces predložitve drugega blaga prispelega v okviru vseh ostalih vrst transporta (R2 in R3) 10](#_Toc138063509)

[5.2.1 Poslovni proces NES 10](#_Toc138063510)

[5.2.2 Sporočila za komunikacijo med sistemom deklaranta in NES 10](#_Toc138063511)

[6 Katalog elektronskih sporočil 10](#_Toc138063512)

[6.1 STANDARDI IN PRAVILA ZA SESTAVO ELEKTRONSKIH SPOROČIL 11](#_Toc138063513)

[6.1.1 STANDARDI 11](#_Toc138063514)

[6.1.2 PRAVILA ZA SESTAVO SPOROČIL V FORMATU XML 11](#_Toc138063515)

[6.2 Strukture XML sporočil 15](#_Toc138063516)

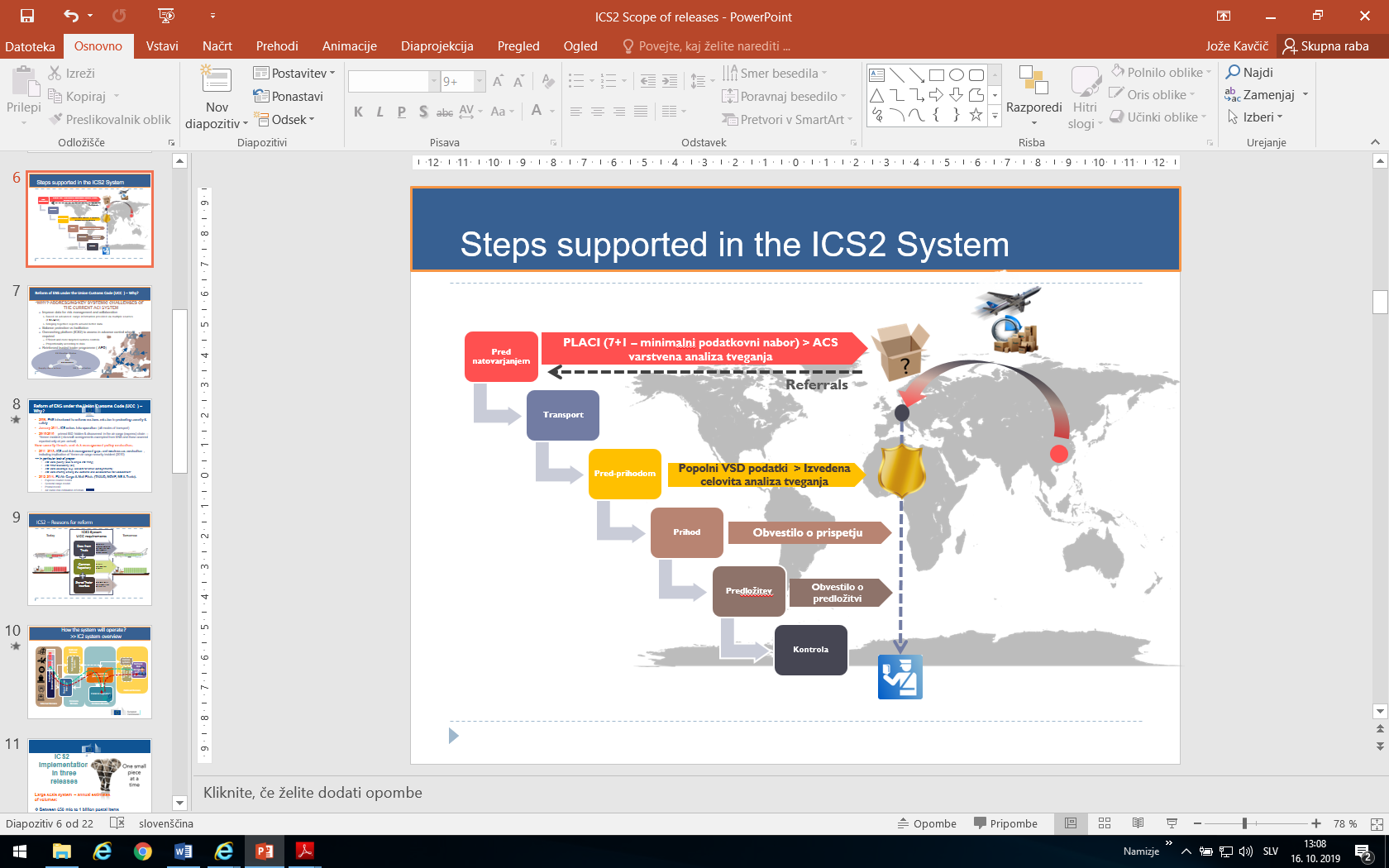
[6.3 Struktura sporočil in XSD sheme 17](#_Toc138063517)

[6.4 Pogoji in pravila podatkovnih skupin oz. elementov 17](#_Toc138063518)

[6.5 Šifranti 18](#_Toc138063519)

# Uvod

Za gospodarsko rast in konkurenčnost Evropske unije (v nadaljevanju EU) ter učinkovit boj proti goljufijam so potrebni enostavni, hitri in poenoteni carinski postopki in procesi. V smislu izboljšanja konkurenčnosti EU in vzpostavitvi enotnih metod obvladovanja tveganj Unije, je svet EU junija 2013 za navedeno področje sprejel novo strategijo in njen akcijski načrt v skladu s katerim je bil sprejet tudi nov Carinski zakonik Unije (v nadaljevanju CZU), ki je vstopil v veljavo 1. junija 2016. Z novim CZU so bile tako uvedene spremembe, ki so jih dolžni po preteku prehodnega obdobja upoštevati in implementirati v svoje postopke in informacijske sisteme gospodarski subjekti in carinski organi držav članic pri izvajanju postopkov v zvezi z vnosom blaga iz tretjih držav v EU. Da bi carinski organi zagotovili pravilno delovanje enotnega trga EU in carinske unije v skladu s sprejeto strategijo in njenim akcijskim načrtom je bil v letu 2015 vzpostavljen program ICS2 (nov sistem nadzora uvoza), ki bo po preteku prehodnega obdobja popolnoma nadomestil obstoječi sistem nadzora uvoza, tj. ICS.



# Namen in cilji ICS2

* uvedba novega sistema nadzora uvoza, ki bo zagotovil pravočasne in kakovostnejše podatke,
* poenotenje podatkovnih zahtev za potrebe izboljšanja kvalitete podatkov
* omogočanje izvajanja skupne analize tveganja na nivoju EU pred samim prihodom oz. naložitvijo blaga na prevozno sredstvo, za potrebe določanja kraja in vrste izvedbe potrebnih ustreznih carinskih ukrepov,
* odprava oprostitve deklariranja pošiljk manjše vrednosti do 22 EUR,
* izmenjava informacij in podatkov med državami članicami v realnem času (v režimu 24/7/365),
* zagotavljanje ustrezne analitične podpore,
* ustrezen zajem rezultatov izvedenih ukrepov na celotnem območju EU v skladu s CZU,
* omogočanja uvedbe sistema večkratnega deklariranja blaga s strani različnih akterjev v dobavni verigi za posamezno vstopno deklaracijo (Multiple Filling).

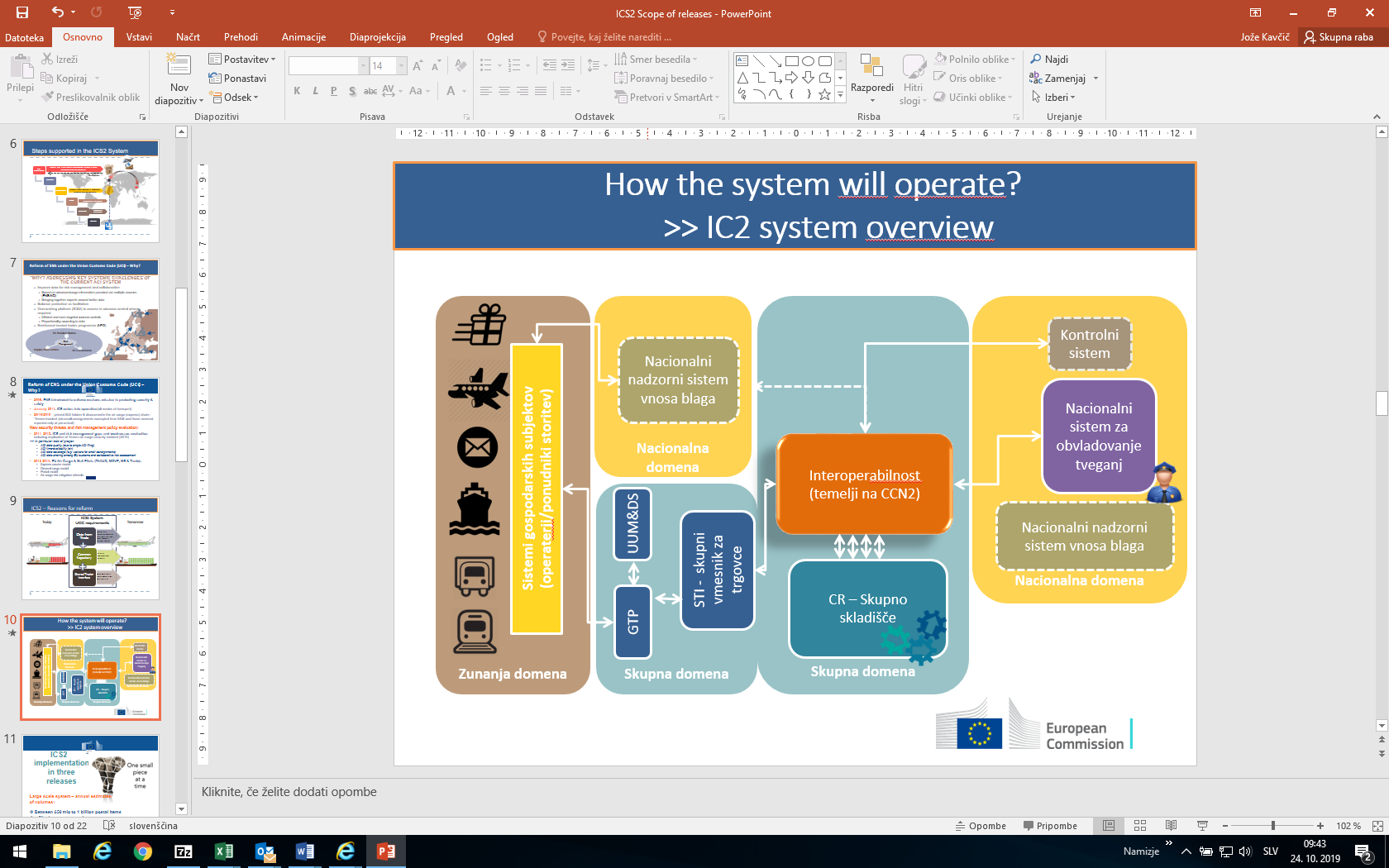
## Časovni okvir uvedbe ICS2

Proces uvedbe novega sistema nadzora uvoza (v nadaljevanju ICS2) poteka za gospodarske subjekte in carinske administracije v 3 fazah. Vsaka faza zajema vzpostavitev različnih procesov. Predvidene so naslednje faze:

1. faza (**R1**) zajema izdelavo novega sistema ICS2 za zajem **minimalnega nabora podatkov pred natovarjanjem** (PLACI) za pošiljke prispele **po pošti** in **hitri pošti po zračnem prometu** vključno s podatki za E-trgovanje, s predvidenim rokom uvedbe **15.03.2021 oz. 1.7. 2021 z vključenimi podatki za E-trgovanje**;
2. faza (**R2**) zajema nadgradnjo izdelanega sistema ICS2 za možnost **prejema in obdelave vstopne skupne deklaracije** (v nadaljevanju VSD) **za celotno blago prispelo v zračnem prometu** in izdelavo novega sistema za podporo izvajanja obvladovanja tveganj, s predvidenim rokom uvedbe **01.03.2023**;
3. faza (**R3**) zajema nadgradnjo sistema ICS2 z možnostjo **zajema in obdelave podatkov VSD za vse preostale vrste transporta cesta, železnica in morje**, s predvidenim rokom uvedbe **01.03.2024**.

# Pregled osnovnih komponent ICS2

Spodnja slika prikazuje glavne komponente sistema ICS2.



## Sistemi gospodarskega subjekta

Sistemi gospodarskega subjekta so odgovorni za pošiljanje in prejemanje elektronskih sporočil med vmesnikom gospodarskega subjekta in vmesnikom EU (STI). Komunikacija med gospodarskim subjektom in STI mora potekati z uporabo odprtega standarda AS4, kot protokola o izmenjavi poslovnih elektronskih sporočil v skladu s specifikacijami e-Delivery AS4 (znano tudi kot e-SENS AS4). Gospodarski subjekt si bo moral predhodno pridobiti digitalni certifikat s strani pristojnega uradnega izdajatelja (certificate authority), se registrirati pri pristojnih carinskih organih kot sistemski operater za ICS2, urediti dostopno točko in obvestiti službo za pomoč (Help desk) o nameri za vzpostavitev dostopne točke z navedbo fizičnega naslova URL, ID stranke (EORI) in javnega ključa digitalnega certifikata.

## UUM&DS

ICS2 bo za čezmejno avtorizacijo in avtentikacijo gospodarskih subjektov ali njihovih predstavnikov uporabljal modul UUM&DS. UUM&DS bodo uporabljali tudi ponudniki IT storitev (v primeru če se bo gospodarski subjekt odločil, da pošiljanje in prejemanje sporočil odda v zunanje izvajanje ponudniku IT storitev), kot pošiljatelji in prejemniki sporočil, za način direktne komunikacije med njihovimi sistemi in sistemom STI.

## STI - skupni vmesnik za gospodarske subjekte

STI predstavlja enoten vmesnik za gospodarske subjekte preko katerega so omogočene storitve povezane s vložitvijo:

1. **VSD**, ne glede na to, ali gre za vložitev ali razveljavitev ter
2. **obvestila o prihodu blaga**.

Vsako sporočilo vloženo ali prejeto preko STI bo preverjeno tako sintaktično (oblika sporočila) kot shematično (vsebina sporočila mora upoštevati pravila in pogoje, določene v skupnih specifikacijah ICS2), pri čemer se preverjanje opira na podatke, pridobljene z uporabo storitev referenčnih sistemov TARIC3, CRS, CS/RD2 in ECICS2. Uspešno preverjena sporočila oziroma vloge se nato posreduje centralni komponenti CR sistema ICS2 za nadaljnjo preverjanje in usklajevanje.

## CR - Skupno skladišče

CR je skupna podatkovna komponenta sistema ICS2, ki bo zagotavljala skupne referenčne podatke, upravljanje logičnih procesov in shranjevanje podatkov VSD, s katero bodo zadevni podatki na voljo carinskim organom držav članic za njihovo enotno izvajanje analize tveganja, izmenjave informacij, enotnemu zajemu rezultatov kontrol in rezultatov analiz tveganj ter zagotavljanju ustrezne analitične podpore.

## CCN2

CCN2 je vseevropsko komunikacijsko omrežje preko katerega bodo komunicirali sistemi STI in CR ter sistema CR in NES. Uporabljala se bo tudi za t.i. zvezno avtorizacijo in avtentikacijo, ki bo državam članicam, gospodarskim subjektom iz držav članic in uporabnikom službe za pomoč uporabnikov, omogočala dostop do spletnih vmesnikov STI in CR.

## NES – Nacionalni sistem nadzora uvoza

Glavne funkcionalnosti NES so naslednje:

* Prejem in obdelava VSD oz. carinskih deklaracij pri carinskem uradu prvega vstopa, pri carinskem uradu naslednjega vstopa ali pri namembnem carinskem uradu,
* izvajanje analize tveganja,
* izvajanje procesov vezanih na prihod prevoznega sredstva, predložitev blaga in kontrolo blaga.

NES se uporablja za komunikacijo :

* s STI za izvajanje postopkov **pred predložitvijo blaga** za namene izvedbe analize tveganja ter za komunikacijo
* s sistemov gospodarskih subjektov **za** namene **izvajanja postopkov predložitve blaga**.

# Funkcijska in tehnična dokumentacija

Funkcijska in tehnična dokumentacija je sestavljena iz:

* opisa poslovnih procesov, ki jih morajo zagotavljati gospodarski subjekti pri komunikaciji z STI in NES v okviru :
  1. poštnih in hitrih pošiljk v okviru letalskem prometu ter
  2. drugega blaga prispelega v okviru vseh vrst transporta (cesta, železnica, morje, letalo),
* tehnične specifikacije za komunikacijo s STI in NES,
* elektronskih sporočil (seznam, XSD sheme) potrebnih za izmenjavo s STI in NES,
* seznama pravil in pogojev, ki jih je potrebno upoštevati pri uporabi elektronskih sporočil,
* seznam šifrantov, ki jih je potrebno upoštevati pri izdelavi in uporabi elektronskih sporočil znotraj sistemov STI in NES

Dokumentacija za gospodarstvo je razdeljena na dva dela, in sicer glede na procese, ki jih mora gospodarski subjekt elektronsko podpreti:

1. **del** **dokumentacije podpira procese pred predložitvijo blaga** in je namenjen vzpostavitvi komunikacije med gospodarskim subjektom in STI (sistemom EU). Ta del dokumentacije je vzdrževan s strani Evropske komisije. Dokumentacija se nahaja na naslednji povezavi [Circabc (europa.eu)](https://circabc.europa.eu/ui/group/528298e7-ca03-47a5-8a59-4cd4f7f5f12d/library/450e1496-0944-465f-ac2f-8894dee2bece) ter
2. **del dokumentacije podpira procese predložitve blaga,**  ki je namenjen vzpostavitvi komunikacije med gospodarskimi subjekti (v nadaljevanju sistem deklaranta) in sistemom carinskih organov (v nadaljevanju sistem NES). Dokumentacija je sestavljena iz:
   * ***poslovnega procesa***, ki s pomočjo notacije BPMN opredeljuje aktivnosti in izmenjavo sporočil med sistemom deklaranta in sistemom NES.

Pomen uporabljenih elementov notacije BPMN znotraj posameznega poslovnega procesa in izmenjave sporočil znotraj posameznega poslovnega procesa je naveden v spodnji tabeli.

|  |  |
| --- | --- |
| Element BPMN | Pomen |
|  | Prejem oz. pošiljanje sporočila |
|  | Začetno sporočilo (začetek procesa) |
|  | Naloga/aktivnost, ki se izvede znotraj procesa |
|  | Prejem sporočilo znotraj procesa na podlagi katerega se izvede naloga/aktivnost |
|  | Posredovanje sporočila znotraj procesa, ki je rezultat izvedene naloge/aktivnosti |
|  | Konec procesa |
|  | Start časovnika za nadaljevanje procesa |
|  | Tok oz. smer izvajanja procesa |
|  | Tok (smer) sporočila |
|  | Prehod, ki usmerja tok zaporedja na točno eno od odhodnih vej |
| CL  CLSI1 | Code list – šifrant |
|  | Stanje predloženega blaga |

*Tabela 1: Pomen uporabljenih elementov BPMN izmenjave sporočil*

* + ***kataloga elektronskih sporočil***, ki predstavlja tehnični opis oz. strukturo elektronskih sporočil ter druga pravila in standarde, ki jih je potrebno upoštevati pri pripravi oz. posredovanju elektronskih sporočil s strani sistema deklaranta v sistem NES.

# Poslovni proces

## Proces predložitve blaga NES – poštne pošiljke v okviru letalskega prometa

V nadaljevanju je opredeljena dokumentacija za potrebe vzpostavitve komunikacije med sistemom deklaranta in sistemom NES za potrebe vzpostavitev procesov predložitve blaga v okviru poštnih pošiljk.

### Poslovni proces NES

Dokument, ki s pomočjo BPMN notacije prikazuje poslovni proces se nahaja spodaj:



### Sporočila za komunikacijo med sistemom deklaranta in sistemom NES

Seznam elektronskih sporočil, ki se izmenjujejo med sistemom deklaranta in sistemom NES je naveden v spodnji tabeli.

| **Oznaka sporočilo** | **Smer komunikacije\*** | **Polno ime** |
| --- | --- | --- |
| IE3S10 | 🡪 NES | Predložitev blaga |
| IE3RS8 | NES 🡪 | Blago predloženo |
| IE3S08 | NES 🡪 | Informacija o izvedbi kontrole |
| IE3QS2 | NES 🡪 | Zahtevek za dodatne informacije |
| IE3RS2 | 🡪 NES | Posredovanje dodatnih informacij |
| IE3SN3 | NES 🡪 | Rezultati kontrole |
| IE3SN4 | 🡪 NES | Strinjanje/nestrinjanje z rezultati kontrole |
| IE3S99 | 🡪 NES | Informacija o zavrnitvi/napaki |
| IE3SN5 | NES 🡪 | Obvestilo o prepustitvi |
| IE3SN6 | 🡪 NES | Obvestilo o vročitvi/nevročitvi blaga |
| IE3SA4 | NES 🡪 | Dopolnitve s strani gospodarskega subjekta VSD (STANJE: V kontroli) |
| IE3SN7 | 🡪 NES | Obvestilo o naknadni vrnitvi blaga (reklamacija) |
| IE3SN9 | NES 🡪 | Obvestilo o zavrnitvi blaga |

\* 🡪 NES: Sporočilo s strani deklaranta posredovano v NES

NES 🡪: Sporočilo s strani NES posredovano deklarantu

Tabela 2: Seznam elektronski sporočil

## Proces predložitve drugega blaga prispelega v okviru vseh ostalih vrst transporta (R2 in R3)

V nadaljevanju je opredeljena dokumentacija za potrebe vzpostavitve komunikacije med sistemom deklaranta in sistemom NES za potrebe vzpostavitev procesov predložitve blaga v okviru drugega blaga prispelega v okviru vseh vrst transporta.

### Poslovni proces NES

Dokument, ki s pomočjo BPMN notacije prikazuje poslovni proces se nahaja spodaj:



### Sporočila za komunikacijo med sistemom deklaranta in NES

Seznam elektronskih sporočil, ki se izmenjujejo med sistemom deklaranta in sistemom NES je naveden v spodnji tabeli.

| **Oznaka sporočilo** | **Smer komunikacije\*** | **Polno ime** |
| --- | --- | --- |
| IE3S10 | 🡪 NES | Predložitev blaga |
| IE3RS8 | NES 🡪 | Blago predloženo |
| IE3S08 | NES 🡪 | Informacija o izvedbi kontrole |
| IE3QS2 | NES 🡪 | Zahtevek za dodatne informacije |
| IE3RS2 | 🡪 NES | Posredovanje dodatnih informacij |
| IE3SN3 | NES 🡪 | Rezultati kontrole |
| IE3SN4 | 🡪 NES | Strinjanje/nestrinjanje z rezultati kontrole |
| IE3S99 | 🡪 NES | Informacija o zavrnitvi/napaki |
| IE3SN9 | NES 🡪 | Obvestilo o vstopu (dovoljen/ni dovoljen) |

\* 🡪 NES: Sporočilo s strani deklaranta posredovano v NES

NES 🡪: Sporočilo s strani NES posredovano deklarantu

Tabela 3: Seznam elektronski sporočil

# Katalog elektronskih sporočil

Dokument, ki navaja tehnični opis oz. strukturo posameznih sporočil, uporabljene šifrante ter pogoje in pravila skupaj z njihovo razlago se nahaja spodaj:

## STANDARDI IN PRAVILA ZA SESTAVO ELEKTRONSKIH SPOROČIL

### STANDARDI

FURS na carinskem področju za izmenjavo elektronskih sporočil znotraj informacijskih sistemov uporablja standard XML v povezavi z elektronskim podpisom.

### PRAVILA ZA SESTAVO SPOROČIL V FORMATU XML

#### Priprava podatkov

Aplikacija pri deklarantu pripravi sporočilo v XML formatu, kot jo prepisujejo XSD sheme sporočil. Sporočilo je sestavljeno iz dveh delov:

* ovojnice sporočila (HEADER), ki je namenjena posredniku za dostavo sporočil in
* vsebine sporočila (body).

**Primer pripravljenega XML sporočila z ovojnico (HEADER):**

|  |
| --- |
| <?xml version=”1.0” encoding=”utf-8”?>  <Message>  <Header>  <Ovojnica FURS V1.0)  <!– vsebina ovojnice --!>  </Ovojnica FURS V1.0)  </Header>  <Body>  <Data>  <IE4XXB>  <!–vsebina sporočila --!>  </Data>  <Signatures/>  </Body>  </Message> |

Popolna dokumentacija o standardu XML se nahaja na internet naslovu <http://www.w3.org/> , domača stran konzorcija z imenom The World Wide Web Consortium (W3C).

#### Podpisovanje dokumentov

Varen elektronski podpis (elektronski podpis kvalificiranega digitalnega potrdila, ki ga je izdal overitelj[[1]](#footnote-1)) je namenjen zagotavljanju varnostnih funkcij avtentikacije (ugotavljanju, kdo je podpisal dokument), celovitosti (podpisani dokument ni mogoče spreminjati, ne da bi se to pri overjanju podpisa ugotovilo) in nezatajljivosti (pošiljatelj ne more zanikati izvedbe transakcije). Te funkcije (poleg funkcije zaupnosti, ki jo zagotavlja šifriranje vsebine in/ali komunikacijskih poti), dajejo digitalno podpisanemu dokumentu pravno veljavnost.

Partner podpiše XML datoteko s svojim osebnim digitalnim potrdilom. Pri podpisovanju se uporabi standarde podpisovanja, ki so navedeni v tabeli 1.

|  |  |  |
| --- | --- | --- |
| **Naziv standarda** | **Oznaka** | **Povezava** |
| **XML Signature Syntax** | XML-DSIG | [**http://www.w3.org/2000/09/xmldsig#**](http://www.w3.org/2000/09/xmldsig) |
| **DigestMethod** | SHA-1 | [**http://www.w3.org/2000/09/xmldsig#sha1**](http://www.w3.org/2000/09/xmldsig#sha1) |
| **CanonicalizationMethod** | W3C2 | [**http://www.w3.org/TR/2001/REC-xml-c14n-20010315**](http://www.w3.org/TR/2001/REC-xml-c14n-20010315) |
| **SignatureMethod** | RSA-SHA-1 | [**http://www.w3.org/2000/09/xmldsig#rsa-sha1**](http://www.w3.org/2000/09/xmldsig#rsa-sha1) |
| **Transform** | **Enveloped** | [**http://www.w3.org/2000/09/xmldsig#enveloped-signature**](http://www.w3.org/2000/09/xmldsig#enveloped-signature) |

Tabela 4: Standardi podpisovanja XML sporočil

**Primer podpisanega XML sporočila:**

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <Message>  <Header>  <!-- tukaj pridejo podatki namenjeni posredniku --!>  </Header>  <Body>  <Data>  <!-- tukaj pride vsebina --!>  </Data>  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">  <SignedInfo>  <CanonicalizationMethod  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>  <SignatureMethod  Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>  <Reference URI="">  <Transforms>  <Transform  Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  </Transforms>  <DigestMethod  Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>  <DigestValue>C46uP0TBETepXkxXZoX3pew2Rzs=</DigestValue>  </Reference>  </SignedInfo>  <SignatureValue>bsm...utU=</SignatureValue>  <KeyInfo>  <KeyValue>  <RSAKeyValue>  <Modulus>vsF...rc=</Modulus>  <Exponent>AQAB</Exponent>  </RSAKeyValue>  </KeyValue>  <X509Data>  <X509Certificate>MIIFlj...oX+</X509Certificate>  <X509SubjectName>CN=Gregor Irt,... O=ACNLB, C=SI</X509SubjectName>  <X509IssuerSerial>  <X509IssuerName>O=ACNLB, C=SI</X509IssuerName>  <X509SerialNumber>1053174896</X509SerialNumber>  </X509IssuerSerial>  </X509Data>  </KeyInfo>  </Signature>  </Body>  </Message> |

#### Šifriranje dokumentov

Šifriranje dokumentov zagotavlja zaupnost elektronskega poslovanja. Vsebino šifriranega sporočila lahko prebere samo prejemnik sporočila. To nepooblaščenim osebam, ki so lahko vključene v postopke elektronskega poslovanja (npr. posrednikom) onemogoča vpogled v vsebino sporočil. Postopek enkripcije dokumenta poteka tako, da se tisti del podpisane datoteke, v kateri je vsebina (*body*), šifrira s carinskim javnim ključem. Pri tem se uporabi standarde za enkripcijo, ki so navedeni v tabeli 2.

|  |  |  |
| --- | --- | --- |
| **Naziv standarda** | **Oznaka** | **Povezava** |
| **XML Encryption Syntax** | XML-ENC | [**http://www.w3.org/2001/04/xmlenc#**](http://www.w3.org/2001/04/xmlenc) |
| **Encryption Type** | Element | [**http://www.w3.org/2001/04/xmlenc#Element**](http://www.w3.org/2001/04/xmlenc#Element) |
| **Element Encryption** | TRIPLE DES | [**http://www.w3.org/2001/04/xmlenc#tripledes-cbc**](http://www.w3.org/2001/04/xmlenc#tripledes-cbc) |
| **Key Encryption** | **RSA1-5** | [**http://www.w3.org/2001/04/xmlenc#rsa-1\_5**](http://www.w3.org/2001/04/xmlenc#rsa-1_5) |

Tabela 5: Standardi za enkripcijo

Pri pošiljanju nazaj je postopek podoben, s to razliko, da se enkripcija dokumenta izvede z javnim ključem prejemnika.

**Primer podpisanega in kodiranega XML sporočila:**

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <Message>  <Header>  <!-- tukaj pridejo podatki namenjeni posredniku --!>  </Header>  <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"  Type="http://www.w3.org/2001/04/xmlenc#Element">  <EncryptionMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1\_5"/>  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">  <KeyName>carina</KeyName>  </KeyInfo>  <CipherData>  <CipherValue>RpkU7cAw...JMF3Y=</CipherValue>  </CipherData>  </EncryptedKey>  </KeyInfo>  <CipherData>  <CipherValue>B+6/jX9DQX... tj3nQoOBBAXeBHuW6t/5ADW7a4fPL6E=</CipherValue>  </CipherData>  </EncryptedData>  </Message> |

#### Kontrola preklicanih certifikatov

Sistem SIAIS2 preverja veljavnost digitalnega potrdila in s tem onemogoči nepooblaščen dostop do sistema. Digitalno potrdilo je veljavno, če ga je izdal registriran overitelj, če datum veljavnosti certifikata ni pretekla in če certifikat ni na listi preklicanih certifikatov.

Listo preklicanih certifikatov (CRL) objavlja vsak registriran overitelj (običajno preko http ali ldap protokola) in so javno dostopne. ICS večkrat dnevno pridobi ažurne liste preklicanih certifikatov.

#### Preklic certifikata

Pri postopku preklica certifikata FURS ne sodeluje direktno. Vlagatelji oz. partnerji morajo preklicati certifikat pri overitelju, ki ga je izdal. FURS pa ob osvežitvi CRL dobi informacijo o preklicu.

#### Časovni žig

Časovni žig se uporablja za zagotavljanje, da je bil dokument podpisan z veljavnim digitalnim potrdilom v določenem časovnem trenutku in sicer na način, da povezujejo datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način. Dokument se časovno žigosa na strani strežnika. FURS uporablja storitev časovnega žigosanja pri zaenkrat edinem registriranem izdajatelju varnih časovnih žigov SI-TSA (<http://www.si-tsa.si/>).

#### Formati polj

Uporabljene formate datumskih polj predstavlja tabela 3.

|  |  |  |
| --- | --- | --- |
| **Polje** | **Format** | **Primer** |
| **Leto** | YYYY | 2006 |
| **Leto in mesec** | YYYY-MM | 2006-01 |
| **Celoten datum** | YYYY-MM-DD | 2006-01-01 |
| **Celoten datum in ura** | YYYY-MM-DDThh:mmTZD | 2006-01-01T19:20+01:00 |
| **Celoten datum, ura, minuta in sekunda** | YYYY-MM-DDThh:mm:ssTZD | 2006-01-01T19:20:30+01:00 |
| **Celoten datum, ura, minuta in sekunda z decimalkami** | YYYY-MM-DDThh:mm:ss.sTZD | 2006-01-01T19:20:30.45+01:00 |

Tabela 6: Formati datumskih polj

Posamezen format datumskega polja predstavlja naslednje:

* **YYYY** = 4-mestna letnica
* **MM** = dve mesti za mesec (01=januar, itd.)
* **DD** = dve mesti za dan v mesecu (01 do 31)
* **hh** = dve mesti za uro (00 do 23) (am/pm ni dovoljeno)
* **mm** = dve mesti za minute (00 do 59)
* **ss** = dve mesti za sekunde (00 do 59)
* **s** = eno ali več mest za decmilna mesta sekunde
* **TZD** = določitev časovnega pasu (Z ali +hh:mm ali -hh:mm)

#### Preverjanje strukture XML dokumentov

Pri preverjanju XML dokumentov se preveri, če je XML pripravljen v obliki, ki jo predpisujejo XSD sheme. Struktura dokumentov preveri dokument do te mere, da je možno vsak dokument, ki prestane to preverjanje, zapisati v bazo podatkov.

Sheme za preverjanje strukture XML dokumentov so del dokumentacije NES.

## Strukture XML sporočil

Strukture elektronskih sporočil sistema NES določajo tehničen in vsebinski pomen posameznih polj znotraj XML sporočil.

Uporabljene oznake in njihov pomen pri določanju strukture elektronskih sporočil je predstavljen v tabeli 4.

|  |  |  |
| --- | --- | --- |
| **Oznaka** |  | **Pomen oznake** |
| **Število ponovitev** | | Označuje minimalna in maksimalna ponovitev podatkovne skupine oz. elementa |
|  | 0..1 | opcijski podatek z maksimalnim številom ponovitve 1 |
|  | 1..1 | obvezen podatek z maksimalnim številom ponovitve 1 |
|  | 0..99 | opcijski podatek z maksimalnim številom ponovitve 99 |
|  | 0..9999 | opcijski podatek z maksimalnim številom ponovitve 9999 |
| **Status** | | Označuje stanje podatkovne skupine oz. posameznega elementa |
|  | M | Obvezno polje (vedno mora biti podatek izpolnjen) |
|  | O | Neobvezno polje (mora biti na voljo, če obstaja) |
|  | C ali D | Pogojno obvezno polje (je obvezno ali neobvezno, odvisno od pogojev, ki veljajo za podatkovno grupo oz. element) |
| **Format polja** | | Oblika posameznega elementa |
|  | a | abecedni znaki |
|  | n | numerični znaki |
|  | a3 | abecedni znaki s fiksno dolžino 3 |
|  | a..3 | abecedni znaki katerih maksimalna dolžina je 3 |
|  | n3 | numerični znaki s fiksno dolžino 3 |
|  | n..3 | numerični znaki katerih maksimalna dolžina je 3, |
|  | an | alfanumerični znaki (abecedni znaki, numerični znaki oz. kombinacija abecednih in numeričnih znakov), |
|  | an3 | alfanumerični znaki (abecedni znaki, numerični znaki oz. kombinacija abecednih in numeričnih znakov) s fiksno dolžino 3. |
|  | an..3 | alfanumerični znaki (abecedni znaki, numerični znaki oz. kombinacija abecednih in numeričnih znakov), katerih maksimalna dolžina je 3. |
|  | n..3,1 | 3 numerični znaki, od katerih je zadnje (1) mesto decimalno mesto. |
| **Vzorec** | | Način izpolnjevanja podatkovnih elementov |
|  | [A-Z] | Podatkovni element lahko vsebuje samo velike črke |
| **CLXXX** | | Referenčna številka uporabljenega šifranta |
| **RXXX** | | Oznaka uporabljenega pravila v podatkovni skupini oz. elementu |
| **CXXX** | | Oznaka uporabljenega pogoja v podatkovni skupini oz. elementu |
|  |  |  |

Tabela 7: Oznake strukture sporočil in njihov pomen

V nadaljevanju so navedena sporočila (z njihovim opisom), ki se uporabljajo v sistemu NES.

|  |  |
| --- | --- |
| **Sporočilo** | **Opis** |
| **IE3S10**  Predložitev blaga | Namen uporabe sporočila: Deklarant obvesti oddelek za carinjenje (OC), da je blago predloženo (IE3S10). V primeru e-trgovanja navede tudi dodatne podatke o pošiljki v segmentu »Calculation of duties« |
| **IE3RS8**  Blago predloženo | Namen uporabe sporočila: OC blaga obvesti deklaranta, da je blago uspešno predloženo (IE3RS8). |
| **IE3S08**  Informacija o izvedbi kontrole | Namen uporabe sporočila: OC predložitve blaga obvesti deklaranta o nameravani izvedbi kontrole nad predloženim blagom (IE3S08). |
| **IE3QS2**  Zahtevek za dodatne informacije | Namen uporabe sporočila: OC predložitve blaga posreduje deklarantu zahtevek za posredovanje dodatnih informacij (podatkov in/ali listin) (IE3QS2). |
| **IE3RS2**  Posredovanje dodatnih informacij | Namen uporabe sporočila: Deklarant na podlagi prejetega zahtevka za dodatne informacije (IE3QS2) posreduje dodatne informacije OC predložitve blaga (IE3RS2). |
| **IE3SN3**  Rezultat kontrole | Namen uporabe sporočila: OC predložitve blaga posreduje deklarantu rezultate opravljene kontrole nad predloženim blagom (IE3SN3). |
| **IE3SN4**  Strinjanje/nestrinjanje z rezultati kontrole | Namen uporabe sporočila: Deklarant na podlagi prejema rezultatov kontrole (IE3SN3) OC predložitve blaga posreduje svoje strinjanje oz. nestrinjanje z rezultati kontrole carinskega urada vložitve predložitve blaga. |
| **IE3SA4**  Dopolnitve s strani deklaranta | Namen uporabe sporočila: Deklarant na podlagi rezultatov kontrole posreduje morebitne dopolnitve VSD. (IE3SA4). |
| **IE3SN5**  Obvestilo o prepustitvi | Namen uporabe sporočila: OC predložitve blaga obvesti deklaranta o prepustitvi blaga (IE3SN5). |
| **IE3SN6**  Obvestilo o vročitvi/ne vročitvi blaga | Namen uporabe sporočila: Deklarant obvesti carinski urad vložitve predložitve blaga o uspešni oz. neuspešni vročitvi blaga (IE3SN6). |
| **IE3SN7**  Obvestilo o naknadni vrnitvi blaga | Namen uporabe sporočila: : Deklarant obvesti carinski urad vložitve predložitve blaga o vrnitvi blaga (IE3SN7). |
| **IE3SN9**  Obvestilo o zavrnitvi blaga | Namen uporabe sporočila: OC predložitve blaga ne prepusti blaga v prost promet (IE3SN9) zaradi potrebe po vložitvi redne uvozne carinske deklaracije. |
| **IE3S99**  Informacije o zavrnitvi/napaki | Namen uporabe sporočila: OC predložitve obvesti deklaranta o zavrnitvi predložitve oz. drugih napakah (IE3S99). |

Tabela 8: Oznake strukture sporočil in njihov pomen

Elektronsko sporočilo mora biti sestavljeno tako, kot ga predpisujejo struktura in XSD sheme.

## Pogoji in pravila podatkovnih skupin oz. elementov

Pri kreiranju posameznih podatkovnih skupin oz. elementov posameznih XML sporočil je potrebno upoštevati tudi določene pogoje in/ali pravil. Obveznost uporabe določenih pogojev in/ali pravil na posamezni podatkovni skupini oz. posameznega elementa je navedena v strukturi posameznega XML sporočila. Seznam vseh pogojev in pravil se nahaja na v spodnji datoteki.



## Šifranti

Šifranti predstavljajo niz določenih vrednosti s pripadajočim pomenom, ki se uporabljajo pri kreiranju posameznih podatkovnih skupin oz. posameznih podatkovnih elementov elektronskih sporočil.

Obveznost uporabe določenega šifranta za določeno podatkovno skupino oz. podatkovni element elektronskega sporočila je navedena v strukturi posameznega XML sporočila.

Seznam in podrobnosti vseh uporabljenih šifrantov v okviru sistema NES se nahaja v spodnji datoteki.



1. Registrirani overitelji digitalnih potrdil v Republiki Sloveniji so trenutno:

   * SIGEN CA
   * AC NLB
   * POŠTA®CA
   * HALCOMCA

   [↑](#footnote-ref-1)