



2023/2790

18.12.2023.

**KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2023/2790**

**(2023. gada 14. decembris),**

**ar ko nosaka funkcionālās un tehniskās specifikācijas valsts jūras vienloga sistēmas ziņošanas saskarņu moduļim**

**(Dokuments attiecas uz EEZ)**

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2019/1239 (2019. gada 20. jūnijs), ar ko izveido Eiropas Jūras vienloga sistēmas vidi un ar ko atceļ Direktīvu 2010/65/ES <sup>(1)</sup>, un jo īpaši tās 6. panta 1. punktu un 12. panta 4. punktu,

apspriedusies ar Digitālā transporta un tirdzniecības veicināšanas komiteju,

tā kā:

- (1) Ziņošanas saskarņu moduļa specifikācijām vajadzētu balstīties uz viegli pieejamu tehnoloģiju, kas būtu viegli uzstādāma un integrējama visās valsts jūras vienloga sistēmās (MNSW), un būtu jāļauj to netraucēti integrēt un uzturēt nākotnē.
- (2) Ziņošanas saskarņu moduļa funkcionālajām un tehniskajām specifikācijām vajadzētu balstīties uz augsta līmeņa sadarbības prasību risinājuma arhitektūras veidņu (HL SAT) konstrukcijas vadlīnijām un pieļaut izsekojamību starp augsta līmeņa un detalizētām sadarbības prasībām.
- (3) Ņemot vērā, ka nosūtītāji izmanto dažādas ziņošanas sistēmas un MNSW ir ieviestas, izmantojot dažādas tehnoloģijas, ziņošanas saskarņu moduli vajadzētu veidot uz tādu tehnoloģiju pamata, kas ļauj apmainīties ar informāciju starp dažādām informācijas sistēmām, kuras izmanto standartizētu protokolu, tādējādi uzlabojot sadarbību.
- (4) Regulas (ES) 2019/1239 pielikumā uzskaitītie ziņošanas pienākumi drīkstētu prasīt deklarētājiem iesniegt personas datus, izmantojot ziņošanas saskarņu moduli, kas apmainītos ar informāciju tā, ka jebkādi personas dati ir apstrādāti saskaņā ar Eiropas Parlamenta un Padomes Regulām (ES) 2018/1725 <sup>(2)</sup> un (ES) 2016/679 <sup>(3)</sup>.
- (5) Tā kā Komisija ir izstrādājusi un atjauninājusi ziņošanas saskarņu moduli un izplatījusi to dalībvalstīm integrēšanai, būtu centralizēti jāpārvalda ziņošanas saskarņu moduļa jaunu versiju izplatīšana, programmatūras pareizas uzstādīšanas pārraudzība un ziņojumu īstenošanas rokasgrāmatas atjaunināšana, pēc iespējas ņemot vērā MNSW IT drošības prasības.
- (6) Lai garantētu ziņošanas saskarņu moduļa stabilitāti, drošību un veiktspēju, dalībvalstīm būtu jāspēj pārraudzīt tīkla datu plūsmu un analizēt sistēmas notikumus, kļūdas un izņēmumus, kā arī integrēt šo informāciju to esošajās pārraudzības sistēmās un procesos. Lai to paveiktu, ziņošanas saskarņu moduļim vajadzētu nodrošināt piemērotas funkcionalitātes, kas ļauj reģistrēt un saglabāt notikumus un nodrošina dalībvalstīm informāciju par tīkla datu plūsmu.

<sup>(1)</sup> OV L 198, 25.7.2019., 64. lpp.

<sup>(2)</sup> Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

<sup>(3)</sup> Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

- (7) Lai nodrošinātu drošu informācijas apmaiņu, izmantojot ziņošanas saskarņu moduli, vajadzīga nosūtītāju autentifikācija. Tāpēc kopīgajam lietotāju reģistram un piekļuves pārvaldības sistēmai būtu vajadzīga centrāla autentifikācijas sistēma un centrālais reģistrs kā galvenie komponenti. Šiem komponentiem būtu jādarbojas kopīgi, lai iespējotu nosūtītāja autentifikāciju visos ziņošanas saskarņu moduļos, nodrošinot vienotu autentifikācijas mehānismu.
- (8) Lai droši apmainītos ar informāciju, izmantojot ziņošanas saskarņu moduli, un nodrošinātu lietotāju atpazīšanu ES līmenī, kad tie piekļūst jebkurai ziņošanas saskarņu modulim, nosūtītājiem būtu jāiegūst kvalificēts elektroniskā zīmoga sertifikāts, kas atbilst Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014 <sup>(4)</sup> noteiktajām prasībām.
- (9) Lai nosūtītājiem nodrošinātu vienotu reģistrāciju nolūkā veikt informācijas apmaiņu dažādās dalībvalstīs, izmantojot harmonizētas ziņošanas saskarnes, dalībvalstīm būtu jāspēj reģistrēt nosūtītājus centrālajā reģistrā. Tas mazinātu vairākkārtīgu reģistrāciju slogu pārrobežu darbībās vairākās MNSW. Jebkādi personas dati centrālajā reģistrā būtu jāpārvalda saskaņā ar Regulām (ES) 2018/1725 un (ES) 2016/679.
- (10) Lai mazinātu dalībvalstu palaušanos uz centrālajiem pakalpojumiem un ņemot vērā to, ka valstu autentifikācijas pakalpojumi jau drīkstētu atbalstīt MNSW, kā alternatīvu Eiropas Jūras vienloga sistēmas vides (EMSW<sub>e</sub>) lietotāju reģistram un piekļuves pārvaldības sistēmai būtu jāļauj dalībvalstīm arī atkārtoti izmantot valstu autentifikācijas pakalpojumus un valstu reģistrus, lai autentificētu nosūtītājus, kuri vēlas izmantot ziņošanas saskarņu moduli.
- (11) Lai ļautu dalībvalstīm pareizi integrēt MNSW ziņošanas saskarņu moduli un lietotāju reģistra un piekļuves pārvaldības sistēmu, šī regula būtu jāpiemēro no tā paša datuma, kad Regula (ES) 2019/1239.
- (12) Saskaņā ar Regulas (ES) 2018/1725 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas sniedza atzinumu 2023. gada 18. oktobrī,

IR PIENĒMUSI ŠO REGULU.

#### 1. pants

#### Definīcijas

Šajā regulā piemēro šādas definīcijas:

- 1) “ziņošanas saskarņu modulis” ir MNSW starpprogrammatūras komponents, kas minēts Regulas (ES) 2019/1239 2. panta 4. punktā;
- 2) “nosūtītājs” ir deklarētājs vai datu pakalpojuma nodrošinātājs, kas darbina IT sistēmu, kura nosūta elektroniskus ziņojumus uz MNSW vai saņem tos ar ziņošanas saskarņu moduļa starpniecību;
- 3) “formalitāte” ir formalitāte, kas definēta Komisijas Īstenošanas regulas (ES) 2023/204 <sup>(5)</sup> 1. pantā;
- 4) “AS4” ir ziņojuma protokols, kura pamatā ir tīmekļa pakalpojumi, drošai ziņojumu apmaiņai starp divām pusēm;
- 5) “ziņojums” ir to formalitāšu vai atbildes ziņojumu digitāla reprezentācija, ko izmanto saziņai starp nosūtītāju un MNSW;
- 6) “AS4 piekļuves punkts” ir servera programmnodrošinājums, kas ir saderīgs ar AS4 ziņojumu protokolu un ziņošanas saskarņu moduļa prasībām, tā iespējot informācijas nosūtīšanu uz ziņošanas saskarņu moduli un saņemšanu no tā nosūtītāja vārdā;

<sup>(4)</sup> Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).

<sup>(5)</sup> Komisijas Īstenošanas regula (ES) 2023/204 (2022. gada 28. oktobris), ar ko nosaka tehniskās specifikācijas, standartus un procedūras Eiropas Jūras vienloga sistēmas videi saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/1239 (OV L 33, 3.2.2023., 1. lpp.).

- 7) "MNSW kodols" ir MNSW tehnisks komponents, kurā ir integrēts ziņošanas saskarņu modulis;
- 8) "sintakses validācija" ir pārbaudes process, kurā pārbauda, vai elektroniskā ziņojumā nav programmēšanas, struktūras vai stila kļūdu;
- 9) "semantikas validācija" ir process, kurā tiek pārbaudīta datu atbilstība specifiskiem datu noteikumiem formalitātes ietvaros;
- 10) "ziņojumu īstenošanas rokasgrāmata" ir funkcionāla specifikācija, kurā noteikti standarti un ziņojumi, ar ko jāapmainās starp nosūtītājiem un MNSW ar ziņošanas saskarņu moduļa starpniecību;
- 11) "reģistrēšana" ir process, kurā fiziska vai juridiska persona identificējas un izveido kontu iestādē, kas minēta Regulas (ES) 2019/1239 12. panta 2. punktā;
- 12) "identifikācija" ir elektroniskā identifikācija, kas definēta Regulas (ES) Nr. 910/2014 3. panta 1. punktā;
- 13) "elektroniskās identifikācijas līdzekļi" ir elektroniska identifikācija, kas definēta Regulas (ES) Nr. 910/2014 3. panta 2. punktā;
- 14) "autentifikācija" ir autentifikācija, kas definēta Regulas (ES) Nr. 910/2014 3. panta 5. punktā;
- 15) "sertifikāts" ir kvalificēts elektroniskā zīmoga sertifikāts, kas definēts Regulas (ES) Nr. 910/2014 3. panta 30. punktā un ko izdevis kvalificēts uzticamības pakalpojumu sniedzējs, kas definēts Regulas (ES) Nr. 910/2014 3. panta 20. punktā;
- 16) "EORI numurs" ir identifikācijas numurs, kas definēts Komisijas Deleģētās regulas (ES) 2015/2446 <sup>(6)</sup> 1. panta 18. punktā;
- 17) "EMSWē lietotāju reģistra un piekļuves pārvaldības sistēma" ir Komisijas pārvaldīta sistēma, kas aptver centrālo reģistru un centrālo autentifikācijas pakalpojumu un nodrošina elektronisko identifikācijas līdzekļu un autentifikācijas savstarpēju atzīšanu drošai pārrobežu datu apmaiņai starp nosūtītājiem un MNSW ar ziņošanas saskarņu moduļa starpniecību;
- 18) "centrālais reģistrs" ir Komisijas pārvaldīts reģistrs, kas satur dalībvalstu sniegtus nosūtītāju reģistrācijas datus nosūtītāju autentifikācijas atvieglošanai;
- 19) "nacionālais reģistrs" ir dalībvalsts pārvaldīts reģistrs, kas satur nosūtītāju reģistrācijas datus un kuru var izmantot, lai atvieglotu nosūtītāju autentifikāciju, ja tā atbilst centrālā autentifikācijas pakalpojuma prasībām;
- 20) "centrālais autentifikācijas pakalpojums" ir Komisijas pārvaldīts pakalpojums, kas autentificē nosūtītājus, kuri izmanto ziņošanas saskarņu moduli;
- 21) "nacionālais autentifikācijas pakalpojums" ir dalībvalsts pārvaldīts pakalpojums, kuru drīkst izmantot, lai autentificētu nosūtītājus, kuri izmanto ziņošanas saskarņu moduli.

## 2. pants

Ziņošanas saskarņu modulis atbilst pielikuma I daļā noteiktajām funkcionālajām un tehniskajām specifikācijām.

Lai palīdzētu ziņošanas saskarņu moduli integrēt MNSW, Komisija ciešā sadarbībā ar valstu EMSWē koordinatoriem:

- definē pamatnostādnes ziņošanas saskarņu moduļa testēšanai un konfigurēšanai, lai to integrētu attiecīgā MNSW;
- definē un ar Eiropas Jūras drošības aģentūras palīdzību uztur ziņojumu īstenošanas rokasgrāmatu.

<sup>(6)</sup> Komisijas Deleģētā regula (ES) 2015/2446 (2015. gada 28. jūlijs), ar ko papildina Eiropas Parlamenta un Padomes Regulu (ES) Nr. 952/2013 attiecībā uz sīki izstrādātiem noteikumiem, kuri attiecas uz dažiem Savienības Muitas kodeksa noteikumiem (OV L 343, 29.12.2015., 1. lpp.).

*3. pants*

Centrālo reģistru un centrālo autentifikācijas pakalpojumu izveido saskaņā ar pielikuma II daļā noteiktajām tehniskajām specifikācijām, standartiem un procedūrām.

*4. pants*

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas Eiropas Savienības Oficiālajā Vēstnesī.

To piemēro no 2025. gada 15. augusta.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2023. gada 14. decembrī

Komisijas vārdā –  
priekšsēdētāja  
Ursula VON DER LEYEN

---

## PIELIKUMS

## I DAĻA

## ZIŅOŠANAS SASKARŅU MODULIS

## ARHITEKTŪRA UN TVĒRUMS

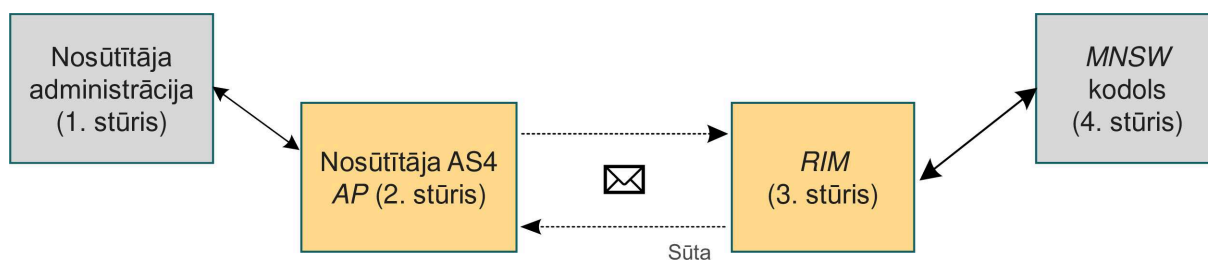
RIM ir daļa no četru stūru modeļa ziņojumiem, ar ko apmainās nosūtītāji (1. stūris) un MNSW kodols (4. stūris) un kas tiek sūtīti caur AS4 piekļuves punktiem (2. un 3. stūris) no katras puses, kura ieviesusi AS4 protokolu pārraidīšanai un drošībai, šādi:

1.stūris: nosūtītāja administrācija sagatavo, iesniedz un saņem ziņojumus no MNSW kodola un sūta tam;

2.stūris: nosūtītāja AS4 piekļuves punkts;

3.stūris: RIM;

4.stūris: MNSW kodols saņem ziņojumus un sūta nosūtītājam atbildes ziņojumus.



Attēls Nr. 1 – augsta līmeņa RIM arhitektūra

RIM neveic ziņojumu semantikas validāciju ārpus ziņojumu īstenošanas rokasgrāmatas specifikācijām, nerēķinās ar to secību un neuzglabā ziņojumus pēc to sekmīgas nosūtīšanas MNSW kodolam vai nosūtītājam.

Kad ziņojums ir nosūtīts no RIM uz MNSW kodolu, dalībvalstis saskaņā ar Regulas (ES) 2019/1239 5. panta 3. punkta c) apakšpunktu attiecīgā gadījumā pārtulko, validē un pārraida formalitātes datus uz attiecīgo iestāžu sistēmām atbilstoši minēto sistēmu specifikācijām.

## RIM FUNKCIONĀLĀS SPECIFIKĀCIJAS

| ID         | Funkcija                                                           | Apraksts                                                                                                                                                                                                                                                            |
|------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LR1</b> | Reģistrācija un uzraudzība                                         | Funkcija nodrošina notikumu (piegādes neveikšanas, aizkavēšanās un kļūdas saņēmēja pusē) reģistrāciju un uzglabāšanu.                                                                                                                                               |
| <b>LR2</b> | Metadatu uzglabāšana                                               | Funkcija nodrošina metadatu uzglabāšanu par ziņojumiem, ar kuriem notikusi apmaiņa.                                                                                                                                                                                 |
| <b>OA1</b> | Tehnisko datu uzglabāšana un uzmeklēšana                           | Funkcija nodrošina to tehnisko datu uzglabāšanu un uzmeklēšanu, kuri prasīti RIM konfigurācijai un darbībai ar saskarnes starpniecību (piem., nosūtītāju AS4 piekļuves punktu tehniskās adreses, ziņojumu īstenošanas rokasgrāmatā norādītās ziņojumu shēmas utt.). |
| <b>OA2</b> | Izņēmumu apstrāde                                                  | Funkcija ar lietotāja saskarnes starpniecību nodrošina paziņojumus par konstatētajām apstrādes kļūdām un/vai anormāliem apstākļiem.                                                                                                                                 |
| <b>OA3</b> | Piekļuve informācijai un metadatiem par reģistrāciju un uzraudzību | Funkcija ar sistēmu savstarpējās komunikācijas saskarnes starpniecību nodrošina MNSW kodolam piekļuvi informācijai un metadatiem par reģistrāciju un uzraudzību attiecībā uz ziņojumiem, ar kuriem notikusi apmaiņa.                                                |

|            |                            |                                                                                                                                                                                                                                                                           |
|------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OA4</b> | Nosūtītāja autentifikācija | Funkcija iedarbina nosūtītāja autentifikācijas procesu, izmantojot centrālo vai nacionālo autentifikācijas pakalpojumu.                                                                                                                                                   |
| <b>OA5</b> | Ziņojuma validācija        | Funkcija veic saņemto ziņojumu sintakses un semantikas validāciju saskaņā ar ziņojuma tehniskajām specifikācijām, kas definētas ziņojumu īstenošanas rokasgrāmatā. Ziņojumu īstenošanas rokasgrāmatā norāda, kuras validācijas veic RIM. RIM attiecīgi paziņo par kļūdām. |
| <b>MF1</b> | Ziņojumu apstrāde          | Funkcija nodrošina to, ka saņemto ziņojumu saturs (formalitāte vai atbilde) tiek bez pārveidojumiem pārraidīts uz attiecīgo stūri, ja validācijas bijušas sekmīgas.                                                                                                       |

## RIM TEHNISKĀS SPECIFIKĀCIJAS

### Integrācija

| ID         | Nosaukums                           | Apraksts                                                                                                                      |
|------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>IA1</b> | Ziņojumapmaiņas protokola standarts | RIM izmanto AS4 ziņojumapmaiņas protokolu, lai atvieglotu sadarbību ar nosūtītāju dažādām tehnoloģijām un ziņošanas sistēmām. |

### Ziņojumapmaiņa

| ID         | Nosaukums                          | Apraksts                                                                                                                       |
|------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>AP1</b> | Asinhrons ziņojumapmaiņas raksturs | RIM atbalsta ziņojumu asinhronu pārraidi uz MNSW kodolu un no tā (formalitāte un atbilde) ar stumšanas un vilkšanas mehānismu. |

### Drošība

| ID         | Nosaukums                                          | Apraksts                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SA1</b> | Informācijas apmaiņas konfidencialitāte un drošība | RIM nodrošina informācijas konfidencialitāti un jebkādu personas datu aizsardzību, ar ko notiek apmaiņa, šifrējot informācijas apmaiņu starp nosūtītāju AS4 piekļuves punktu un RIM. RIM atšifrē nosūtītāja sūtītos ziņojumus un dara pieejamus MNSW kodolam. RIM izmanto tīmekļa pakalpojumu drošību (WSS) kā standartu, kas ļauj droši apmainīties ar ziņojumiem starp nosūtītāja AS4 piekļuves punktu un RIM. |
| <b>SA2</b> | Ziņojumu nenoliedzamība                            | Ziņojumu komunikācija un validācija caur RIM ietver drošības pasākumus, ar ko nodrošina ziņojumu autentiskumu un izvairās no ziņojumu noliegšanas.                                                                                                                                                                                                                                                               |

|            |                        |                                                                                                                                                                                                                                                   |
|------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SA3</b> | Integritāte            | Veic tehniskus pasākumus, lai nodrošinātu integritāti datiem, ar kuriem notikusi apmaiņa.                                                                                                                                                         |
| <b>SA4</b> | Lietojums Drošība      | RIM balstās uz programmatūras veidošanas paraugpraksi, kas ļauj konstatēt ļaunprātīgas aktivitātes, un sensitīvas informācijas drošu pārraidi.                                                                                                    |
| <b>SA5</b> | Pakalpojuma pieejamība | Uzticamas komunikācijas un informācijas izplatīšanas nolūkā starp nosūtītājiem un valsts jūras vienloga sistēmām RIM īsteno mehānismus, kas nodrošina to, ka ziņojumi, ar kuriem notiek apmaiņa ar RIM, nezūd pakalpojuma nepieejamības gadījumā. |

### Veiktspēja un mērogojamība

| ID         | Nosaukums                  | Apraksts                                                                                                                                                                                       |
|------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PS1</b> | Veiktspēja un mērogojamība | RIM spēj atbilst tādiem pašreizējiem un nākotnes veiktspējas mērķiem kā reakcijas laiks, vienlaicīgi ziņojumus sūtošu nosūtītāju skaits un ziņojumu, ar kuriem notiek apmaiņa, skaits/lielums. |

### Pārnesamība un izvēršana

| ID         | Nosaukums                        | Apraksts                                                                                                                                                                                                                       |
|------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PD1</b> | Platformas neatkarība            | RIM ir saderīgs ar visizplatītākajām aparatūras arhitektūrām un operētājsistēmām, kur RIM varētu tikt izvērsts. RIM nevajadzētu uzstādīšanas vai konfigurācijas nolūkā prasīt īpašniekprogrammatūru vai īpašniekprogrammatūru. |
| <b>PD2</b> | Pašinstalējoša lietojumprogramma | RIM nodrošina kā programmatūras pakotni, kas satur visus RIM vajadzīgos lietojumprogrammas komponentus. Katrā informācijā par RIM laidieni uzskaita nodrošinātās un vajadzīgās atkarības.                                      |

## II DAĻA

### EMSWē LIETOTĀJU REĢISTRA UN PIEKĻUVES PĀRVALDĪBAS SISTĒMA

#### CENTRĀLAIS REĢISTRS

Pēc nosūtītāja pieprasījuma dalībvalstis, kuras nenodrošina nacionālo reģistru, kas atbilst šajā pielikumā noteiktajām centrālā reģistra specifikācijām, centrālajā reģistrā reģistrē EORI numuru un nosūtītāja sertifikātu un ir atbildīgas par datu verifikāciju, precizitāti un pārvaldību saskaņā ar Regulas (ES) 2019/1239 12. panta 2. punktu. Centrālais reģistrs nodrošina dalībvalstīm saskarni, kas veic nosūtītāju reģistrāciju un pārvaldību.

CENTRĀLAIS AUTENTIFIKĀCIJAS PAKALPOJUMS

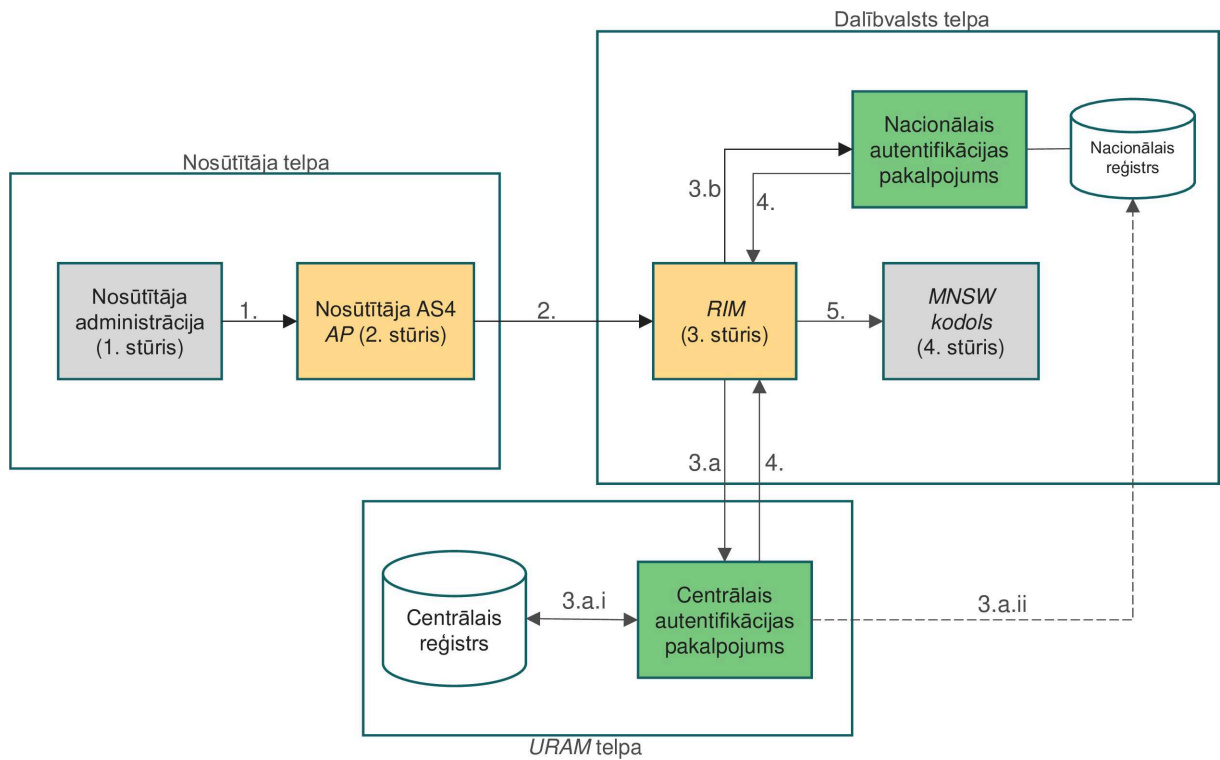
Turpmāk shēmā ilustrēti secīgi tā nosūtītāja autentifikācijas soļi, kurš sagatavo un nosūta ziņojumu RIM (1., 2. solis).

RIM izpilda “nosūtītāja autentifikācijas” funkciju <sup>(1)</sup>, izmantojot centrālo autentifikācijas pakalpojumu (3.a solis).

3.a solis. Centrālais autentifikācijas pakalpojums autentificē nosūtītāju, sūtot pieprasījumu centrālajam reģistram un pārbaudot relevanto ierakstu (3.a.i.) vai, ja nosūtītāja centrālajā reģistrā nav, sūtot pieprasījumu nosūtītāja valsts nacionālajam reģistram, ja tāds pieejams, un pārbaudot relevanto ierakstu (3.a.ii.).

3.b solis. Ja dalībvalstī ir izveidots un pieejams nacionālais autentifikācijas pakalpojums, RIM izpilda “nosūtītāja autentifikācijas” funkciju, izmantojot šo nacionālo autentifikācijas pakalpojumu, lai autentificētu tikai tos nosūtītājus, kuri izmanto minētajā dalībvalstī izdotu sertifikātu.

4. solis. Autentifikācijas rezultāts tiek sūtīts atpakaļ uz RIM. Ja autentifikācija ir sekmīga, ziņojums ir pieejams 4. stūrim (MNSW kodolam) (5. solis). Ja autentifikācija nav sekmīga, kļūmes ziņojums tiek nosūtīts atpakaļ uz 2. stūri.



Attēls Nr. 2

URAM TEHNISKĀS SPECIFIKĀCIJAS

Integrācija

| ID      | Nosaukums              | Apraksts                                                                                                                               |
|---------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| URAM.01 | Sadarbspējas standarti | URAM programmatūra izmanto standarta protokolus un robustas drošības īpašības, rādot tās saskarnes un integrējoties citos komponentos. |

<sup>(1)</sup> Identificēta šā pielikuma I daļā kā OA4 RIM funkcionālajās specifikācijās.



|                |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URAM.02</b> | <i>eIDAS</i> atbilstība | URAM programmatūra izmanto atvērtus ES standartus un risinājumus un īsteno nepieciešamos kontroles mehānismus, lai pārbaudītu nosūtītāja sertifikātus uzticamo sarakstā, ko dalībvalstis publicē saskaņā ar Regulas (ES) Nr. 910/2014 22. pantu un Komisijas Īstenošanas lēmumu (ES) 2015/1505 <sup>(2)</sup> , tai skaitā informāciju saistībā ar kvalificētiem uzticamības pakalpojuma sniedzējiem, kuri izdod sertifikātus elektronisko zīmogu izmantošanai. |
|----------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Drošība

| ID             | Nosaukums                               | Apraksts                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URAM.03</b> | Informācijas apmaiņas konfidencialitāte | Lai nodrošinātu URAM programmatūras un jebkādu personas datu apmaiņas drošību, īsteno šādus protokolus un šifrēšanas metodes: <ul style="list-style-type: none"> <li>— transporta slāņa drošība (TLS): visa URAM programmatūra ir padarīta droša, izmantojot TLS, lai nodrošinātu tīkla līmeņa datu šifrēšanu un integritāti nolūkā aizsargāt datus pārraides laikā, novērst nesankcionētu piekļuvi vai neatļautu iejaukšanos.</li> <li>— TLS konfigurāciju ievieš, lai komunicētu ar URAM programmatūru.</li> </ul>                                                                                     |
| <b>URAM.04</b> | Lietojumprogrammas drošība              | URAM programmatūra garantē ļaunprātīgu aktivitāšu konstatāciju un sensitīvas informācijas drošu pārraidi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>URAM.05</b> | Personas datu aizsardzība               | Nosūtītāju reģistrācijas nolūkā dalībvalstu iestādēm piešķir piekļuves tiesības atbilstoši Regulas (ES) 2019/1239 12. panta 2. punktam. URAM programmatūrā īsteno piekļuves kontroles mehānismus, lai nodrošinātu tās lietotāja informācijas aizsardzību, kas ir personas dati, ko apstrādā tikai nolūkā izveidot lietotāja kontus un pārvaldīt attiecīgās piekļuves tiesības. Centrālais autentifikācijas pakalpojums patur nosūtītāju personas datus ne ilgāk, kā tas vajadzīgs autentifikācijai. Centrālais reģistrs patur nosūtītāju personas datus ne ilgāk, kā tas nepieciešams konta pārvaldībai. |

### Ilgtermiņa un pārnesamība

| ID             | Nosaukums               | Apraksts                                                                                                                                                                                                                                 |
|----------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URAM.06</b> | Tehnoloģijas neatkarība | URAM programmatūra atļauj mijiedarbību ar RIM un citiem relevantiem pakalpojumiem bez vajadzības pēc īpašniekprogrammatūras vai īpašniekaparātūras un atļauj integrāciju ar RIM neatkarīgi no tehnoloģiskās vides, kurā RIM ir izvērsti. |

<sup>(2)</sup> Komisijas Īstenošanas lēmums (ES) 2015/1505 (2015. gada 8. septembris), kurā saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 22. panta 5. punktu izklāstītas tehniskās specifikācijas un formāti, kas attiecas uz uzticamības sarakstiem (OV L 235, 9.9.2015., 26. lpp.).

|                |                       |                                                                                                                                                                                                                |
|----------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URAM.07</b> | Neatkarīga izvērsšana | URAM programmatūra neprasa no RIM specifiskas izvērsšanas prasības izpildi. RIM vajadzētu nodrošināt tikai piekļuvi internetam un ar URAM programmatūras drošību un protokoliem saistītu standartu ievērošanu. |
|----------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Centrālā autentifikācijas pakalpojuma funkcijas

No centrālā autentifikācijas pakalpojuma RIM ir darīti pieejami šādi pakalpojumi.

| ID             | Nosaukums                    | Apraksts                                                                                                                                                                                                                                                                                                              |
|----------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URAM.08</b> | Autentifikācijas pakalpojums | Centrālais autentifikācijas pakalpojums ir atbildīgs par nosūtītāja autentifikāciju, verificējot sertifikāta derīgumu, EORI numuru un saikni starp nosūtītāja EORI numuru un tā sertifikātu. Tas apstrādā RIM sūtītos autentifikācijas pieprasījumus un nodrošina atbildes par sekmīgu vai nesekmīgu autentifikāciju. |

### Centrālā reģistra specifikācijas

| ID             | Nosaukums                     | Apraksts                                                                                                                                                                                                                                    |
|----------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URAM.09</b> | Nosūtītāja reģistrācija       | Centrālais reģistrs nodrošina dalībvalstīm grafisku lietotāja saskarni nosūtītāja datu reģistrācijai. Nosūtītājs ir reģistrēts visās dalībvalstīs, tiklīdz tas reģistrēts centrālajā reģistrā.                                              |
| <b>URAM.10</b> | Nosūtītāja skats un meklēšana | Centrālais reģistrs ļauj dalībvalstīm redzēt visus datus par nosūtītājiem, kurus tā iepriekš reģistrējusi. Tas nodrošina arī meklēšanas funkciju, kas izgūst tās reģistrēto nosūtītāju datus pēc dažādiem meklēšanas kritērijiem.           |
| <b>URAM.11</b> | Nosūtītāja atjauninājums      | Centrālais reģistrs ļauj dalībvalstij pārveidot visus tās iepriekš reģistrēto nosūtītāju datus, lai nodrošinātu datu precizitāti un derīgumu.                                                                                               |
| <b>URAM.12</b> | Nosūtītāja deaktivācija       | Centrālais reģistrs ļauj dalībvalstij deaktivēt tās iepriekš reģistrētus nosūtītājus.                                                                                                                                                       |
| <b>URAM.13</b> | Audits un ziņošana            | Centrālais reģistrs piedāvā ziņošanas iespējas, kas ļauj dalībvalstīm analizēt tādas tās iepriekš reģistrētu nosūtītāju datus kā reģistrācijas datums un sertifikāta derīgums.                                                              |
| <b>URAM.14</b> | Paziņojumi                    | Centrālais reģistrs piedāvā dalībvalstīm iespēju saņemt paziņojumu no centrālā reģistra ikreiz, kad minētās dalībvalsts reģistrēts nosūtītājs tiek reģistrēts, atjaunināts vai deaktivēts, kā arī tad, kad beidzas tā sertifikāta derīgums. |