Úradný vestník
Európskej únie

SK
Séria L

2023/2790

18.12.2023

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2023/2790

zo 14. decembra 2023,

ktorým sa stanovujú funkčné a technické špecifikácie modulu rozhrania na ohlasovanie vnútroštátnych námorných jednotných kontaktných miest

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1239 z 20. júna 2019, ktorým sa zriaďuje európske prostredie jednotnej námornej platformy a ktorým sa zrušuje smernica 2010/65/EÚ ([1]), a najmä na jeho článok 6 ods. 1 a článok 12 ods. 4,

po porade s Výborom na podporu digitálnej dopravy a obchodu,

keďže:

(1) Špecifikácie modulu rozhrania na ohlasovanie by mali byť založené na technológii, ktorá je ľahko prístupná, jednoducho sa inštaluje a integruje do všetkých vnútroštátnych námorných jednotných kontaktných miest a mala by v budúcnosti umožňovať bezproblémovú integráciu a údržbu.

(2) Funkčné a technické špecifikácie modulu rozhrania na ohlasovanie by mali byť založené na usmerneniach k návrhu vzoru architektúry riešení požiadaviek na interoperabilitu na vysokej úrovni, aby sa umožnila vysledovateľnosť medzi požiadavkami na interoperabilitu na vysokej úrovni a podrobnými požiadavkami na interoperabilitu.

(3) Vzhľadom na to, že odosielatelia používajú rôzne systémy ohlasovania a vnútroštátne námorné jednotné kontaktné miesta sa implementujú pomocou rôznych technológií, modul rozhrania na ohlasovanie by mal byť založený na technológiách, ktoré umožňujú výmenu informácií medzi rôznymi informačnými systémami, ktoré používajú štandardizovaný protokol, čo umožňuje väčšiu interoperabilitu.

(4) V rámci ohlasovacích povinností uvedených v prílohe k nariadeniu (EÚ) 2019/1239 možno od deklarantov vyžadovať predloženie osobných údajov prostredníctvom modulu rozhrania na ohlasovanie, pri ktorom by sa mali vymieňať informácie tak, aby sa akékoľvek osobné údaje spracúvali v súlade s nariadeniami Európskeho parlamentu a Rady (EÚ) 2018/1725 ([2]) a (EÚ) 2016/679 ([3]).

(5) Keďže modul rozhrania na ohlasovanie vyvíja a aktualizuje Komisia a distribuuje ho členským štátom na účely integrácie, distribúcia nových verzií modulu rozhrania na ohlasovanie, monitorovanie správnej inštalácie softvéru a aktualizácia vykonávacej príručky pre správy by sa mali riadiť centrálne, pričom vždy, keď je to možné, by sa mali zohľadniť požiadavky na IT bezpečnosť vnútroštátnych námorných jednotných kontaktných miest.

(6) Na zaručenie stability, bezpečnosti a výkonnosti modulu rozhrania na ohlasovanie by mali byť členské štáty schopné monitorovať sieťovú prevádzku a analyzovať systémové udalosti, chyby a výnimky, ako aj integrovať tieto informácie do svojich existujúcich monitorovacích systémov a procesov. Na dosiahnutie tohto cieľa by modul rozhrania na ohlasovanie mal poskytovať vhodné funkcie, ktoré umožňujú zaznamenávanie a ukladanie udalostí a poskytovanie informácií o sieťovej prevádzke členským štátom.

([1]) Ú. v. EÚ L 198, 25.7.2019, s. 64.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

(7) Na zaistenie bezpečnej výmeny informácií prostredníctvom modulu rozhrania na ohlasovanie odosielatelia vyžadujú autentifikáciu. Na tento účel by spoločný systém správy registra používateľov a riadenia prístupu mal mať ako kľúčové komponenty centrálnu autentifikačnú službu a centrálny register. Tieto komponenty by mali spolupracovať, aby umožnili autentifikáciu odosielateľa naprieč všetkými modulmi rozhrania na ohlasovanie, čím by sa poskytol jednotný mechanizmus autentifikácie.

(8) Na bezpečnú výmenu informácií pomocou modulu rozhrania na ohlasovanie a na zabezpečenie rozpoznania používateľov na úrovni EÚ pri prístupe k niektorému z modulov rozhrania na ohlasovanie by odosielatelia mali získať kvalifikovaný certifikát pre elektronické pečate v súlade s požiadavkami stanovenými v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([4]).

(9) S cieľom zabezpečiť jednotnú registráciu pre odosielateľov na výmenu informácií prostredníctvom harmonizovaných rozhraní na ohlasovanie v rôznych členských štátoch by členské štáty mali mať možnosť registrovať odosielateľov v centrálnom registri. Tým by sa malo znížiť zaťaženie spôsobené viacnásobnými registráciami pre cezhraničné operácie vo viacerých vnútroštátnych námorných jednotných kontaktných miestach. Všetky osobné údaje v centrálnom registri by sa mali spravovať v súlade s nariadením (EÚ) 2018/1725 a nariadením (EÚ) 2016/679.

(10) Na minimalizovanie odkázanosti členských štátov na centrálne služby a vzhľadom na to, že vnútroštátne námorné jednotné kontaktné miesta už môžu byť podporované národnými autentifikačnými službami, členské štáty by mali mať takisto možnosť opätovne použiť svoje vlastné národné autentifikačné služby a národné registre na autentifikáciu odosielateľov, ktorí chcú používať modul rozhrania na ohlasovanie, ako alternatívu k systému správy registra používateľov a riadenia prístupu k európskemu prostrediu jednotnej námornej platformy (EMSWe).

(11) Toto nariadenie by sa malo uplatňovať od rovnakého dátumu ako nariadenie (EÚ) 2019/1239, aby sa členským štátom umožnilo správne integrovať modul rozhrania na ohlasovanie a systém správy registra používateľov a riadenia prístupu s vnútroštátnymi námornými jednotnými kontaktnými miestami.

(12) V súlade s článkom 42 ods. 1 nariadenia (EÚ) 2018/1725 sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý 18. októbra 2023 vydal stanovisko,

PRIJALA TOTO NARIADENIE:

Článok 1

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „modul rozhrania na ohlasovanie“ je midlvér vo vnútroštátnom námornom jednotnom kontaktnom mieste uvedený v článku 2 bode 4 nariadenia (EÚ) 2019/1239;

2. „odosielateľ“ je deklarant alebo poskytovateľ dátových služieb prevádzkujúci IT systém, ktorým sa posielajú elektronické správy vnútroštátnemu námornému jednotnému kontaktnému miestu alebo sa prijímajú prostredníctvom modulu rozhrania na ohlasovanie;

3. „formalita“ je formalita vymedzená v článku 1 vykonávacieho nariadenia Komisie (EÚ) 2023/204 ([5]);

4. „AS4“ je protokol pre správy založený na webových službách na bezpečnú výmenu správ medzi dvoma stranami;

5. „správa“ je digitálna reprezentácia formalít alebo správ s odpoveďou používaná na výmenu medzi odosielateľom a vnútroštátnym námorným jednotným kontaktným miestom;

6. „prístupový bod AS4“ je operačný softvér servera, ktorý je kompatibilný s protokolom zasielania správ AS4 a požiadavkami modulu rozhrania na ohlasovanie, ktorý umožňuje odosielanie a prijímanie informácií v mene odosielateľa z modulu rozhrania na ohlasovanie a doň;

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

([5]) Vykonávacie nariadenie Komisie (EÚ) 2023/204 z 28. októbra 2022, ktorým sa stanovujú technické špecifikácie, normy a postupy na zriadenie európskeho prostredia jednotnej námornej platformy podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1239 (Ú. v. EÚ L 33, 3.2.2023, s. 1).

7. „jadro vnútroštátneho námorného jednotného kontaktného miesta“ je technický komponent vnútroštátneho námorného jednotného kontaktného miesta, s ktorým je integrovaný modul rozhrania na ohlasovanie;

8. „kontrola syntaxe“ je proces overenia, či elektronická správa neobsahuje programové, štrukturálne alebo štylistické chyby;

9. „sémantická kontrola“ je proces, pri ktorom sa overuje zhoda údajov s konkrétnymi pravidlami pre údaje v rámci formality;

10. „vykonávacia príručka pre správy“ je funkčná špecifikácia stanovujúca normy a správy, ktoré si majú odosielatelia a vnútroštátne námorné jednotné kontaktné miesta vymieňať prostredníctvom modulu rozhrania na ohlasovanie;

11. „registrácia“ je proces, pri ktorom sa fyzická alebo právnická osoba identifikuje a vytvorí si účet v rámci orgánu uvedeného v článku 12 ods. 2 nariadenia (EÚ) 2019/1239;

12. „identifikácia“ je elektronická identifikácia vymedzená v článku 3 bode 1 nariadenia (EÚ) č. 910/2014;

13. „elektronická identifikácia“ je elektronická identifikácia vymedzená v článku 3 bode 2 nariadenia (EÚ) č. 910/2014;

14. „autentifikácia“ je autentifikácia vymedzená v článku 3 bode 5 nariadenia (EÚ) č. 910/2014;

15. „certifikát“ je kvalifikovaný certifikát pre elektronickú pečať vymedzený v článku 3 bode 30 nariadenia (EÚ) č. 910/2014 vydaný kvalifikovaným poskytovateľom dôveryhodných služieb vymedzeným v článku 3 bode 20 nariadenia (EÚ) č. 910/2014;

16. „číslo EORI“ je identifikačné číslo vymedzené v článku 1 bode 18 delegovaného nariadenia Komisie (EÚ) 2015/2446 ([6]);

17. „systém správy registra používateľov a riadenia prístupu k EMSWe“ je systém prevádzkovaný Komisiou, ktorý zahŕňa centrálny register a centrálnu autentifikačnú službu a zabezpečuje vzájomné uznávanie prostriedkov elektronickej identifikácie a autentifikácie na bezpečnú cezhraničnú výmenu údajov medzi odosielateľmi a vnútroštátnymi námornými jednotnými kontaktnými miestami prostredníctvom modulu rozhrania na ohlasovanie;

18. „centrálny register“ je register prevádzkovaný Komisiou, v ktorom sa uchovávajú registračné údaje odosielateľov poskytnuté členskými štátmi s cieľom uľahčiť autentifikáciu odosielateľov;

19. „národný register“ je register prevádzkovaný členským štátom, v ktorom sa uchovávajú registračné údaje odosielateľov a ktorý možno použiť na uľahčenie autentifikácie odosielateľov, ak je v súlade s požiadavkami centrálnej autentifikačnej služby;

20. „centrálna autentifikačná služba“ je služba prevádzkovaná Komisiou, ktorá overuje odosielateľov, ktorí používajú modul rozhrania na ohlasovanie;

21. „národná autentifikačná služba“ je služba prevádzkovaná členským štátom, ktorú možno použiť na autentifikáciu odosielateľov, ktorí používajú modul rozhrania na ohlasovanie.

Článok 2

Modul rozhrania na ohlasovanie musí spĺňať funkčné a technické špecifikácie uvedené v časti I prílohy.

S cieľom pomôcť integrovať modul rozhrania na ohlasovanie do vnútroštátneho námorného jednotného kontaktného miesta Komisia v úzkej spolupráci s vnútroštátnymi koordinátormi pre EMSWe:

— vymedzí usmernenia na testovanie a konfiguráciu modulu rozhrania na ohlasovanie v záujme integrácie do príslušných vnútroštátnych námorných jednotných kontaktných miest,

— s pomocou Európskej námornej bezpečnostnej agentúry vymedzí a bude spravovať vykonávaciu príručku pre správy.

([6]) Delegované nariadenie Komisie (EÚ) 2015/2446 z 28. júla 2015, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 952/2013, pokiaľ ide o podrobné pravidlá, ktorými sa bližšie určujú niektoré ustanovenia Colného kódexu Únie (Ú. v. EÚ L 343, 29.12.2015, s. 1).

Článok 3

Centrálny register a centrálna autentifikačná služba sa zriadia v súlade s technickými špecifikáciami, normami a postupmi uvedenými v časti II prílohy.

Článok 4

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od 15. augusta 2025.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 14. decembra 2023

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA

ČASŤ I

MODUL ROZHRANIA NA OHLASOVANIE

ARCHITEKTÚRA A ROZSAH

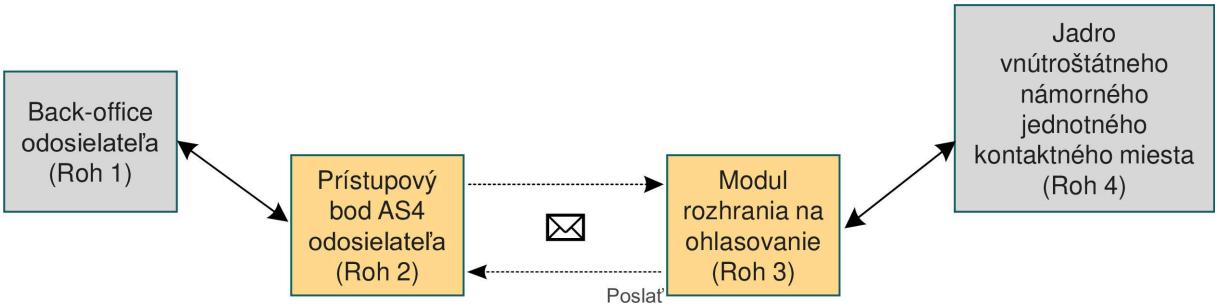
Modul rozhrania na ohlasovanie je súčasťou modelu štyroch rohov pre správy vymieňané medzi odosielateľmi (roh 1) a jadrom vnútroštátneho námorného jednotného kontaktného miesta (roh 4) prenášané cez prístupové body AS4 (rohy 2 a 3) na každej strane vykonávajúcej protokol AS4 na prenos a bezpečnosť takto:

Roh 1: back-office odosielateľa pripravuje, odosiela a prijíma správy z jadra vnútroštátneho námorného jednotného kontaktného miesta a doň;

Roh 2: prístupový bod AS4 odosielateľa;

Roh 3: modul rozhrania na ohlasovanie;

Roh 4: jadro vnútroštátneho námorného jednotného kontaktného miesta prijíma správy odosielateľa a odpovedá na ne.



Obrázok 1 – Architektúra modulu rozhrania na ohlasovanie na vysokej úrovni

Modul rozhrania na ohlasovanie nevykonáva sémantickú kontrolu správ nad rámec špecifikácií vykonávacej príručky pre správy, nespracováva ich poradie ani neuchováva správy dlhšie, než je čas potrebný na to, aby boli úspešne prenesené do jadra vnútroštátneho námorného jednotného kontaktného miesta alebo odosielateľovi.

V súlade s článkom 5 ods. 3 písm. c) nariadenia (EÚ) 2019/1239 členské štáty po prenose správy z modulu rozhrania na ohlasovanie do jadra vnútroštátneho námorného jednotného kontaktného miesta v prípade potreby preložia, overia a prenesú údaje formality do systémov príslušných orgánov v súlade so špecifikáciami týchto systémov.

FUNKČNÉ ŠPECIFIKÁCIE MODULU ROZHRANIA NA OHLASOVANIE

ID	Funkcia	Opis
LR1	Zaznamenávanie a monitorovanie	Funkcia zabezpečuje zaznamenávanie a ukladanie udalostí (chyby doručenia, oneskorenia a chyba príjemcu).
LR2	Ukladanie metaúdajov	Funkcia zabezpečuje uchovávanie metaúdajov vymieňaných správ.
OA1	Ukladanie a vyhľadávanie technických údajov	Funkcia zabezpečuje ukladanie a vyhľadávanie technických údajov potrebných na konfiguráciu a fungovanie modulu rozhrania na ohlasovanie cez rozhranie (napr. technické adresy prístupových bodov AS4 odosielateľov, schémy správ vo vykonávacej príručke pre správy atď.).
OA2	Spracovanie výnimiek	Funkcia poskytuje oznámenia o zistených chybách spracovania a/alebo anomálnych podmienkach prostredníctvom používateľského rozhrania.
OA3	Prístup k zaznamenávaniu a monitorovaniu informácií a metaúdajov	Funkcia poskytuje jadru vnútroštátneho námorného jednotného kontaktného miesta prístup k zaznamenávaniu a monitorovaniu informácií a metaúdajov vymieňaných správ prostredníctvom rozhrania medzi systémami.

OA4	Autentifikácia odosielateľa	Funkcia spúšťa proces autentifikácie odosielateľa pomocou centrálnej alebo národnej autentifikačnej služby.
OA5	Kontrola správy	Funkcia vykoná kontrolu syntaxe a sémantickú kontrolu prijatých správ v súlade s technickými špecifikáciami správ vymedzenými vo vykonávacej príručke pre správy. Vo vykonávacej príručke pre správy sa špecifikuje, ktoré kontroly vykoná modul rozhrania na ohlasovanie. Modul rozhrania na ohlasovanie zodpovedajúcim spôsobom oznámi chyby.
MF1	Spracovanie správ	Funkcia zabezpečuje, aby sa obsah prijatých správ (formalita alebo odpoveď) preniesol bez úprav do príslušného rohu, ak boli kontroly úspešné.

TECHNICKÉ ŠPECIFIKÁCIE MODULU ROZHRANIA NA OHLASOVANIE

Integrácia

ID	Názov	Opis
IA1.	Štandard protokolu zasielania správ	Modul rozhrania na ohlasovanie používa protokol zasielania správ AS4 na uľahčenie interoperability s rôznymi technológiami a systémami ohlasovania odosielateľov.

Výmena správ

ID	Názov	Opis
AP1.	Model asynchrónnej výmeny správ	Modul rozhrania na ohlasovanie podporuje asynchrónny prenos správ do jadra vnútroštátneho námorného jednotného kontaktného miesta (formalita) a z neho (odpoveď) mechanizmom „push and pull“.

Zabezpečenie

ID	Názov	Opis
SA1.	Dôvernosť a bezpečnosť výmeny informácií	Modul rozhrania na ohlasovanie zabezpečuje dôvernosť informácií a ochranu všetkých vymieňaných osobných údajov šifrovaním informácií vymieňaných medzi prístupovým bodom AS4 odosielateľa a modulom rozhrania na ohlasovanie. Modul rozhrania na ohlasovanie dešifruje a sprístupní správy zaslané odosielateľom jadru vnútroštátneho námorného jednotného kontaktného miesta. Modul rozhrania na ohlasovanie štandardne využíva zabezpečenie webových služieb (WSS) na umožnenie bezpečnej výmeny správ medzi prístupovým bodom AS4 odosielateľa a modulom rozhrania na ohlasovanie.
SA2.	Neodmietanie správ	Komunikácia a kontrola správ prostredníctvom modulu rozhrania na ohlasovanie zahŕňa bezpečnostné opatrenia na zaistenie pravosti správ a zabránenie ich odmietaniu.

SA3.	Integrita	Zavedú sa technické opatrenia na zabezpečenie integrity vymieňaných údajov.
SA4.	Zabezpečenie aplikácie	Modul rozhrania na ohlasovanie bude vychádzať z najlepších postupov vývoja softvéru, ktoré umožňujú zisťovanie škodlivých činností a bezpečný prenos citlivých informácií.
SA5.	Dostupnosť služby	V záujme spoľahlivej komunikácie a distribúcie informácií medzi odosielateľmi a vnútroštátnymi námornými jednotnými kontaktnými miestami zavedie modul rozhrania na ohlasovanie mechanizmy, ktoré zabezpečia, aby sa správy vymieňané s modulom rozhrania na ohlasovanie nestratili v prípade nedostupnosti služby.

Výkon a škálovateľnosť

ID	Názov	Opis
PS1.	Výkon a škálovateľnosť	Modul rozhrania na ohlasovanie musí byť schopný splniť existujúce a budúce výkonnostné ciele, ako je čas odozvy, počet súbežných odosielateľov a množstvo/veľkosť vymieňaných správ.

Prenosnosť a nasadenie

ID	Názov	Opis
PD1.	Nezávislosť platformy	Modul rozhrania na ohlasovanie musí byť kompatibilný s najbežnejšou hardvérovou architektúrou a operačnými systémami, v ktorých bude nasadený. Modul rozhrania na ohlasovanie by na inštaláciu alebo konfiguráciu nemal vyžadovať vlastný hardvér ani softvér.
PD2.	Samoinštalačná aplikácia	Modul rozhrania na ohlasovanie sa poskytuje ako balík softvéru, ktorý obsahuje všetky aplikačné komponenty požadované týmto modulom. Poskytnuté a požadované závislosti sú uvedené v každej poznámke k vydaniu modulu rozhrania na ohlasovanie.

ČASŤ II

SYSTÉM SPRÁVY REGISTRA POUŽÍVATEĽOV A RIADENIA PRÍSTUPU K EMSWE

CENTRÁLNY REGISTER

Na žiadosť odosielateľa členské štáty, ktoré neposkytujú národný register v súlade so špecifikáciami centrálneho registra stanovenými v tejto prílohe, zaregistrujú číslo EORI a certifikát odosielateľa v centrálnom registri a sú zodpovedné za overenie, presnosť a riadenie údajov v súlade s článkom 12 ods. 2 nariadenia (EÚ) 2019/1239. Centrálny register poskytuje členským štátom rozhranie na vykonávanie registrácie a správy odosielateľov.

CENTRÁLNA AUTENTIFIKAČNÁ SLUŽBA

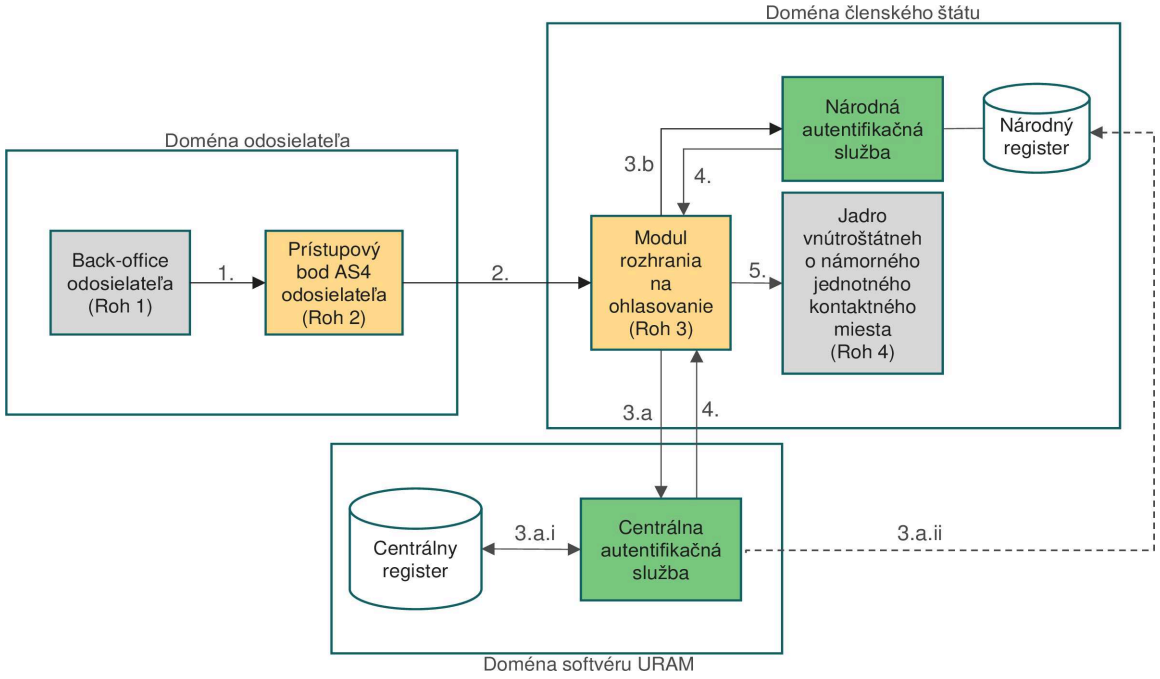
Diagram uvedený ďalej znázorňuje postupné kroky na autentifikáciu odosielateľa, ktorý pripravuje a odosiela správu do modulu rozhrania na ohlasovanie (krok 1, 2).

Modul rozhrania na ohlasovanie vykoná funkciu „autentifikácie odosielateľa“ ([1]) pomocou centrálnej autentifikačnej služby (krok 3.a).

Krok 3.a: Centrálna autentifikačná služba overí odosielateľa dotazom v centrálnom registri a skontrolovaním príslušného záznamu (3.a.i) alebo, ak odosielateľ nie je prítomný v centrálnom registri, dotazom v národnom registri krajiny odosielateľa, ak je dostupný, a skontrolovaním príslušného záznamu (krok 3.a.ii).

Krok 3.b: Ak je v členskom štáte zriadená a sprístupnená národná autentifikačná služba, modul rozhrania na ohlasovanie vykoná funkciu „autentifikácie odosielateľa“ pomocou tejto národnej autentifikačnej služby len na autentifikáciu odosielateľov pomocou certifikátu vydaného v tomto členskom štáte.

Krok 4: Výsledok autentifikácie sa zašle späť do modulu rozhrania na ohlasovanie. V prípade úspešnej autentifikácie sa správa sprístupní rohu 4 (jadro vnútroštátneho námorného jednotného kontaktného miesta) (krok 5). V prípade neúspešnej autentifikácie sa správa o zlyhaní odošle späť do rohu 2.



Obrázok 2

TECHNICKÉ ŠPECIFIKÁCIE URAM

Integrácia

ID	Názov	Opis
URAM.01	Interoperabilné štandardy	Softvér URAM musí dodržiavať štandardné protokoly a využívať spoľahlivé bezpečnostné prvky pri odhaľovaní svojich rozhraní a integrácii s inými komponentmi.

([1]) Identifikované ako OA4 v oddiele funkčných špecifikácií modulu rozhrania na ohlasovanie v časti I tejto prílohy.

URAM.02	Súlad s eIDAS	Softvér URAM využíva otvorené štandardy a riešenia EÚ a implementuje potrebné kontrolné mechanizmy na kontrolu certifikátov odosielateľa v porovnaní s dôveryhodnými zoznamami uverejnenými členskými štátmi v súlade s článkom 22 nariadenia (EÚ) č. 910/2014 a vykonávacím rozhodnutím Komisie (EÚ) 2015/1505 ([2]) vrátane informácií týkajúcich sa kvalifikovaných poskytovateľov dôveryhodných služieb vydávajúcich certifikáty používané na elektronické pečate.

Zabezpečenie

ID	Názov	Opis
URAM.03	Dôvernosť výmeny informácií	Na zaistenie bezpečnosti softvéru URAM a výmeny akýchkoľvek osobných údajov sa zavedú tieto protokoly a metódy šifrovania: — Zabezpečenie prenosovej vrstvy (TLS): celý softvér URAM musí byť zabezpečený pomocou protokolu TLS, aby sa zabezpečilo šifrovanie na úrovni siete a integrita údajov s cieľom pomôcť chrániť údaje počas prenosu a zabrániť neoprávnenému prístupu alebo manipulácii. — Na komunikáciu so softvérom URAM sa musí implementovať konfigurácia protokolu TLS.
URAM.04	Zabezpečenie aplikácie	Softvér URAM zaručuje zisťovanie škodlivých činností a bezpečný prenos citlivých informácií.
URAM 05	Ochrana osobných údajov	Prístupové práva sa udeľujú orgánom členských štátov podľa článku 12 ods. 2 nariadenia (EÚ) 2019/1239 na účely registrácie odosielateľov. Softvér URAM musí implementovať mechanizmy kontroly prístupu na zabezpečenie ochrany informácií používateľa, teda osobných údajov, ktoré sa spracúvajú výhradne na účel vytvárania používateľských účtov a riadenia zodpovedajúcich prístupových práv. Centrálna autentifikačná služba uchováva osobné údaje odosielateľov len tak dlho, ako je potrebné na účely autentifikácie. Centrálny register uchováva osobné údaje odosielateľov len tak dlho, ako je potrebné na správu účtu.

Udržateľnosť a prenosnosť

ID	Názov	Opis
URAM.06	Nezávislosť technológií	Softvér URAM umožňuje interakcie s modulom rozhrania na ohlasovanie a inými relevantnými službami bez potreby vlastného softvéru alebo hardvéru a umožňuje integráciu s modulom rozhrania na ohlasovanie bez ohľadu na technologické prostredie, v ktorom je modul rozhrania na ohlasovanie nasadený.

([2]) Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9.9.2015, s. 26).

URAM.07	Nezávislé nasadenie	Softvér URAM nepresadzuje špecifické požiadavky na nasadenie modulu rozhrania na ohlasovanie. Modul rozhrania na ohlasovanie by mal zabezpečiť iba internetové pripojenie a rešpektovanie noriem týkajúcich sa zabezpečenia a protokolov softvéru URAM.

Funkcie centrálnej autentifikačnej služby

Modulu rozhrania na ohlasovanie sa z centrálnej autentifikačnej služby sprístupnia tieto služby.

ID	Názov	Opis
URAM.08	Služba autentifikácie	Centrálna autentifikačná služba je zodpovedná za autentifikáciu odosielateľov overením platnosti certifikátu, čísla EORI a asociácie medzi číslom EORI odosielateľa a jeho certifikátom. Spracováva žiadosti o autentifikáciu zaslané modulom rozhrania na ohlasovanie a poskytuje odpovede označujúce úspešnú alebo neúspešnú autentifikáciu.

Špecifikácie centrálneho registra

ID	Názov	Opis
URAM.09	Registrácia odosielateľa	Centrálny register poskytuje členským štátom grafické používateľské rozhranie na registráciu údajov odosielateľa. Po zaregistrovaní v centrálnom registri sa odosielateľ zaregistruje vo všetkých členských štátoch.
URAM.10	Zobrazenie a vyhľadávanie odosielateľa	Centrálny register umožňuje členskému štátu prezerať si všetky údaje o odosielateľoch, ktoré predtým zaregistroval. Poskytuje aj funkciu vyhľadávania na získanie údajov svojich registrovaných odosielateľov na základe rôznych kritérií vyhľadávania.
URAM.11	Aktualizácia odosielateľa	Centrálny register umožňuje členskému štátu upraviť všetky údaje svojich predtým zaregistrovaných odosielateľov na zabezpečenie presnosti a platnosti údajov.
URAM.12	Deaktivácia odosielateľa	Centrálny register umožňuje členskému štátu deaktivovať svojich predtým zaregistrovaných odosielateľov.
URAM.13	Audit a ohlasovanie	Centrálny register ponúka spôsobilosti ohlasovania, ktoré umožňujú členskému štátu analyzovať konkrétne údaje svojich predtým zaregistrovaných odosielateľov, ako je dátum registrácie a platnosť certifikátu.
URAM.14	Oznámenia	Centrálny register ponúka členským štátom možnosť dostať oznámenie z centrálneho registra vždy, keď sa odosielateľ, ktorý bol predtým zaregistrovaný týmto členským štátom, zaregistruje, aktualizuje alebo deaktivuje, ako aj po skončení platnosti certifikátu.