2023/2790

18.12.2023

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2023/2790

ze dne 14. prosince 2023,

kterým se stanoví funkční a technické specifikace pro modul rozhraní pro podávání zpráv v rámci vnitrostátních jednotných námořních portálů

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2019/1239 ze dne 20. června 2019, kterým se zřizuje evropské prostředí jednotného námořního portálu a zrušuje směrnice 2010/65/EU ([1]), a zejména na čl. 6 odst. 1 a čl. 12 odst. 4 uvedeného nařízení,

po konzultaci s Výborem pro usnadňování digitální dopravy a obchodu,

vzhledem k těmto důvodům:

(1) Specifikace modulu rozhraní pro podávání zpráv by měly být založeny na technologii, která je snadno dostupná, snadno instalovatelná a snadno integrovatelná do všech vnitrostátních jednotných námořních portálů, a měly by v budoucnu umožňovat bezproblémovou integraci a údržbu.

(2) Funkční a technické specifikace modulu rozhraní pro podávání zpráv by měly být založeny na pokynech k návrhu šablony pro architekturu řešení požadavků interoperability na vysoké úrovni, aby byla umožněna sledovatelnost mezi požadavky na interoperabilitu na vysoké úrovni a podrobnými požadavky na interoperabilitu.

(3) Vzhledem k tomu, že odesílatelé používají různé systémy podávání zpráv a že vnitrostátní jednotné námořní portály jsou zaváděny pomocí různých technologií, měl by být modul rozhraní pro podávání zpráv založen na technologiích, které umožňují výměnu informací mezi různými informačními systémy, jež používají standardizovaný protokol, což umožní větší interoperabilitu.

(4) Oznamovací povinnosti uvedené v příloze nařízení (EU) 2019/1239 mohou od deklarantů vyžadovat, aby poskytovali prostřednictvím modulu rozhraní pro podávání zpráv osobní údaje; tento modul by měl vyměňovat informace tak, aby byly veškeré osobní údaje zpracovávány v souladu s nařízeními Evropského parlamentu a Rady (EU) 2018/1725 ([2]) a (EU) 2016/679 ([3]).

(5) Vzhledem k tomu, že modul rozhraní pro podávání zpráv vyvíjí a aktualizuje Komise a distribuuje ho členským státům za účelem integrace, distribuce nových verzí modulu rozhraní pro podávání zpráv, monitorování správné instalace softwaru a aktualizace pokynů pro výměnu zpráv by měly být řízeny centrálně, a to pokud možno s přihlédnutím k požadavkům vnitrostátních jednotných námořních portálů na bezpečnost IT.

(6) Aby byla zaručena stabilita, bezpečnost a výkonnost modulu rozhraní pro podávání zpráv, měly by mít členské státy možnost monitorovat síťový provoz a analyzovat systémové události, chyby a výjimky a začlenit tyto informace do svých stávajících monitorovacích systémů a procesů. Za tímto účelem by modul rozhraní pro podávání zpráv měl poskytovat vhodné funkce, které umožní zaznamenávat a ukládat události a poskytovat členským státům informace o síťovém provozu.

([1]) Úř. věst. L 198, 25.7.2019, s. 64.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

([3]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

(7) K zajištění bezpečné výměny informací prostřednictvím modulu rozhraní pro podávání zpráv potřebují odesílatelé autentizaci. Za tímto účelem by společný systém registrace uživatelů a správy přístupu měl mít jako klíčové prvky centrální autentizační službu a centrální registr. Tyto složky by měly spolupracovat, aby umožnily autentizaci odesílatele ve všech modulech rozhraní pro podávání zpráv a zajistily jednotný mechanismus autentizace.

(8) Za účelem bezpečné výměny informací pomocí modulu rozhraní pro podávání zpráv a zajištění toho, aby byli uživatelé rozpoznáni na úrovni EU při přístupu ke kterémukoli z modulů rozhraní pro podávání zpráv, by odesílatelé měli získat kvalifikovaný certifikát pro elektronické pečetě, který bude v souladu s požadavky stanovenými v nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([4]).

(9) Za účelem zajištění jediné registrace pro odesílatele k výměně informací prostřednictvím harmonizovaných rozhraní pro podávání zpráv v různých členských státech by členské státy měly mít možnost registrovat odesílatele v centrálním registru. To by mělo snížit zátěž spojenou s vícenásobnými registracemi u přeshraničních operací ve více vnitrostátních jednotných námořních portálech. Veškeré osobní údaje v centrálním registru by měly být spravovány v souladu s nařízeními (EU) 2018/1725 a (EU) 2016/679.

(10) Aby se minimalizovala závislost členských států na centrálních službách a vzhledem k tomu, že vnitrostátní jednotné námořní portály již mohou mít podporu vnitrostátních autentizačních služeb, měly by mít členské státy rovněž možnost opětovně použít své vlastní vnitrostátní autentizační služby a vnitrostátní registry k ověření odesílatelů, kteří chtějí používat modul rozhraní pro podávání zpráv, jako alternativu k systému registrace uživatelů a správy přístupu k evropskému prostředí jednotného námořního portálu.

(11) Aby mohly členské státy správně integrovat modul rozhraní pro podávání zpráv a systém registrace uživatelů a správy přístupu s vnitrostátními jednotnými námořními portály, mělo by se toto nařízení použít od stejného data jako nařízení (EU) 2019/1239.

(12) V souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 18. října 2023,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Definice

Pro účely tohoto nařízení se rozumí:

1) „modulem rozhraní pro podávání zpráv“ middlewarová součást vnitrostátního jednotného námořního portálu uvedená v čl. 2 bodě 4 nařízení (EU) 2019/1239;

2) „odesílatelem“ deklarant nebo poskytovatel datových služeb provozující IT systém, který odesílá elektronické zprávy do vnitrostátního jednotného námořního portálu nebo je přijímá prostřednictvím modulu rozhraní pro podávání zpráv;

3) „formalitou“ formalita ve smyslu článku 1 prováděcího nařízení Komise (EU) 2023/204 ([5]);

4) „AS4“ protokol zpráv založený na on-line službách pro bezpečnou výměnu zpráv mezi dvěma stranami;

5) „zprávou“ digitální znázornění formalit nebo zpráv s odpovědí používaných pro komunikaci mezi odesílatelem a vnitrostátním jednotným námořním portálem;

6) „přístupovým bodem AS4“ operační software serveru, jenž je kompatibilní s protokolem podávání zpráv AS4 a požadavky na modul rozhraní pro podávání zpráv a který umožňuje odesílat a přijímat informace jménem odesílatele z modulu rozhraní pro podávání zpráv a do něj;

([4]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73).

([5]) Prováděcí nařízení Komise (EU) 2023/204 ze dne 28. října 2022, kterým se stanoví technické specifikace, normy a postupy pro evropské prostředí jednotného námořního portálu podle nařízení Evropského parlamentu a Rady (EU) 2019/1239 (Úř. věst. L 33, 3.2.2023, s. 1).

7) „jádrem vnitrostátního jednotného námořního portálu“ technická součást vnitrostátního jednotného námořního portálu, s níž je modul rozhraní pro podávání zpráv integrován;

8) „syntaktickým ověřením“ proces kontroly, zda elektronická zpráva neobsahuje programovací, strukturální nebo stylistické chyby;

9) „sémantickým ověřením“ proces, při němž je kontrolována shoda údajů se zvláštními pravidly pro údaje v rámci formality;

10) „pokyny pro výměnu zpráv“ funkční specifikace, která stanoví standardy a zprávy, jež mají být vyměňovány mezi odesílateli a vnitrostátními jednotnými námořními portály prostřednictvím modulu rozhraní pro podávání zpráv;

11) „registrací“ postup, při němž se fyzická nebo právnická osoba identifikuje a vytvoří si účet u orgánu uvedeného v čl. 12 odst. 2 nařízení (EU) 2019/1239;

12) „identifikací“ elektronická identifikace ve smyslu čl. 3 bodu 1 nařízení (EU) č. 910/2014;

13) „prostředkem pro elektronickou identifikaci“ elektronická identifikace ve smyslu čl. 3 bodu 2 nařízení (EU) č. 910/2014;

14) „autentizací“ autentizace definovaná v čl. 3 bodě 5 nařízení (EU) č. 910/2014;

15) „certifikátem“ kvalifikovaný certifikát pro elektronickou pečeť ve smyslu čl. 3 bodu 30 nařízení (EU) č. 910/2014 vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru ve smyslu čl. 3 bodu 20 nařízení (EU) č. 910/2014;

16) „číslem EORI“ elektronické identifikační číslo ve smyslu čl. 1 bodu 18 nařízení Komise v přenesené pravomoci (EU) 2015/2446 ([6]);

17) „systémem registrace uživatelů a správy přístupu k evropskému prostředí jednotného námořního portálu“ systém provozovaný Komisí, který zahrnuje centrální registr a centrální autentizační službu a zajišťuje vzájemné uznávání prostředků pro elektronickou identifikaci a autentizace pro bezpečnou přeshraniční výměnu údajů mezi odesílateli a vnitrostátními jednotnými námořními portály prostřednictvím modulu rozhraní pro podávání zpráv;

18) „centrálním registrem“ registr provozovaný Komisí, který obsahuje registrační údaje odesílatelů poskytnuté členskými státy pro usnadnění autentizace odesílatelů;

19) „vnitrostátním registrem“ registr provozovaný členským státem, který obsahuje registrační údaje odesílatelů a může být použit k usnadnění autentizace odesílatelů, pokud je v souladu s požadavky centrální autentizační služby;

20) „centrální autentizační službou“ služba provozovaná Komisí, jež autentizuje odesílatele, kteří používají modul rozhraní pro podávání zpráv;

21) „vnitrostátní autentizační službou“ služba provozovaná členským státem, jež může být použita k autentizaci odesílatelů, kteří používají modul rozhraní pro podávání zpráv.

Článek 2

Modul rozhraní pro podávání zpráv musí být v souladu s funkčními a technickými specifikacemi stanovenými v části I přílohy.

S cílem pomoci začlenit modul rozhraní pro podávání zpráv do vnitrostátních jednotných námořních portálů provádí Komise v úzké spolupráci s národními koordinátory evropského prostředí jednotného námořního portálu tyto činnosti:

— vypracovává pokyny pro testování a konfiguraci modulu rozhraní pro podávání zpráv za účelem integrace do příslušných vnitrostátních jednotných námořních portálů,

— vypracovává a spravuje, s pomocí Evropské agentury pro námořní bezpečnost, pokyny pro výměnu zpráv.

([6]) Nařízení Komise v přenesené pravomoci (EU) 2015/2446 ze dne 28. července 2015, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 952/2013, pokud jde o podrobná pravidla k některým ustanovením celního kodexu Unie (Úř. věst. L 343, 29.12.2015, s. 1).

Článek 3

Centrální registr a centrální autentizační služba se zřídí v souladu s technickými specifikacemi, standardy a postupy stanovenými v části II přílohy.

Článek 4

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se ode dne 15. srpna 2025.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 14. prosince 2023.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

ČÁST I

MODUL ROZHRANÍ PRO PODÁVÁNÍ ZPRÁV

ARCHITEKTURA A OBLAST PŮSOBNOSTI

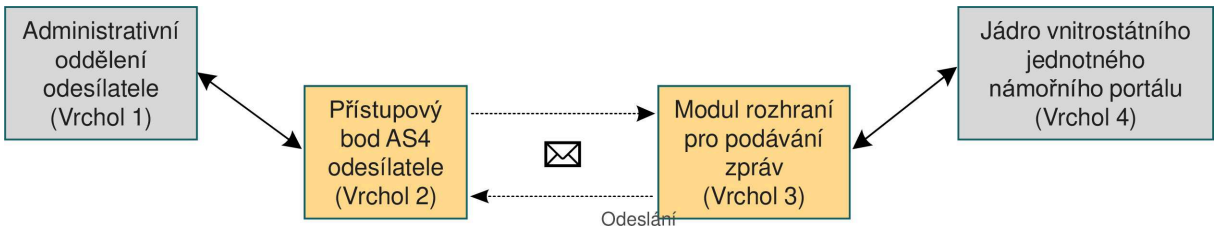
Modul rozhraní pro podávání zpráv je součástí čtyřvrcholového modelu pro zprávy vyměňované mezi odesílateli (vrchol 1) a jádrem vnitrostátního jednotného námořního portálu (vrchol 4) přenášené prostřednictvím přístupových bodů AS4 (vrcholy 2 a 3) na každé straně používajících protokol AS4 pro přenos a bezpečnost, a to tímto způsobem:

vrchol 1: administrativní oddělení odesílatele, které připravuje zprávy, odesílá je do jádra vnitrostátního jednotného námořního portálu a přijímá je z něj,

vrchol 2: přístupový bod AS4 odesílatele,

vrchol 3: modul rozhraní pro podávání zpráv,

vrchol 4: jádro vnitrostátního jednotného námořního portálu, které přijímá zprávy a zasílá zprávy s odpovědí odesílateli.



Obrázek 1 – Vysokoúrovňová architektura modulu rozhraní pro podávání zpráv

Modul rozhraní pro podávání zpráv nesmí provádět sémantické ověření zpráv nad rámec specifikací uvedených v pokynech pro výměnu zpráv, zpracovávat jejich posloupnost ani ukládat zprávy na dobu delší, než je jejich úspěšný přenos do jádra vnitrostátního jednotného námořního portálu nebo odesílateli.

V souladu s čl. 5 odst. 3 písm. c) nařízení (EU) 2019/1239, jakmile je zpráva převedena z modulu rozhraní pro podávání zpráv do jádra vnitrostátního jednotného námořního portálu, členské státy případně převedou údaje formality do systémů příslušných orgánů v souladu se specifikacemi těchto systémů.

FUNKČNÍ SPECIFIKACE MODULU ROZHRANÍ PRO PODÁVÁNÍ ZPRÁV

ID	Funkce	Popis
LR1	Zaznamenávání a monitorování	Funkce zajišťuje zaznamenávání a ukládání událostí (nedoručení, zpoždění a chyby příjemce).
LR2	Ukládání metadat	Funkce zajišťuje ukládání metadat vyměňovaných zpráv.
OA1	Ukládání a vyhledávání technických údajů	Funkce zajišťuje ukládání a vyhledávání technických údajů potřebných pro konfiguraci a fungování modulu rozhraní pro podávání zpráv prostřednictvím rozhraní (např. technické adresy přístupových bodů AS4 odesílatelů, schémata zpráv uvedená v pokynech výměnu zpráv atd.).
OA2	Řešení výjimek	Funkce poskytuje oznámení o zjištěných chybách při zpracování a/nebo neobvyklých podmínkách prostřednictvím uživatelského rozhraní.
OA3	Přístup k informacím o zaznamenávání a monitorování a k metadatům	Funkce poskytuje přístup jádra vnitrostátního jednotného námořního portálu k informacím o zaznamenávání a monitorování a k metadatům vyměňovaných zpráv prostřednictvím rozhraní mezi systémy.

OA4	Autentizace odesílatele	Funkce spustí proces autentizace odesílatele pomocí centrální nebo vnitrostátní autentizační služby.
OA5	Ověření zprávy	Funkce provádí syntaktické a sémantické ověření přijatých zpráv v souladu s technickými specifikacemi zpráv definovanými v pokynech pro výměnu zpráv. Pokyny pro výměnu zpráv uvádějí, která ověření musí být provedena prostřednictvím modulu rozhraní pro podávání zpráv. Modul rozhraní pro podávání zpráv podle toho oznámí chyby.
MF1	Zpracování zpráv	Funkce zajišťuje, aby byl obsah obdržených zpráv (formalita nebo odpověď) přenesen beze změn do příslušného vrcholu, pokud byla ověření úspěšná.

TECHNICKÉ SPECIFIKACE MODULU ROZHRANÍ PRO PODÁVÁNÍ ZPRÁV

Integrace

ID	Název	Popis
IA1.	Standard protokolu pro zasílání zpráv	Modul rozhraní pro podávání zpráv používá protokol pro zasílání zpráv AS4 k usnadnění interoperability s různými technologiemi a systémy odesílatelů pro podávání zpráv.

Výměna zpráv

ID	Název	Popis
AP1.	Schéma pro asynchronní výměnu zpráv	Modul rozhraní pro podávání zpráv musí podporovat asynchronní přenos zpráv (formality a odpovědi) do jádra vnitrostátního jednotného námořního portálu a z něj mechanismem push a pull.

Bezpečnost

ID	Název	Popis
SA1.	Důvěrnost a bezpečnost výměny informací	Modul rozhraní pro podávání zpráv zajišťuje důvěrnost informací a ochranu veškerých vyměňovaných osobních údajů zašifrováním vyměňovaných informací mezi přístupovým bodem AS4 odesílatele a modulem rozhraní pro podávání zpráv. Modul rozhraní pro podávání zpráv dešifruje zprávy odeslané odesílatelem a zpřístupní je jádru vnitrostátního jednotného námořního portálu. Modul rozhraní pro podávání zpráv používá jako standard Web Service Security (WSS), který umožňuje bezpečnou výměnu zpráv mezi přístupovým bodem AS4 odesílatele a modulem rozhraní pro podávání zpráv.
SA2.	Neodmítnutelnost zpráv	Přenos a ověření zpráv prostřednictvím modulu rozhraní pro podávání zpráv musí zahrnovat bezpečnostní opatření, která zajistí pravost zpráv a zabrání jejich odmítnutí.

SA3.	Integrita	Zavedou se technická opatření k zajištění integrity vyměňovaných údajů.
SA4.	Bezpečnost aplikací	Modul rozhraní pro podávání zpráv vychází z osvědčených postupů vývoje softwaru, které umožňují odhalit škodlivé činnosti a zajišťují bezpečný přenos citlivých informací.
SA5.	Dostupnost služby	Pro spolehlivou komunikaci a distribuci informací mezi odesílateli a vnitrostátními jednotnými námořními portály zavede modul rozhraní pro podávání zpráv mechanismy, které zajistí, aby zprávy vyměňované prostřednictvím tohoto modulu nebyly v případě nedostupnosti služby ztraceny.

Výkonnost a rozšiřitelnost

ID	Název	Popis
PS1.	Výkonnost a rozšiřitelnost	Modul rozhraní pro podávání zpráv musí být schopen splnit stávající a budoucí výkonnostní cíle, jako je doba odezvy, počet souběžných odesílatelů a množství/velikost vyměňovaných zpráv.

Přenositelnost a nasazení

ID	Název	Popis
PD1.	Nezávislost platformy	Modul rozhraní pro podávání zpráv musí být kompatibilní s nejběžnější architekturou hardwaru a operačními systémy, kde by se měl nasazovat. Modul rozhraní pro podávání zpráv by pro instalaci nebo konfiguraci neměl vyžadovat proprietární hardware nebo software.
PD2	Samoinstalační aplikace	Modul rozhraní pro podávání zpráv se poskytuje jako balík softwaru, jenž zahrnuje všechny součásti aplikace, které modul potřebuje. Poskytnuté a požadované závislosti musí být uvedeny poznámkách ke každé vydané verzi modulu.

ČÁST II

SYSTÉM REGISTRACE UŽIVATELŮ EVROPSKÉHO PROSTŘEDÍ JEDNOTNÉHO NÁMOŘNÍHO PORTÁLU A SPRÁVY PŘÍSTUPU K NĚMU

CENTRÁLNÍ REGISTR

Na žádost odesílatele zaregistrují členské státy, které nevedou vnitrostátní registr splňující specifikace centrálního registru stanovené v této příloze, číslo EORI a certifikát odesílatele v centrálním registru a odpovídají za ověření, přesnost a správu údajů v souladu s čl. 12 odst. 2 nařízení (EU) 2019/1239. Centrální registr poskytuje členským státům rozhraní pro registraci a správu odesílatelů.

CENTRÁLNÍ AUTENTIZAČNÍ SLUŽBA

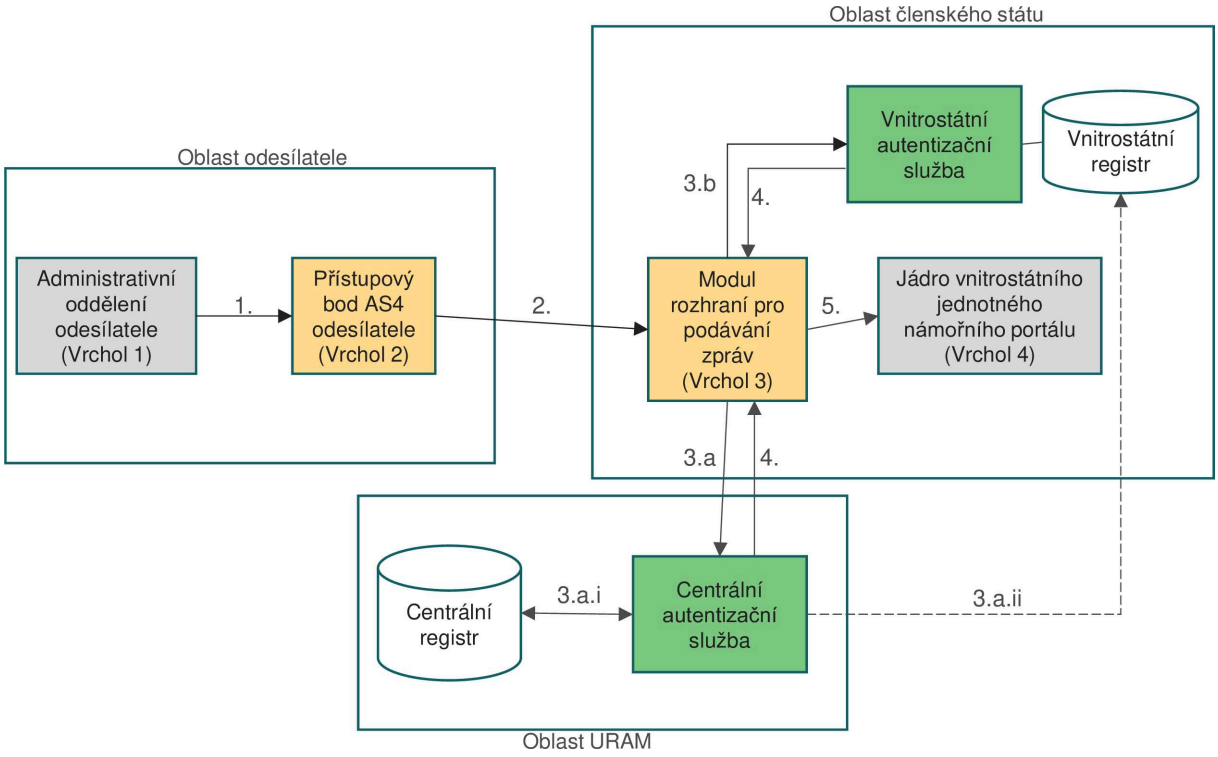
Níže uvedené schéma znázorňuje postupné kroky pro autentizaci odesílatele, který připraví a zašle zprávu do modulu rozhraní pro podávání zpráv (krok 1, 2).

Modul rozhraní pro podávání zpráv provede funkci „autentizace odesílatele“ ([1]) pomocí centrální autentizační služby (krok 3.a).

Krok 3.a: Centrální autentizační služba autentizuje odesílatele vyhledáním v centrálním registru a kontrolou příslušného záznamu (3.a.i), nebo není-li odesílatel v centrálním registru uveden, vyhledáním ve vnitrostátním registru země odesílatele, je-li k dispozici, a kontrolou příslušného záznamu (krok 3.a.ii).

Krok 3.b: Je-li vnitrostátní autentizační služba v členském státě zřízena a zpřístupněna, provádí modul rozhraní pro podávání zpráv funkci „autentizace odesílatele“ pomocí této vnitrostátní autentizační služby pouze při autentizaci odesílatelů používajících certifikát vydaný v daném členském státě.

Krok 4: Výsledek autentizace se zašle zpět do modulu rozhraní pro podávání zpráv. V případě úspěšné autentizace musí být zpráva zpřístupněna vrcholu 4 (jádru vnitrostátního jednotného námořního portálu) (krok 5). Pokud je autentizace neúspěšná, musí být zpráva o selhání odeslána zpět do vrcholu 2.



Obrázek 2

TECHNICKÉ SPECIFIKACE URAM

Integrace

ID	Název	Popis
URAM.01	Interoperabilní standardy	Software URAM musí být v souladu se standardními protokoly a při expozici svých rozhraní a integraci s jinými součástmi používat spolehlivé bezpečnostní prvky.

([1]) Označená jako OA4 v oddíle funkčních specifikací modulu rozhraní pro podávání zpráv v části I této přílohy.

URAM.02	Soulad s eIDAS	Software URAM využívá otevřené standardy a řešení EU a zavádí nezbytné kontrolní mechanismy pro kontrolu certifikátů odesílatele na základě důvěryhodných seznamů zveřejněných členskými státy v souladu s článkem 22 nařízení (EU) č. 910/2014 a prováděcím rozhodnutím Komise (EU) 2015/1505 ([2]), včetně informací týkajících se kvalifikovaných poskytovatelů služeb vytvářejících důvěru, kteří vydávají certifikáty používané pro elektronické pečetě.

Bezpečnost

ID	Název	Popis
URAM.03	Důvěrnost výměny informací	K zajištění bezpečnosti softwaru URAM a výměny jakýchkoli osobních údajů se zavedou tyto protokoly a metody šifrování: — Transport Layer Security (TLS): veškerý software v rámci systému URAM musí být zabezpečen pomocí TLS, aby zajišťoval šifrování na úrovni sítě a integritu údajů, a pomáhal tak chránit údaje během přenosu a bránil neoprávněnému přístupu nebo manipulaci. — Pro komunikaci se softwarem URAM musí být zavedena konfigurace TLS.
URAM.04	Bezpečnost aplikací	Software URAM musí zajišťovat odhalení škodlivých činností a bezpečný přenos citlivých informací.
URAM.05	Ochrana osobních údajů	Přístupová práva se udělují orgánům členských států podle čl. 12 odst. 2 nařízení (EU) 2019/1239 pro účely registrace odesílatelů. Software URAM zavede mechanismy pro kontrolu přístupu, aby byla zajištěna ochrana informací uživatelů, které jsou osobními údaji a jsou zpracovávány výhradně pro účely vytváření uživatelských účtů a správy odpovídajících přístupových práv. Centrální autentizační služba uchovává osobní údaje odesílatelů nejdéle po dobu nezbytnou pro účely autentizace. Centrální registr uchovává osobní údaje odesílatelů nejdéle po dobu nezbytnou pro správu účtu.

Udržitelnost a přenositelnost

ID	Název	Popis
URAM.06	Technologická nezávislost	Software URAM musí umožňovat interakci s modulem rozhraní pro podávání zpráv a dalšími relevantními službami, aniž by bylo zapotřebí proprietárního softwaru nebo hardwaru, a musí umožňovat integraci s uvedeným modulem bez ohledu na technologické prostředí, v němž je modul nasazen.

([2]) Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů podle čl. 22 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 235, 9.9.2015, s. 26).

URAM.07	Nezávislé nasazení	Software URAM nesmí mít zvláštní požadavky na nasazení modulu rozhraní pro podávání zpráv. Modul by měl pouze zajistit internetové připojení a dodržování standardů týkajících se bezpečnosti a protokolů softwaru URAM.

Funkce centrální autentizační služby

Centrální autentizační služba musí modulu rozhraní pro podávání zpráv poskytovat tyto služby.

ID	Název	Popis
URAM.08	Autentizační služba	Centrální autentizační služba odpovídá za autentizaci odesílatelů ověřováním platnosti certifikátu, čísla EORI a spojení mezi číslem EORI odesílatele a jeho certifikátem. Tato služba zpracovává žádosti o autentizaci odeslané prostřednictvím modulu rozhraní pro podávání zpráv a zasílá odpovědi o úspěšné nebo neúspěšné autentizaci.

Specifikace centrálního registru

ID	Název	Popis
URAM.09	Registrace odesílatele	Centrální registr poskytuje členským státům grafické uživatelské rozhraní pro registraci údajů o odesílateli. Po registraci v centrálním registru je odesílatel registrován ve všech členských státech.
URAM.10	Zobrazení a vyhledávání odesílatele	Centrální registr umožňuje členskému státu zobrazit všechny údaje o odesílatelích, které dosud zaregistroval. Poskytuje rovněž vyhledávací funkci pro vyhledávání údajů o zaregistrovaných odesílatelích podle různých vyhledávacích kritérií.
URAM.11	Aktualizace odesílatele	Centrální registr umožňuje členskému státu měnit všechny údaje o odesílatelích, které dosud zaregistroval, aby byla zajištěna přesnost a platnost údajů.
URAM.12	Deaktivace odesílatele	Centrální registr umožňuje členskému státu deaktivovat odesílatele, které dosud zaregistroval.
URAM.13	Audit a vykazování	Centrální registr poskytuje funkci vykazování, jež členskému státu umožní analyzovat konkrétní údaje o odesílatelích, které dosud zaregistroval, jako je datum registrace a platnost certifikátu.
URAM.14	Oznamování	Centrální registr poskytuje členským státům možnost dostávat od centrálního registru oznámení pokaždé, když je odesílatel, který byl dosud registrován tímto členským státem, zaregistrován, aktualizován nebo deaktivován a také když končí platnost jeho certifikátu.