2023/2790

18.12.2023

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2023/2790

z dnia 14 grudnia 2023 r.

ustanawiające specyfikacje funkcjonalne i techniczne na potrzeby modułu interfejsu sprawozdawczości morskiego krajowego pojedynczego punktu kontaktowego

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1239 z dnia 20 czerwca 2019 r. ustanawiające europejski system morskich pojedynczych punktów kontaktowych i uchylające dyrektywę 2010/65/UE ([1]), w szczególności jego art. 6 ust. 1 i art. 12 ust. 4,

po zasięgnięciu opinii Komitetu ds. Cyfrowych Ułatwień w Transporcie i Handlu,

a także mając na uwadze, co następuje:

(1) Specyfikacje modułu interfejsu sprawozdawczości powinny się opierać na powszechnie dostępnej technologii, łatwej do zainstalowania i zintegrowania ze wszystkimi morskimi krajowymi pojedynczymi punktami kontaktowymi (MNSW) oraz powinny umożliwiać sprawną integrację i utrzymanie w przyszłości.

(2) Specyfikacje funkcjonalne i techniczne modułu interfejsu sprawozdawczości powinny opierać się na wytycznych dotyczących projektowania szablonów architektury rozwiązań w zakresie wysokopoziomowych wymagań interoperacyjności (HL SAT), aby umożliwić identyfikowalność między ogólnymi i szczegółowymi wymogami interoperacyjności.

(3) Biorąc pod uwagę, że nadawcy korzystają z różnych systemów sprawozdawczych, a MNSW są wdrażane z wykorzystaniem różnych technologii, moduł interfejsu sprawozdawczości powinien opierać się na technologiach umożliwiających wymianę informacji między różnymi systemami informacyjnymi wykorzystującymi znormalizowany protokół, co umożliwia większą interoperacyjność.

(4) Obowiązki sprawozdawcze wymienione w załączniku do rozporządzenia (UE) 2019/1239 mogą wymagać od podmiotów zgłaszających przekazywania danych osobowych za pośrednictwem modułu interfejsu sprawozdawczości, który powinien wymieniać informacje w taki sposób, aby wszelkie dane osobowe były przetwarzane zgodnie z rozporządzeniem (UE) 2018/1725 ([2]) i rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([3]).

(5) Ponieważ moduł interfejsu sprawozdawczości jest opracowywany i aktualizowany przez Komisję i przekazywany państwom członkowskim w celu integracji, należy centralnie zarządzać dystrybucją nowych wersji modułu interfejsu sprawozdawczości, monitorowaniem prawidłowej instalacji oprogramowania i aktualizacją przewodnika wdrażania komunikatów, z uwzględnieniem, w miarę możliwości, wymogów bezpieczeństwa informatycznego MNSW.

(6) Aby zagwarantować stabilność, bezpieczeństwo i wydajność modułu interfejsu sprawozdawczości, państwa członkowskie powinny mieć możliwość monitorowania ruchu w sieci oraz analizowania zdarzeń w systemie, błędów i wyjątków, a także włączania tych informacji do swoich funkcjonujących systemów i procesów monitorowania. Aby to osiągnąć, moduł interfejsu sprawozdawczości powinien zapewniać odpowiednie funkcje umożliwiające rejestrowanie i przechowywanie zdarzeń oraz dostarczanie państwom członkowskim informacji o ruchu w sieci.

([1]) Dz.U. L 198 z 25.7.2019, s. 64.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

(7) W celu zapewnienia bezpiecznej wymiany informacji za pośrednictwem modułu interfejsu sprawozdawczości, nadawcy wymagają uwierzytelnienia. W związku z tym wspólny system rejestru użytkowników i zarządzania dostępem powinien obejmować centralną usługę uwierzytelniania i centralny rejestr jako kluczowe komponenty. Elementy te powinny ze sobą współdziałać, aby umożliwiać uwierzytelnianie nadawcy we wszystkich modułach interfejsu sprawozdawczości, zapewniając jednolity mechanizm uwierzytelniania.

(8) W celu bezpiecznej wymiany informacji za pomocą modułu interfejsu sprawozdawczości i zapewnienia, aby użytkownicy byli rozpoznawalni na szczeblu UE w momencie uzyskiwania dostępu do któregokolwiek z modułów interfejsu sprawozdawczości, nadawcy powinni uzyskać kwalifikowany certyfikat pieczęci elektronicznych zgodny z wymogami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([4]).

(9) Aby zapewnić nadawcom jedną rejestrację w celu wymiany informacji za pośrednictwem zharmonizowanych interfejsów sprawozdawczości w różnych państwach członkowskich, państwa członkowskie powinny mieć możliwość rejestrowania nadawców w centralnym rejestrze. Powinno to zmniejszyć obciążenie związane z wielokrotną rejestracją operacji transgranicznych w wielu MNSW. Wszystkimi danymi osobowymi w centralnym rejestrze należy zarządzać zgodnie z rozporządzeniami (UE) 2018/1725 i (UE) 2016/679.

(10) Aby zminimalizować zależność państw członkowskich od usług centralnych oraz biorąc pod uwagę, że MNSW mogą już być wspierane przez krajowe usługi uwierzytelniania, państwa członkowskie powinny mieć również możliwość ponownego wykorzystania własnych krajowych usług uwierzytelniania i rejestrów krajowych do celów uwierzytelnienia nadawców pragnących korzystać z modułu interfejsu sprawozdawczości jako alternatywy dla systemu rejestru użytkowników i zarządzania dostępem w europejskim systemie morskich pojedynczych punktów kontaktowych (EMSWe).

(11) Aby umożliwić państwom członkowskim prawidłowe zintegrowanie modułu interfejsu sprawozdawczości oraz systemu rejestru użytkowników i zarządzania dostępem do MNSW, niniejsze rozporządzenie powinno mieć zastosowanie od tego samego dnia co rozporządzenie (UE) 2019/1239.

(12) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który swoją opinię wydał w dniu 18 października 2023 r.,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „moduł interfejsu sprawozdawczości" oznacza element oprogramowania pośredniczącego w MNSW, o którym mowa w art. 2 pkt 4 rozporządzenia (UE) 2019/1239;

2) „nadawca" oznacza podmiot zgłaszający lub dostawcę usług w zakresie danych, który obsługuje system informatyczny wysyłający wiadomości elektroniczne do MNSW lub odbierający je za pośrednictwem modułu interfejsu sprawozdawczości;

3) „formalność" oznacza formalność zgodnie z definicją w art. 1 rozporządzenia wykonawczego Komisji (UE) 2023/204 ([5]);

4) „AS4" oznacza protokół komunikatu oparty na usługach sieciowych, służący bezpiecznej wymianie komunikatów między dwiema stronami;

5) „komunikat" oznacza cyfrowe przedstawienie formalności lub komunikatów odpowiedzi wykorzystywane do wymiany między nadawcą a MNSW;

6) „punkt dostępu AS4" oznacza oprogramowanie sterujące serwerem kompatybilne z protokołem komunikacyjnym AS4 i wymogami modułu interfejsu sprawozdawczości, umożliwiające wysyłanie i odbieranie informacji w imieniu nadawcy z modułu interfejsu sprawozdawczości i do niego;

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

([5]) Rozporządzenie wykonawcze Komisji (UE) 2023/204 z dnia 28 października 2022 r. ustanawiające specyfikacje techniczne, normy i procedury na potrzeby europejskiego systemu morskich pojedynczych punktów kontaktowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/1239 (Dz.U. L 33 z 3.2.2023, s. 1).

7) „podstawa morskiego krajowego pojedynczego punktu kontaktowego (podstawa MNSW)" oznacza komponent techniczny MNSW, z którym zintegrowany jest moduł interfejsu sprawozdawczości;

8) „walidacja syntaktyczna" oznacza proces sprawdzania, czy wiadomość elektroniczna nie zawiera błędów programowania, strukturalnych lub stylistycznych;

9) „walidacja semantyczna" oznacza proces, w którym sprawdzana jest zgodność danych ze szczegółowymi zasadami dotyczącymi danych w ramach formalności;

10) „przewodnik wdrażania komunikatów" oznacza specyfikację funkcjonalną określającą normy i komunikaty, które mają być wymieniane między nadawcami a MNSW za pośrednictwem modułu interfejsu sprawozdawczości;

11) „rejestracja" oznacza proces, w ramach którego osoba fizyczna lub prawna identyfikuje się i tworzy konto za pośrednictwem organu, o którym mowa w art. 12 ust. 2 rozporządzenia (UE) 2019/1239;

12) „identyfikacja" oznacza identyfikację elektroniczną zgodnie z definicją w art. 3 pkt 1 rozporządzenia (UE) nr 910/2014;

13) „środek identyfikacji elektronicznej" oznacza identyfikację elektroniczną zgodnie z definicją w art. 3 pkt 2 rozporządzenia (UE) nr 910/2014;

14) „uwierzytelnianie" oznacza uwierzytelnianie zgodnie z definicją w art. 3 pkt 5 rozporządzenia (UE) nr 910/2014;

15) „certyfikat" oznacza kwalifikowany certyfikat pieczęci elektronicznej zgodnie z definicją w art. 3 pkt 30 rozporządzenia (UE) nr 910/2014 wydany przez kwalifikowanego dostawcę usług zaufania zgodnie z definicją w art. 3 pkt 20 rozporządzenia (UE) nr 910/2014;

16) „numer EORI" oznacza numer identyfikacyjny zgodnie z definicją w art. 1 pkt 18 rozporządzenia delegowanego Komisji (UE) 2015/2446 ([6]);

17) „system rejestru użytkowników i zarządzania dostępem europejskiego systemu morskich pojedynczych punktów kontaktowych (EMSWe)" oznacza system obsługiwany przez Komisję, który obejmuje centralny rejestr i centralną usługę uwierzytelniania oraz zapewnia wzajemne uznawanie środków identyfikacji elektronicznej i uwierzytelnianie na potrzeby bezpiecznej transgranicznej wymiany danych między nadawcami a MNSW za pośrednictwem modułu interfejsu sprawozdawczości;

18) „centralny rejestr" oznacza prowadzony przez Komisję rejestr, w którym przechowuje się dane rejestracyjne nadawców przekazane przez państwa członkowskie w celu ułatwienia uwierzytelniania nadawców;

19) „rejestr krajowy" oznacza rejestr prowadzony przez państwo członkowskie, w którym przechowuje się dane rejestracyjne nadawców i który może być wykorzystywany do ułatwienia uwierzytelniania nadawców, jeżeli jest zgodny z wymogami centralnej usługi uwierzytelniania;

20) „centralna usługa uwierzytelniania" oznacza usługę obsługiwaną przez Komisję, w ramach której uwierzytelnia się nadawców korzystających z modułu interfejsu sprawozdawczości;

21) „krajowa usługa uwierzytelniania" oznacza usługę obsługiwaną przez państwo członkowskie, która może być wykorzystana do uwierzytelniania nadawców korzystających z modułu interfejsu sprawozdawczości.

Artykuł 2

Moduł interfejsu sprawozdawczości musi być zgodny ze specyfikacjami funkcjonalnymi i technicznymi określonymi w części I załącznika.

Aby pomóc w zintegrowaniu modułu interfejsu sprawozdawczości z MNSW, Komisja, w ścisłej współpracy z koordynatorami krajowymi europejskiego systemu morskich pojedynczych punktów kontaktowych:

— określa wytyczne dotyczące testowania i konfigurowania modułu interfejsu sprawozdawczości w celu włączenia do odpowiednich MNSW;

— definiuje i utrzymuje, przy wsparciu Europejskiej Agencji Bezpieczeństwa Morskiego, przewodnik wdrażania komunikatów.

([6]) Rozporządzenie delegowane Komisji (UE) 2015/2446 z dnia 28 lipca 2015 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 952/2013 w odniesieniu do szczegółowych zasad dotyczących niektórych przepisów unijnego kodeksu celnego (Dz.U. L 343 z 29.12.2015, s. 1).

Artykuł 3

Centralny rejestr i centralną usługę uwierzytelniania ustanawia się zgodnie ze specyfikacjami technicznymi, normami i procedurami określonymi w części II załącznika.

Artykuł 4

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia 15 sierpnia 2025 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 14 grudnia 2023 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

CZĘŚĆ I

MODUŁ INTERFEJSU SPRAWOZDAWCZOŚCI (RIM)

ARCHITEKTURA I ZAKRES

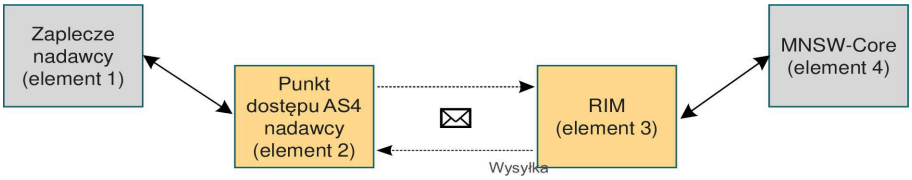
RIM jest częścią czteroelementowego modelu dla komunikatów wymienianych między nadawcami (element 1) a podstawą morskiego krajowego pojedynczego punktu kontaktowego (MNSW-Core) (element 4), przesyłanych za pośrednictwem punktów dostępu AS4 (elementy 2 i 3) dla każdej strony wdrażającej protokół AS4 w zakresie transportu i bezpieczeństwa, w następujący sposób:

Element 1: zaplecze nadawcy przygotowuje, przekazuje i odbiera wiadomości z i do MNSW-Core;

Element 2: punkt dostępu AS4 nadawcy;

Element 3: RIM;

Element 4: MNSW-Core odbiera komunikaty i wysyła komunikaty odpowiedzi do nadawcy.



Rysunek 1 – Architektura RIM wysokiego szczebla

RIM nie może przeprowadzać walidacji semantycznej komunikatów wykraczających poza specyfikacje przewodnika wdrażania komunikatów, obsługiwać ich sekwencji ani przechowywać komunikatów po ich pomyślnym przekazaniu do MNSW-Core lub nadawcy.

Zgodnie z art. 5 ust. 3 lit. c) rozporządzenia (UE) 2019/1239 po przekazaniu komunikatu z RIM do MNSW-Core państwa członkowskie, w stosownych przypadkach, tłumaczą, walidują i przekazują dane dotyczące formalności do systemów odpowiednich organów zgodnie ze specyfikacjami tych systemów.

SPECYFIKACJE FUNKCJONALNE RIM

Numer identyfikacyjny	Funkcja	Opis
LR1	Rejestrowanie i monitorowanie	Funkcja ta zapewnia rejestrowanie i przechowywanie zdarzeń (przypadki braku dostarczenia, opóźnienia i błędy odbiorcy).
LR2	Przechowywanie metadanych	Funkcja ta zapewnia przechowywanie metadanych wymienianych komunikatów.
OA1	Przechowywanie i wyszukiwanie danych technicznych	Funkcja ta zapewnia przechowywanie i wyszukiwanie danych technicznych koniecznych do konfiguracji i funkcjonowania RIM za pośrednictwem interfejsu (np. adresy techniczne punktów dostępu AS4 nadawców, schematy komunikatów przewodnika wdrażania komunikatów itp.).
OA2	Postępowanie z wyjątkami.	Funkcja ta przekazuje powiadomienia o wykrytych błędach przetwarzania lub nietypowych warunkach za pośrednictwem interfejsu użytkownika.
OA3	Dostęp do informacji i metadanych dotyczących rejestrowania i monitorowania	Funkcja ta zapewnia dostęp MNSW-Core do rejestrowania i monitorowania informacji i metadanych wymienianych komunikatów za pośrednictwem interfejsu międzysystemowego.

OA4	Uwierzytelnianie nadawcy	Funkcja uruchamia proces uwierzytelniania nadawcy korzystającego z centralnej lub krajowej usługi uwierzytelniania.
OA5	Walidacja komunikatów	Funkcja ta realizuje walidację składniową i semantyczną otrzymanych komunikatów zgodnie ze specyfikacjami technicznymi komunikatu zdefiniowanymi w przewodniku wdrażania komunikatów. W przewodniku wdrażania komunikatów określa się, które walidacje mają być wykonywane przez RIM. RIM powiadamia odpowiednio o błędach.
MF1	Obsługa komunikatów	Funkcja ta zapewnia, aby treść otrzymanych komunikatów (formalność lub odpowiedź) była przekazywana do odpowiedniego elementu bez zmian, jeżeli zatwierdzenia były pozytywne.

SPECYFIKACJE TECHNICZNE RIM

Integracja

Numer identyfikacyjny	Nazwa	Opis
IA1.	Standard protokołu przesyłania komunikatów	RIM wykorzystuje protokół przesyłania komunikatów AS4 w celu wspierania interoperacyjności z różnymi technologiami i systemami sprawozdawczości nadawców.

Wymiana komunikatów

Numer identyfikacyjny	Nazwa	Opis
AP1.	Model asynchronicznej wymiany komunikatów	RIM musi obsługiwać asynchroniczne przekazywanie komunikatów (formalność i odpowiedź) do i z MNSW-Core za pomocą mechanizmu „push and pull".

Bezpieczeństwo

Numer identyfikacyjny	Nazwa	Opis
SA1.	Poufność i bezpieczeństwo wymiany informacji	RIM zapewnia poufność informacji i ochronę wszystkich wymienianych danych osobowych poprzez szyfrowanie informacji wymienianych między punktem dostępu AS4 nadawców a RIM. RIM odszyfrowuje i udostępnia MNSW-Core komunikaty wysłane przez nadawcę. RIM stosuje jako standard protokół Web Service Security (WSS) w celu umożliwienia bezpiecznej wymiany komunikatów między punktem dostępu AS4 nadawcy a RIM.
SA2.	Niezaprzeczalność komunikatów	Przekazywanie i walidacja komunikatów za pośrednictwem RIM musi obejmować środki bezpieczeństwa mające na celu zapewnienie autentyczności wiadomości i uniknięcie ich zaprzeczenia

SA3.	Integralność	Należy wprowadzić środki techniczne zapewniające integralność wymienianych danych.
SA4.	Stosowanie Bezpieczeństwo	Postawę RIM muszą stanowić najlepsze praktyki w zakresie opracowywania oprogramowania, które umożliwiają wykrywanie szkodliwych działań oraz bezpieczne przekazywanie informacji szczególnie chronionych.
SA5.	Dostępność usług	W celu zapewnienia niezawodnej komunikacji i dystrybucji informacji między nadawcami a morskimi krajowymi pojedynczymi punktami kontaktowymi RIM musi wdrożyć mechanizmy zapewniające, aby komunikaty wymieniane z RIM nie zostały utracone w przypadku niedostępności usługi.

Wydajność i skalowalność

Numer identyfikacyjny	Nazwa	Opis
PS1.	Wydajność i skalowalność	RIM musi być w stanie osiągnąć obecne i przyszłe cele w zakresie wydajności, takie jak czas odpowiedzi, liczba równoczesnych nadawców oraz liczba/rozmiar wymienianych komunikatów.

Przenośność i wdrażanie

Numer identyfikacyjny	Nazwa	Opis
PD1.	Niezależność od platformy	RIM musi być kompatybilny z najpowszechniej występującą architekturą sprzętową i systemami operacyjnymi, w których byłby wdrażany. RIM nie powinien wymagać zastrzeżonego sprzętu ani oprogramowania zamkniętego do celów instalacji lub konfiguracji.
PD2	Aplikacja samoinstalacyjna	RIM należy dostarczać jako pakiet oprogramowania, który obejmuje wszystkie elementy aplikacji wymagane przez RIM. Zapewnione i wymagane zależności wymienia się w każdej nocie wydania RIM.

CZĘŚĆ II

SYSTEM REJESTRU UŻYTKOWNIKÓW I ZARZĄDZANIA DOSTĘPEM EUROPEJSKIEGO SYSTEMU MORSKICH POJEDYNCZYCH PUNKTÓW KONTAKTOWYCH

CENTRALNY REJESTR

Na wniosek nadawcy państwa członkowskie, które nie zapewniają krajowego rejestru zgodnego ze specyfikacjami centralnego rejestru określonymi w niniejszym załączniku, rejestrują numer EORI i certyfikat nadawcy w centralnym rejestrze oraz są odpowiedzialne za weryfikację i dokładność danych oraz zarządzanie nimi zgodnie z art. 12 ust. 2 rozporządzenia (UE) 2019/1239. Centralny rejestr zapewnia państwom członkowskim interfejs umożliwiający rejestrację nadawców i zarządzanie nimi.

CENTRALNA USŁUGA UWIERZYTELNIANIA

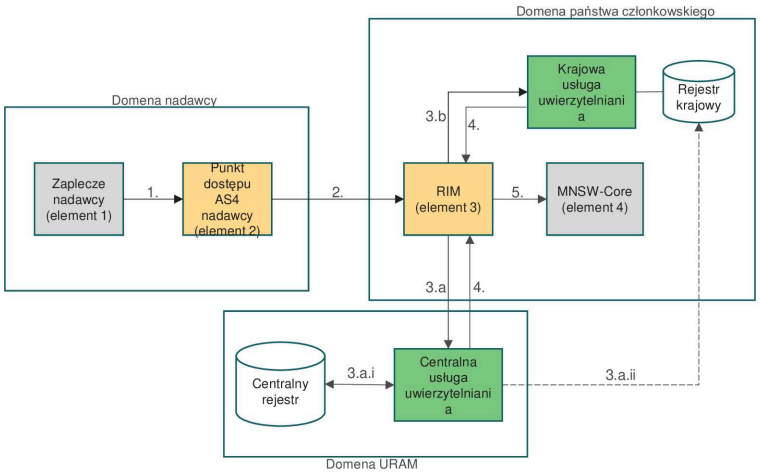
Poniższy schemat ilustruje kolejne etapy uwierzytelniania nadawcy, który przygotowuje i wysyła wiadomość do RIM (etap 1, 2).

RIM realizuje funkcję „uwierzytelniania dostawcy" ([1]) za pomocą centralnej usługi uwierzytelniania (etap 3.a).

Etap 3.a: Centralna usługa uwierzytelniania uwierzytelnia nadawcę, przeszukując centralny rejestr i sprawdzając odpowiedni rekord (3.a.i) lub, jeżeli nadawca nie występuje w centralnym rejestrze, przeszukując krajowy rejestr państwa nadawcy, jeżeli jest dostępny, oraz sprawdzając odpowiedni wpis (etap 3.a.ii).

Etap 3.b: W przypadku gdy krajowa usługa uwierzytelniania została ustanowiona i udostępniona w państwie członkowskim, RIM pełni funkcję „uwierzytelniania dostawcy" za pomocą tej krajowej usługi uwierzytelniania wyłącznie do celów uwierzytelnienia nadawców korzystających z certyfikatu wydanego w tym państwie członkowskim.

Etap 4: Wynik uwierzytelnienia należy odesłać do RIM. W przypadku pomyślnego uwierzytelnienia komunikat udostępnia się w elemencie 4 (MNSW-Core) (etap 5). Jeżeli uwierzytelnienie się nie powiedzie, komunikat o tym należy odesłać do elementu 2.



Rysunek 2

SPECYFIKACJE TECHNICZNE URAM

Integracja

Numer identyfikacyjny	Nazwa	Opis
URAM.01	Standardy interoperacyjne	Oprogramowanie URAM musi być zgodne ze standardowymi protokołami i posiadać solidne zabezpieczenia podczas ekspozycji swoich interfejsów i integracji z innymi komponentami.

([1]) Określoną jako OA4 w sekcji specyfikacji funkcjonalnych RIM w części I niniejszego załącznika.

URAM.02	Zgodność z eIDAS	Oprogramowanie URAM musi wykorzystywać otwarte normy i rozwiązania UE oraz wdrażać niezbędne mechanizmy kontroli w celu sprawdzenia certyfikatów nadawcy na podstawie zaufanych list publikowanych przez państwa członkowskie zgodnie z art. 22 rozporządzenia (UE) nr 910/2014 i decyzją wykonawczą Komisji (UE) 2015/1505 ([2]), z uwzględnieniem informacji dotyczących kwalifikowanych dostawców usług zaufania wydających certyfikaty wykorzystywane do pieczęci elektronicznych.

Bezpieczeństwo

Numer identyfikacyjny	Nazwa	Opis
URAM.03	Poufność wymiany informacji	Aby zapewnić bezpieczeństwo oprogramowania URAM i wymianę wszelkich danych osobowych, wdraża się następujące protokoły i metody szyfrowania: — Protokół TLS (Transport Layer Security): całe oprogramowanie w URAM musi być zabezpieczone za pomocą TLS w celu zapewnienia szyfrowania na poziomie sieci i integralności danych, aby pomóc chronić dane podczas transmisji, zapobiegając nieuprawnionemu dostępowi lub manipulacjom. — Aby komunikować się z oprogramowaniem URAM, należy wdrożyć konfigurację TLS.
URAM.04	Bezpieczeństwo aplikacji	Oprogramowanie URAM musi gwarantować wykrywanie szkodliwych działań oraz bezpieczne przekazywanie informacji szczególnie chronionych.
URAM.05	Ochrona danych osobowych	Prawa dostępu przyznaje się organom państw członkowskich zgodnie z art. 12 ust. 2 rozporządzenia (UE) 2019/1239 do celów rejestracji nadawców. Oprogramowanie URAM wdraża mechanizmy kontroli dostępu w celu zapewnienia ochrony informacji użytkownika będących danymi osobowymi, które są przetwarzane wyłącznie w celu tworzenia kont użytkowników i zarządzania odpowiednimi prawami dostępu. Centralna usługa uwierzytelniania przechowuje dane osobowe nadawców nie dłużej, niż jest to konieczne do celów uwierzytelnienia. Centralny rejestr przechowuje dane osobowe nadawców nie dłużej, niż jest to konieczne do celów zarządzania kontem.

Zrównoważoność i przenośność

Numer identyfikacyjny	Nazwa	Opis
URAM.06	Niezależność technologii	Oprogramowanie URAM umożliwia interakcje z RIM i innymi odpowiednimi usługami bez potrzeby posiadania oprogramowania zamkniętego lub zastrzeżonego sprzętu oraz umożliwia integrację z RIM niezależnie od środowiska technologicznego, w którym RIM jest wdrażany.

([2]) Decyzja wykonawcza Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U. L 235 z 9.9.2015, s. 26).

URAM.07	Niezależne wdrożenie	Oprogramowanie URAM nie może nakładać na RIM specjalnych wymogów dotyczących wdrożenia. RIM powinien zapewniać wyłącznie łączność internetową i przestrzeganie norm związanych z bezpieczeństwem i protokołami oprogramowania URAM.

Funkcje centralnej usługi uwierzytelniania

Należy udostępnić RIM następujące usługi uwierzytelniania za pomocą specjalnej usługi uwierzytelniania

Numer identyfikacyjny	Nazwa	Opis
URAM.08	Serwis uwierzytelniania	Centralna usługa uwierzytelniania musi odpowiadać za uwierzytelnianie nadawców poprzez weryfikację ważności certyfikatu, numeru EORI i powiązania między numerem EORI nadawcy a jego certyfikatem. Musi przetwarzać wnioski o uwierzytelnienie wysłane przez RIM i udzielać odpowiedzi wskazujących na pomyślne lub nieskuteczne uwierzytelnienie.

Specyfikacje centralnego rejestru

Numer identyfikacyjny	Nazwa	Opis
URAM.09	Rejestracja nadawcy	Centralny rejestr musi zapewniać państwom członkowskim graficzny interfejs użytkownika umożliwiający rejestrację danych nadawcy. Po zarejestrowaniu w centralnym rejestrze nadawca musi być zarejestrowany we wszystkich państwach członkowskich.
URAM.10	Widok i wyszukiwanie nadawcy	Centralny rejestr musi umożliwiać państwu członkowskiemu przeglądanie wszystkich danych nadawców, które wcześniej zarejestrowało. Musi on również zapewniać funkcję wyszukiwania umożliwiającą wyszukiwanie danych zarejestrowanych nadawców w oparciu o różne kryteria wyszukiwania.
URAM.11	Aktualizacja nadawcy	Centralny rejestr musi umożliwiać państwu członkowskiemu modyfikację wszystkich wcześniej zarejestrowanych danych nadawców w celu zapewnienia dokładności i ważności danych.
URAM.12	Dezaktywacja nadawcy	Centralny rejestr musi umożliwiać państwu członkowskiemu dezaktywację wcześniej zarejestrowanych nadawców.
URAM.13	Kontrola i sprawozdawczość	Centralny rejestr musi zapewniać możliwości sprawozdawcze umożliwiające państwu członkowskiemu analizę wcześniej zarejestrowanych danych określonych nadawców, takich jak data rejestracji i ważność certyfikatu.
URAM.14	Powiadomienia	Centralny rejestr musi dawać państwom członkowskim możliwość otrzymywania powiadomienia z centralnego rejestru za każdym razem, gdy nadawca uprzednio zarejestrowany przez dane państwo członkowskie jest zarejestrowany, aktualizowany lub dezaktywowany, a także gdy wygasa jego certyfikatu.