Amtsblatt
der Europäischen Union

DE
Reihe L

2023/2790

18.12.2023

DURCHFÜHRUNGSVERORDNUNG (EU) 2023/2790 DER KOMMISSION

vom 14. Dezember 2023

zur Festlegung funktionaler und technischer Spezifikationen für das Meldeschnittstellenmodul der nationalen zentralen Meldeportale für den Seeverkehr

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/1239 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Einrichtung eines europäischen Umfelds zentraler Meldeportale für den Seeverkehr und zur Aufhebung der Richtlinie 2010/65/EU ([1]), insbesondere auf Artikel 6 Absatz 1 und Artikel 12 Absatz 4,

nach Anhörung des Ausschusses für die Erleichterung der Digitalisierung in Verkehr und Handel,

in Erwägung nachstehender Gründe:

(1) Die Spezifikationen für das Meldeschnittstellenmodul sollten auf einer Technologie beruhen, die ohne Weiteres zugänglich und leicht installierbar ist und leicht in jedes nationale zentrale Meldeportal für den Seeverkehr integriert werden kann, und eine reibungslose Integration und Instandhaltung in Zukunft gewährleisten.

(2) Die funktionalen und technischen Spezifikationen für das Meldeschnittstellenmodul sollten auf den Designleitlinien im Architekturlösungsmuster für hochrangige Interoperabilitätsanforderungen (high-level Interoperability Requirements Solution Architecture Template (HL SAT) Design Guidelines) beruhen, um die Rückverfolgbarkeit zwischen hochrangigen und detaillierten Interoperabilitätsanforderungen zu ermöglichen.

(3) Da die Absender unterschiedliche Meldesysteme verwenden und die nationalen zentralen Meldeportale für den Seeverkehr unter Verwendung unterschiedlicher Technologien umgesetzt werden, sollte das Meldeschnittstellenmodul auf Technologien beruhen, die den Informationsaustausch zwischen verschiedenen, ein standardisiertes Protokoll verwendenden Informationssystemen ermöglichen, und damit größere Interoperabilität gewährleisten.

(4) Im Rahmen der Meldeverpflichtungen im Anhang der Verordnung (EU) 2019/1239 müssen die Anmelder gegebenenfalls personenbezogene Daten über das Meldeschnittstellenmodul übermitteln, über das die Informationen so ausgetauscht werden sollten, dass personenbezogene Daten im Einklang mit den Verordnungen (EU) 2018/1725 ([2]) und (EU) 2016/679 ([3]) des Europäischen Parlaments und des Rates verarbeitet werden.

(5) Da das Meldeschnittstellenmodul von der Kommission entwickelt und aktualisiert und von dieser zur Integration an die Mitgliedstaaten verteilt wird, sollten die Verteilung neuer Versionen des Meldeschnittstellenmoduls, die Überwachung der korrekten Installation der Software und die Aktualisierung des Leitfadens für Nachrichten zentral gesteuert werden, wobei die IT-Sicherheitsanforderungen der nationalen zentralen Meldeportale für den Seeverkehr soweit möglich zu berücksichtigen sind.

(6) Um die Stabilität, Sicherheit und Leistungsfähigkeit des Meldeschnittstellenmoduls zu gewährleisten, sollten die Mitgliedstaaten in der Lage sein, den Netzverkehr zu überwachen, Systemereignisse, Fehler und Ausnahmen zu analysieren und die betreffenden Informationen in ihre bestehenden Überwachungssysteme und -verfahren zu integrieren. Daher sollte das Meldeschnittstellenmodul geeignete Funktionen bieten, mit denen Ereignisse protokolliert und gespeichert werden können, und den Mitgliedstaaten Informationen über den Netzverkehr zur Verfügung stellen.

([1]) ABl. L 198 vom 25.7.2019, S. 64.

([2]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

([3]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

(7) Um einen sicheren Informationsaustausch über das Meldeschnittstellenmodul zu gewährleisten, benötigen Absender eine Authentifizierung. Daher sollte das gemeinsame Nutzerregistrierungs- und Zugangsverwaltungssystem über einen zentralen Authentifizierungsdienst und ein Zentralregister als Schlüsselkomponenten verfügen. Diese Komponenten sollten ineinandergreifen, um in allen Meldeschnittstellenmodulen eine Authentifizierung von Absendern zu ermöglichen und so einen einheitlichen Authentifizierungsmechanismus zu schaffen.

(8) Um Informationen sicher über das Meldeschnittstellenmodul auszutauschen und zu gewährleisten, dass die Nutzer auf EU-Ebene erkannt werden, wenn sie auf eines der Meldeschnittstellenmodule zugreifen, sollten die Absender ein qualifiziertes Zertifikat für elektronische Siegel erhalten, das den Anforderungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([4]) entspricht.

(9) Damit sich die Absender nur einmal für den Informationsaustausch über die harmonisierten Meldeschnittstellen in verschiedenen Mitgliedstaaten registrieren müssen, sollten die Mitgliedstaaten die Absender im Zentralregister registrieren können. Dadurch dürften sich die Belastung durch Mehrfachregistrierungen in verschiedenen nationalen zentralen Meldeportalen für den Seeverkehr bei grenzüberschreitenden Tätigkeiten verringern. Alle personenbezogenen Daten im Zentralregister sollten im Einklang mit den Verordnungen (EU) 2018/1725 und (EU) 2016/679 verwaltet werden.

(10) Damit die Mitgliedstaaten so wenig wie möglich auf zentrale Dienste angewiesen sind und da die nationalen zentralen Meldeportale für den Seeverkehr möglicherweise bereits von nationalen Authentifizierungsdiensten unterstützt werden, sollten die Mitgliedstaaten zur Authentifizierung von Absendern, die das Meldeschnittstellenmodul nutzen möchten, auch ihre nationalen Authentifizierungsdienste und nationalen Register als Alternative zum Nutzerregistrierungs- und Zugangsverwaltungssystem des europäischen Umfelds zentraler Meldeportale für den europäischen Seeverkehr nutzen dürfen.

(11) Damit die Mitgliedstaaten das Meldeschnittstellenmodul und das Nutzerregistrierungs- und Zugangsverwaltungssystem ordnungsgemäß in die nationalen zentralen Meldeportale für den Seeverkehr integrieren können, sollte diese Verordnung ab demselben Datum gelten wie die Verordnung (EU) 2019/1239.

(12) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 18. Oktober 2023 eine Stellungnahme abgegeben.

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Meldeschnittstellenmodul“ eine Middleware-Komponente im nationalen zentralen Meldeportal für den Seeverkehr (Maritime National Single Window, MNSW) gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2019/1239;
2. „Absender“ einen Anmelder oder Datendienstleister, der das IT-System betreibt, das über das Meldeschnittstellenmodul elektronische Nachrichten an nationale zentrale Meldeportale für den Seeverkehr sendet oder diese empfängt;
3. „Förmlichkeit“ eine Förmlichkeit gemäß Artikel 1 der Durchführungsverordnung (EU) 2023/204 der Kommission ([5]);
4. „AS4“ ein auf Webdiensten beruhendes Nachrichtenprotokoll zum sicheren Austausch von Nachrichten zwischen zwei Parteien;
5. „Nachricht“ eine digitale Darstellung von Förmlichkeiten oder Antwortnachrichten, die für den Austausch zwischen dem Absender und dem nationalen zentralen Meldeportal für den Seeverkehr verwendet wird;
6. „AS4-Zugangspunkt“ eine Server-Betriebssoftware, die mit dem AS4-Nachrichtenprotokoll und den Anforderungen des Meldeschnittstellenmoduls kompatibel ist und die es ermöglicht, im Namen eines Absenders Informationen über das Meldeschnittstellenmodul zu senden und zu empfangen;

([4]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

([5]) Durchführungsverordnung (EU) 2023/204 der Kommission vom 28. Oktober 2022 zur Festlegung von technischen Spezifikationen, Normen und Verfahren für das europäische Umfeld zentraler Meldeportale für den Seeverkehr gemäß der Verordnung (EU) 2019/1239 des Europäischen Parlaments und des Rates ABl. L 33 vom 3.2.2023, S. 1).

7. „Kern des nationalen zentralen Meldeportals für den Seeverkehr (MNSW-Core)“ eine technische Komponente des nationalen zentralen Meldeportals für den Seeverkehr, in die das Meldeschnittstellenmodul integriert ist;

8. „syntaktische Validierung“ das Verfahren zur Überprüfung, ob eine elektronische Nachricht frei von Programmier-, Struktur- oder Stilfehlern ist;

9. „semantische Validierung“ das Verfahren zur Überprüfung, ob Daten den spezifischen Datenvorschriften innerhalb einer Förmlichkeit entsprechen;

10. „Leitfaden für Nachrichten“ eine funktionale Spezifikation für Standards und Nachrichten, die über das Meldeschnittstellenmodul zwischen Absendern und nationalen zentralen Meldeportalen für den Seeverkehr ausgetauscht werden;

11. „Registrierung“ das Verfahren, in dem sich eine natürliche oder juristische Person gegenüber der in Artikel 12 Absatz 2 der Verordnung (EU) 2019/1239 genannten Behörde identifiziert und ein Konto bei ihr anlegt;

12. „Identifizierung“ die elektronische Identifizierung gemäß Artikel 3 Nummer 1 der Verordnung (EU) Nr. 910/2014;

13. „elektronisches Identifizierungsmittel“ ein elektronisches Identifizierungsmittel gemäß Artikel 3 Nummer 2 der Verordnung (EU) Nr. 910/2014;

14. „Authentifizierung“ die Authentifizierung gemäß Artikel 3 Nummer 5 der Verordnung (EU) Nr. 910/2014;

15. „Zertifikat“ ein qualifiziertes Zertifikat für elektronische Siegel gemäß Artikel 3 Nummer 30 der Verordnung (EU) Nr. 910/2014, das von einem qualifizierten Vertrauensdiensteanbieter gemäß Artikel 3 Nummer 20 der Verordnung (EU) Nr. 910/2014 ausgestellt wurde;

16. „EORI-Nummer“ eine Kennnummer gemäß Artikel 1 Nummer 18 der Delegierten Verordnung (EU) 2015/2446 der Kommission ([6]);

17. „Nutzerregistrierungs- und Zugangsverwaltungssystem für das europäische Umfeld zentraler Meldeportale für den Seeverkehr“ ein von der Kommission betriebenes System, das ein Zentralregister und einen zentralen Authentifizierungsdienst umfasst und die gegenseitige Anerkennung elektronischer Identifizierungsmittel sowie die Authentifizierung für einen sicheren grenzüberschreitenden Datenaustausch zwischen Absendern und nationalen zentralen Meldeportalen für den Seeverkehr über das Meldeschnittstellenmodul gewährleistet;

18. „Zentralregister“ ein von der Kommission geführtes Register, in dem die von den Mitgliedstaaten übermittelten Registrierungsdaten der Absender gespeichert werden, um die Authentifizierung der Absender zu erleichtern;

19. „nationales Register“ ein von einem Mitgliedstaat geführtes Register, in dem die Registrierungsdaten der Absender gespeichert sind und das zur Erleichterung der Authentifizierung der Absender verwendet werden kann, sofern es den Anforderungen des zentralen Authentifizierungsdienstes entspricht;

20. „zentraler Authentifizierungsdienst“ einen von der Kommission betriebenen Dienst, der Absender authentifiziert, die das Meldeschnittstellenmodul verwenden;

21. „nationaler Authentifizierungsdienst“ einen von einem Mitgliedstaat betriebenen Dienst, der zur Authentifizierung von Absendern, die das Meldeschnittstellenmodul verwenden, verwendet werden kann.

Artikel 2

Das Meldeschnittstellenmodul muss den funktionalen und technischen Spezifikationen in Teil I des Anhangs entsprechen.

Um die Integration des Meldeschnittstellenmoduls in die nationalen zentralen Meldeportale zu unterstützen, wird die Kommission in enger Zusammenarbeit mit den nationalen Koordinatoren des europäischen Umfelds zentraler Meldeportale für den Seeverkehr

— Leitlinien zur Erprobung und Konfiguration des Meldeschnittstellenmoduls für die Integration in das jeweilige nationale zentrale Meldeportal erstellen;

— mit Unterstützung der Europäischen Agentur für die Sicherheit des Seeverkehrs den Leitfaden für Nachrichten erstellen und pflegen.

([6]) Delegierte Verordnung (EU) 2015/2446 der Kommission vom 28. Juli 2015 zur Ergänzung der Verordnung (EU) Nr. 952/2013 des Europäischen Parlaments und des Rates mit Einzelheiten zur Präzisierung von Bestimmungen des Zollkodex der Union (ABl. L 343 vom 29.12.2015, S. 1).

Artikel 3

Das Zentralregister und der zentrale Authentifizierungsdienst werden gemäß den technischen Spezifikationen, Standards und Verfahren in Teil II des Anhangs eingerichtet.

Artikel 4

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 15. August 2025.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 14. Dezember 2023

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

TEIL I

MELDESCHNITTSTELLENMODUL

ARCHITEKTUR UND ANWENDUNGSBEREICH

Das Meldeschnittstellenmodul ist Teil eines Viereckpunktemodells für Nachrichten, die zwischen den Absendern (Eckpunkt 1) und dem MNSW-Core (Eckpunkt 4) ausgetauscht werden und über AS4-Zugangspunkte (Eckpunkte 2 und 3) auf jeder Seite weitergeleitet werden, wobei das AS4-Protokoll für Transport und Sicherheit wie folgt umzusetzen ist:

Eckpunkt 1: Backoffice des Absenders, das Nachrichten erstellt, an den MNSW-Core sendet und von diesem empfängt;

Eckpunkt 2: AS4-Zugangspunkt des Absenders;

Eckpunkt 3: Meldeschnittstellenmodul;

Eckpunkt 4: MNSW-Core, der Nachrichten empfängt und Antwortnachrichten an den Absender sendet.

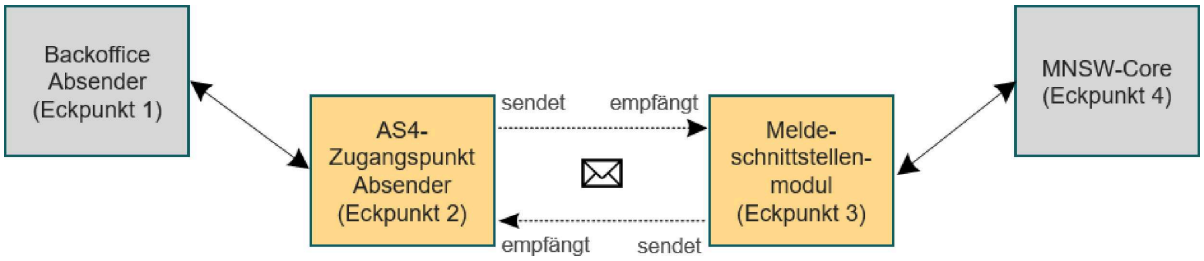

Abbildung 1 — Hochrangige Architektur des Meldeschnittstellenmoduls

Das Meldeschnittstellenmodul darf — über die Spezifikationen im Leitfaden für Nachrichten hinaus — keine semantische Validierung von Nachrichten durchführen, deren Sequenz nicht bearbeiten und Nachrichten nicht länger speichern, als bis sie erfolgreich an den MNSW-Core oder den Absender übermittelt wurden.

Gemäß Artikel 5 Absatz 3 Buchstabe c der Verordnung (EU) 2019/1239 müssen die Mitgliedstaaten, sobald die Nachricht vom Meldeschnittstellenmodul an den MNSW-Core übermittelt wurde, die Förmlichkeitsdaten, soweit erforderlich, übersetzen, validieren und an die Systeme der zuständigen Behörden gemäß den Spezifikationen dieser Systeme übermitteln.

FUNKTIONALE SPEZIFIKATIONEN FÜR DAS MELDESCHNITTSTELLENMODUL

ID	Funktion	Beschreibung
LR1	Protokollierung und Überwachung	Die Funktion muss die Protokollierung und Speicherung von Ereignissen (Zustellfehler, Verzögerungen und Fehler des Empfängers) gewährleisten.
LR2	Metadatenspeicherung	Die Funktion muss die Speicherung der Metadaten von ausgetauschten Nachrichten gewährleisten.
OA1	Technische Datenspeicherung und Suche	Die Funktion muss die Speicherung der für die Konfiguration und Funktionsweise des Meldeschnittstellenmoduls erforderlichen technischen Daten (z. B. die technischen Adressen der AS4-Zugangspunkte der Absender, die Nachrichtenschemata des Leitfadens für Nachrichten usw.) und die Suche nach diesen Daten über eine Schnittstelle gewährleisten.
OA2	Behandlung von Ausnahmen	Die Funktion muss über eine Benutzerschnittstelle Benachrichtigungen über festgestellte Verarbeitungsfehler und/oder anomale Bedingungen bereitstellen.
OA3	Zugang zu Protokollierungs- und Überwachungsinformationen und Metadaten	Die Funktion muss dem MNSW-Core über eine System-zu-System-Schnittstelle Zugang zu Protokollierungs- und Überwachungsinformationen und Metadaten von ausgetauschten Nachrichten bieten.

OA4	Absenderauthentifizierung	Die Funktion muss das Authentifizierungsverfahren für einen Absender, der einen zentralen oder nationalen Authentifizierungsdienst nutzt, starten.
OA5	Validierung von Nachrichten	Die Funktion muss die syntaktische und semantische Validierung eingegangener Nachrichten gemäß den im Leitfaden für Nachrichten festgelegten technischen Spezifikationen für Nachrichten durchführen. Im Leitfaden für Nachrichten muss aufgeführt werden, welche Validierungen vom Meldeschnittstellenmodul durchzuführen sind. Das Meldeschnittstellenmodul muss über die entsprechenden Fehler benachrichtigen.
MF1	Behandlung von Nachrichten	Die Funktion muss gewährleisten, dass der Inhalt der eingegangenen Nachrichten (Förmlichkeit oder Antwortnachricht) nach erfolgreicher Validierung unverändert an den entsprechenden Eckpunkt übermittelt wird.

FUNKTIONALE SPEZIFIKATIONEN FÜR DAS MELDESCHNITTSTELLENMODUL

Integration

ID	Bezeichnung	Beschreibung
IA1.	Standard des Nachrichtenprotokolls	Das Meldeschnittstellenmodul muss zur Förderung der Interoperabilität mit unterschiedlichen Technologien und Meldesystemen der Absender das AS4-Nachrichtenprotokoll verwenden.

Austausch von Nachrichten

ID	Bezeichnung	Beschreibung
AP1.	Asynchrones Nachrichtenaustauschmuster	Das Meldeschnittstellenmodul muss die asynchrone Übermittlung von Nachrichten (Formalität und Antwortnachricht) an den und vom MNSW-Core mittels Push- und Pull-Mechanismus unterstützen.

Sicherheit

ID	Bezeichnung	Beschreibung
SA1.	Vertraulichkeit und Sicherheit des Informationsaustauschs	Das Meldeschnittstellenmodul muss die Vertraulichkeit der ausgetauschten Informationen und den Schutz aller ausgetauschten personenbezogenen Daten durch Verschlüsselung der zwischen dem AS4-Zugangspunkt der Absender und dem Meldeschnittstellenmodul übermittelten Informationen gewährleisten. Das Meldeschnittstellenmodul entschlüsselt die von einem Absender gesendeten Nachrichten und leitet sie an den MNSW-Core weiter. Das Meldeschnittstellenmodul muss zum sicheren Austausch von Nachrichten zwischen dem AS4-Zugangspunkt des Absenders und dem Meldeschnittstellenmodul ein WS-Security (Web Service Security) als Standard verwenden.
SA2.	Nichtabstreitbarkeit von Nachrichten	Die Kommunikation und Validierung von Nachrichten über das Meldeschnittstellenmodul muss Sicherheitsmaßnahmen umfassen, mit denen die Authentizität der Nachrichten gewährleistet und eine Verleugnung der Nachrichten verhindert wird.

SA3.	Integrität	Es müssen technische Maßnahmen getroffen werden, um die Integrität der ausgetauschten Daten zu gewährleisten.
SA4.	Sicherheit der Anwendung	Das Meldeschnittstellenmodul muss auf bewährten Verfahren der Softwareentwicklung beruhen, um die Aufdeckung böswilliger Aktivitäten und die sichere Übertragung sensibler Informationen zu ermöglichen.
SA5.	Dienstverfügbarkeit	Im Interesse einer zuverlässigen Kommunikation und eines zuverlässigen Informationsaustauschs zwischen den Absendern und den nationalen zentralen Meldeportalen für den Seeverkehr muss das Meldeschnittstellenmodul Mechanismen vorsehen, um sicherzustellen, dass die über das Meldeschnittstellenmodul ausgetauschten Nachrichten bei Nichtverfügbarkeit des Dienstes nicht verloren gehen.

Leistung und Skalierbarkeit

ID	Bezeichnung	Beschreibung
PS1.	Leistung und Skalierbarkeit	Das Meldeschnittstellenmodul muss in der Lage sein, bestehende und künftige Leistungsziele, z. B. in Bezug auf die Reaktionszeit, die Anzahl gleichzeitiger Absender oder die Menge/Größe der ausgetauschten Nachrichten, zu erreichen.

Übertragbarkeit und Einführung

ID	Bezeichnung	Beschreibung
PD1.	Unabhängigkeit der Plattform	Das Meldeschnittstellenmodul muss mit den gängigsten Hardwarearchitektur- und Betriebssystemen am Ort seiner Einführung kompatibel sein. Das Meldeschnittstellenmodul darf zur Installation oder Konfiguration keine proprietäre Hardware oder Software benötigen.
PD2	Selbstinstallierende Anwendung	Das Meldeschnittstellenmodul wird als Softwarepaket bereitgestellt, das alle für das Meldeschnittstellenmodul erforderlichen Anwendungskomponenten umfasst. Die bereitgestellten und erforderlichen Abhängigkeiten müssen im jeweiligen Veröffentlichungsvermerk des Meldeschnittstellenmoduls aufgeführt werden.

TEIL II

NUTZERREGISTRIERUNGS- UND ZUGANGSVERWALTUNGSSYSTEM FÜR DAS EUROPÄISCHE UMFELD ZENTRALER MELDEPORTALE FÜR DEN SEEVERKEHR (EUROPEAN MARITIME SINGLE WINDOW ENVIRONMENT, EMSWE)

ZENTRALREGISTER

Mitgliedstaaten, die kein nationales Register haben, das den Spezifikationen für das Zentralregister gemäß diesem Anhang entspricht, registrieren auf Antrag des Absenders die EORI-Nummer und das Zertifikat des Absenders im Zentralregister und sind gemäß Artikel 12 Absatz 2 der Verordnung (EU) 2019/1239 für die Überprüfung, Richtigkeit und Verwaltung der Daten verantwortlich. Das Zentralregister muss den Mitgliedstaaten eine Schnittstelle für die Registrierung und Verwaltung der Absender bieten.

ZENTRALER AUTHENTIFIZIERUNGSDIENST

Das nachstehende Diagramm veranschaulicht, in welchen Schritten die Authentifizierung eines Absenders erfolgt, der eine Nachricht erstellt und an das Meldeschnittstellenmodul gesendet hat (Schritte 1 und 2).

Das Meldeschnittstellenmodul muss die Funktion „Absenderauthentifizierung“ ([1]) mithilfe des zentralen Authentifizierungsdienstes durchführen (Schritt 3.a).

Schritt 3.a: Der zentrale Authentifizierungsdienst authentifiziert den Absender durch Abfrage des Zentralregisters und Überprüfung des entsprechenden Eintrags (3.a.i) oder, falls der Absender nicht im Zentralregister aufgeführt ist, durch Abfrage des nationalen Registers des Landes des Absenders, sofern vorhanden, und Überprüfung des entsprechenden Eintrags (Schritt 3.a.ii).

Schritt 3.b: Wird in einem Mitgliedstaat ein nationaler Authentifizierungsdienst eingerichtet und bereitgestellt, so darf das Meldeschnittstellenmodul die Funktion „Absenderauthentifizierung“ nur für die Authentifizierung von Absendern, die ein in diesem Mitgliedstaat ausgestelltes Zertifikat verwenden, mithilfe des betreffenden nationalen Authentifizierungsdienstes durchführen.

Schritt 4: Das Ergebnis der Authentifizierung muss an das Meldeschnittstellenmodul zurückgesendet werden. Ist die Authentifizierung erfolgreich, wird die Nachricht an Eckpunkt 4 (MNSW-Core) weitergeleitet (Schritt 5). Ist die Authentifizierung erfolglos, muss eine Fehlermeldung an Eckpunkt 2 zurückgesendet werden.

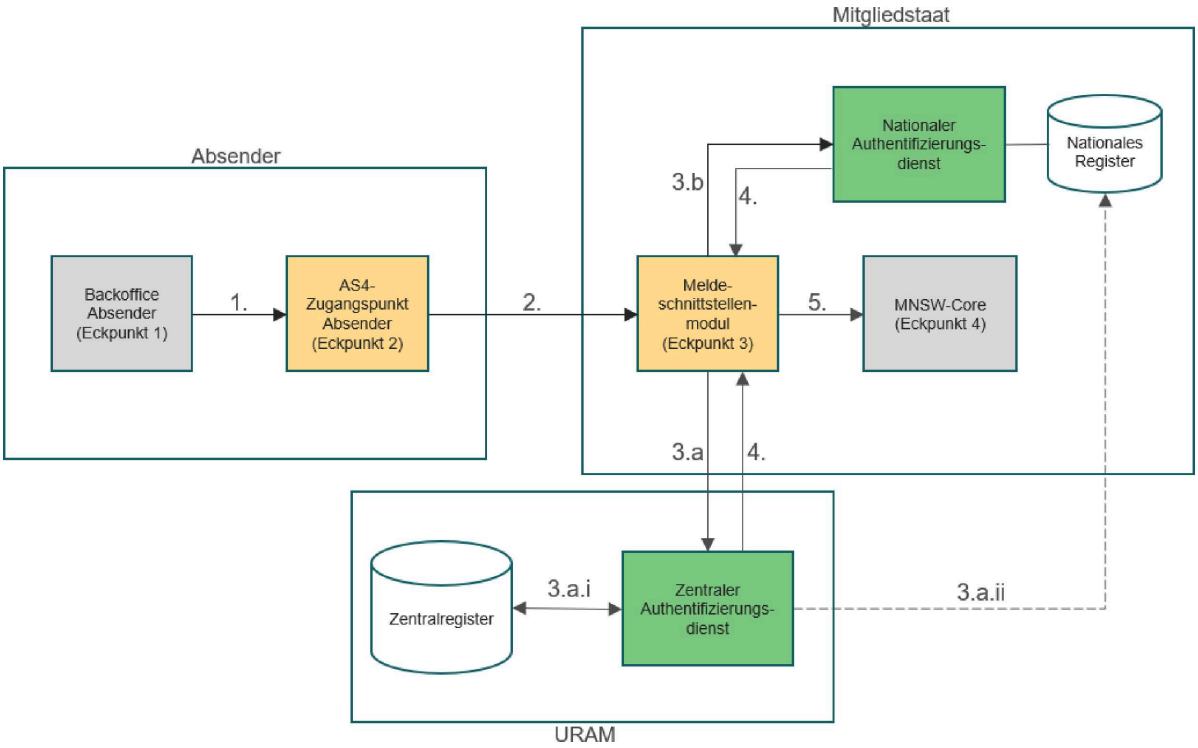

Abbildung 2

TECHNISCHE SPEZIFIKATIONEN FÜR NUTZERREGISTER UND ZUGANGSVERWALTUNG (USER REGISTRY AND ACCESS MANAGEMENT, URAM)

Integration

ID	Bezeichnung	Beschreibung
URAM.01	Interoperable Standards	Die URAM-Software muss den Standardprotokollen entsprechen und robuste Sicherheitsmerkmale verwenden, wenn ihre Schnittstellen exponiert und mit anderen Komponenten integriert werden.

([1]) OA4 im Abschnitt über die funktionalen Spezifikationen für das Meldeschnittstellenmodul in Teil I dieses Anhangs.

URAM.02	Konformität mit eIDAS	Die URAM-Software muss offene EU-Standards und -Lösungen nutzen und die erforderlichen Kontrollmechanismen vorsehen, um die Zertifikate der Absender mit den von den Mitgliedstaaten gemäß Artikel 22 der Verordnung (EU) Nr. 910/2014 und Durchführungsbeschluss (EU) 2015/1505 der Kommission ([2]) veröffentlichten Vertrauenslisten einschließlich Informationen über qualifizierte Vertrauensdiensteanbieter, die Zertifikate für elektronische Siegel ausstellen, abzugleichen.

Sicherheit

ID	Bezeichnung	Beschreibung
URAM.03	Vertraulichkeit des Informationsaustauschs	Um die Sicherheit der URAM-Software und des Austauschs personenbezogener Daten zu gewährleisten, müssen folgende Protokolle und Verschlüsselungsmethoden verwendet werden: — Transport Layer Security (TLS): Die gesamte URAM-Software muss mithilfe von TLS gesichert werden, um die Verschlüsselung auf Netzwerkebene und die Datenintegrität zu gewährleisten und damit zum Schutz der Daten während der Übertragung beizutragen und den Zugriff oder Manipulationen Unbefugter zu verhindern. — Für die Kommunikation mit der URAM-Software muss eine TLS-Konfiguration vorgesehen sein.
URAM.04	Sicherheit der Anwendung	Die URAM-Software muss die Aufdeckung böswilliger Aktivitäten und die sichere Übertragung sensibler Informationen gewährleisten.
URAM.05	Schutz personenbezogener Daten	Den Behörden der Mitgliedstaaten werden gemäß Artikel 12 Absatz 2 der Verordnung (EU) 2019/1239 Zugangsrechte für die Zwecke der Registrierung von Absendern gewährt. Die URAM-Software muss Zugangskontrollen vorsehen, um den Schutz von Nutzerinformationen zu gewährleisten, bei denen es sich um personenbezogene Daten handelt, die ausschließlich zum Zweck der Einrichtung von Nutzerkonten und der Verwaltung der entsprechenden Zugangsrechte verarbeitet werden. Der zentrale Authentifizierungsdienst speichert personenbezogene Daten der Absender nicht länger, als dies für die Authentifizierung erforderlich ist. Das Zentralregister speichert personenbezogene Daten der Absender nicht länger, als dies für die Kontoverwaltung erforderlich ist.

Nachhaltigkeit und Übertragbarkeit

ID	Bezeichnung	Beschreibung
URAM.06	Technologische Unabhängigkeit	Die URAM-Software muss die Interaktion mit dem Meldeschnittstellenmodul und anderen einschlägigen Diensten ermöglichen, ohne dass dafür eine proprietäre Software oder Hardware erforderlich wäre, und sie muss die Integration mit dem Meldeschnittstellenmodul ermöglichen, und zwar unabhängig von der technologischen Umgebung, in der das Meldeschnittstellenmodul eingeführt wird.

([2]) Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 235 vom 9.9.2015, S. 26).

URAM.07	Unabhängige Einführung	Die URAM-Software darf mit keiner spezifischen Einführungsanforderung für das Meldeschnittstellenmodul verbunden sein. Das Meldeschnittstellenmodul sollte nur eine Internetanbindung und die Konformität mit den Standards für die Sicherheit und die Protokolle der URAM-Software gewährleisten.

Zentraler Authentifizierungsdienst

Die folgenden Dienste müssen dem Meldeschnittstellenmodul vom zentralen Authentifizierungsdienst zur Verfügung gestellt werden.

ID	Bezeichnung	Beschreibung
URAM.08	Authentifizierungsdienst	Der zentrale Authentifizierungsdienst authentifiziert die Absender, indem er die Gültigkeit des Zertifikats, die EORI-Nummer und die Verbindung zwischen der EORI-Nummer des Absenders und dem Zertifikat überprüft. Er bearbeitet Authentifizierungsanträge, die vom Meldeschnittstellenmodul gesendet werden, und antwortet mit der Anzeige erfolgreicher oder erfolgloser Authentifizierung.

Spezifikationen für das Zentralregister

ID	Bezeichnung	Beschreibung
URAM.09	Absenderregistrierung	Das Zentralregister muss den Mitgliedstaaten eine grafische Benutzerschnittstelle für die Registrierung der Absenderdaten bieten. Sobald der Absender im Zentralregister registriert ist, muss er in allen Mitgliedstaaten registriert sein.
URAM.10	Absenderanzeige und Suche	Das Zentralregister muss es einem Mitgliedstaat ermöglichen, alle Daten der Absender einzusehen, die er registriert hat. Außerdem muss es eine Suchfunktion für den Abruf der Daten der registrierten Absender bieten, die verschiedene Suchkriterien vorsieht.
URAM.11	Absenderaktualisierung	Das Zentralregister muss es einem Mitgliedstaat ermöglichen, alle Daten der von ihm registrierten Absender zu ändern, um die Richtigkeit und Gültigkeit der Daten zu gewährleisten.
URAM.12	Absenderdeaktivierung	Das Zentralregister muss es einem Mitgliedstaat ermöglichen, die von ihm registrierten Absender zu deaktivieren.
URAM.13	Prüfung und Meldung	Das Zentralregister muss Meldefähigkeiten vorsehen, die es einem Mitgliedstaat ermöglichen, die von ihm registrierten spezifischen Absenderdaten, z. B. das Datum der Registrierung und die Gültigkeit des Zertifikats, zu analysieren.
URAM.14	Benachrichtigungen	Das Zentralregister muss den Mitgliedstaaten die Möglichkeit bieten, jedes Mal eine Benachrichtigung vom Zentralregister zu erhalten, wenn ein von dem betreffenden Mitgliedstaat registrierter Absender registriert, aktualisiert oder deaktiviert wird und wenn das betreffende Zertifikat abläuft.