2023/2790

18.12.2023

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2023/2790

af 14. december 2023

om fastsættelse af funktionsspecifikationer og tekniske specifikationer for meldegrænseflademodulet til de nationale søfartsmiljøer med ét kontaktpunkt

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2019/1239 af 20. juni 2019 om oprettelse af et europæisk søfartsmiljø med ét kontaktpunkt og om ophævelse af direktiv 2010/65/EU ([1]), særlig artikel 6, stk. 1, og artikel 12, stk. 4, og

efter høring af Udvalget for Digital Transport og Handel, og

ud fra følgende betragtninger:

(1) Specifikationerne for meldegrænseflademodulet bør være baseret på en teknologi, som er umiddelbart tilgængelig og let at installere og integrere i alle nationale søfartsmiljøer med ét kontaktpunkt og bør give mulighed for gnidningsløs integration og vedligeholdelse i fremtiden.

(2) Meldegrænseflademodulets funktionsspecifikationer og tekniske specifikationer bør være baseret på retningslinjerne for udformning af skabeloner for løsningsarkitektur for interoperabilitetskrav på højt niveau (high-level Interoperability Requirements Solution Architecture Template (HL SAT) Design Guideline)) for at muliggøre sporbarhed mellem interoperabilitetskrav på højt niveau og detaljerede interoperabilitetskrav.

(3) I betragtning af, at afsendere anvender forskellige meldesystemer, og at de nationale søfartsmiljøer med ét kontaktpunkt gennemføres ved hjælp af forskellige teknologier, bør meldegrænseflademodelet bygge på teknologier, som gør det muligt at udveksle oplysninger mellem forskellige informationssystemer, som anvender en standardiseret protokol, hvilket muliggør større interoperabilitet.

(4) Meldeforpligtelserne i bilaget til forordning (EU) 2019/1239 kan indebære krav om, at klarerne fremsender personoplysninger via meldegrænseflademodulet, som skal udveksle oplysninger på en sådan måde, at personoplysninger behandles i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([2]) og (EU) 2016/679 ([3]).

(5) Da meldegrænseflademodulet er udviklet og opdateres af Kommissionen og distribueres til medlemsstaterne med henblik på integration, bør distributionen af nye versioner af meldegrænseflademodulet, overvågning af, at softwaren installeres korrekt, og ajourføringen af vejledningen til gennemførelse af meddelelser forvaltes centralt, om muligt under hensyntagen til de IT-sikkerhedskrav, der gælder for de nationale søfartsmiljøer med ét kontaktpunkt.

(6) For at garantere meldegrænseflademodulets stabilitet, sikkerhed og ydeevne bør medlemsstaterne kunne overvåge nettrafikken, analysere hændelser, fejl og afvigelser i systemet og integrere disse oplysninger i deres eksisterende overvågningssystemer og -processer. Med henblik herpå bør meldegrænseflademodulet have passende funktioner, som gør det muligt at logge og gemme hændelser og forsyne medlemsstaterne med oplysninger om nettrafikken.

([1]) EUT L 198 af 25.7.2019, s. 64.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

(7) Afsenderne skal autentificeres for at sikre sikker udveksling af oplysninger via meldegrænseflademodulet. Til dette formål bør det fælles brugerregister og adgangsadministrationssystem have en central autentifikationstjeneste og et centralt register som væsentlige komponenter. Disse komponenter bør fungere sammen for at muliggøre autentifikation af afsenderen på tværs af alle meldegrænseflademoduler og således sikre en forenet autentifikationsmekanisme.

(8) For at udveksle oplysninger på sikker vis ved hjælp af meldegrænseflademodulet og sikre, at brugere genkendes på EU-plan, når de tilgår et af meldegrænseflademodulerne, bør afsendere anskaffe et kvalificeret certifikat for elektroniske segl, som overholder de krav, der er fastsat ved Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([4]).

(9) Medlemsstaterne bør være i stand til at registrere afsendere i det centrale register, for at afsendere med blot én enkelt registrering kan udveksle oplysninger via de harmoniserede meldegrænseflader i forskellige medlemsstater. Dette bør mindske den byrde, der er forbundet med adskillige registreringer ved grænseoverskridende operationer i flere nationale søfartsmiljøer med ét kontaktpunkt. Alle personoplysninger i det centrale register bør forvaltes i overensstemmelse med forordning (EU) 2018/1725 og (EU) 2016/679.

(10) For at minimere medlemsstaternes afhængighed af centrale tjenester og i betragtning af, at nationale søfartsmiljøer med ét kontaktpunkt muligvis allerede understøttes af nationale autentifikationstjenester, bør det også være tilladt medlemsstaterne at genbruge deres egne nationale autentifikationstjenester og nationale registre til at autentificere afsendere, som ønsker at benytte meldegrænseflademodulet, som et alternativ til at benytte det brugerregister og adgangsadministrationssystem, som er en del af det europæiske søfartsmiljø med ét kontaktpunkt (EMSWe).

(11) Med henblik på at gøre det muligt for medlemsstaterne at integrere meldegrænseflademodulet, brugerregistret og adgangsadministrationssystemet korrekt i de nationale søfartsmiljøer med ét kontaktpunkt bør denne forordning finde anvendelse fra samme dato som forordning (EU) 2019/1239.

(12) Den Europæiske Tilsynsførende for Databeskyttelse er hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav udtalelse den 18. oktober 2023 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Definitioner

I denne forordning forstås ved:

(1) »meldegrænseflademodul«: en middlewarekomponent i det nationale søfartsmiljø med ét kontaktpunkt, jf. artikel 2, stk. 4, i forordning (EU) 2019/1239

(2) »afsender«: en klarer eller datatjenesteudbyder, som driver det IT-system, der sender elektroniske meddelelser til et nationalt søfartsmiljø med ét kontaktpunkt eller modtager dem via meldegrænseflademodulet

(3) »formalitet«: en formalitet som defineret i artikel 1 i Kommissionens gennemførelsesforordning (EU) 2023/204 ([5])

(4) »AS4«: en meddelelsesprotokol baseret på webtjenester til sikker udveksling af meddelelser mellem to parter

(5) »meddelelse«: en digital gengivelse af formaliteter eller svarmeddelelser, der anvendes til udvekslingen mellem afsenderen og det nationale søfartsmiljø med ét kontaktpunkt

(6) »AS4-adgangspunkt«: en server, der kører software, som er kompatibel med AS4-meddelelsesprotokollen og kravene til meldegrænseflademodulet, og som gør det muligt at sende og modtage oplysninger på vegne af en afsender til og fra meldegrænseflademodulet

([4]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

([5]) Kommissionens gennemførelsesforordning (EU) 2023/204 af 28. oktober 2022 om fastsættelse af tekniske specifikationer, standarder og procedurer for det europæiske søfartsmiljø med ét kontaktpunkt i henhold til Europa-Parlamentets og Rådets forordning (EU) 2019/1239 (EUT L 33 af 3.2.2023, s. 1).

(7) »MNSW-kerne«: en teknisk komponent, hvormed meldegrænseflademodulet er integreret

(8) »syntaksvalidering«: en proces til kontrol af, hvorvidt en elektronisk meddelelse er fri for programmeringsfejl, strukturelle fejl eller stilistiske fejl

(9) »semantisk validering«: en proces til kontrol af, at data overholder specifikke dataregler inden for en formalitet

(10) »vejledning til gennemførelse af meddelelser«: en funktionsspecifikation, hvorved der fastsættes standarder og meddelelser, som skal udveksles mellem afsendere og nationale søfartsmiljøer med ét kontaktpunkt via meldegrænseflademodulet

(11) »registrering«: proces, hvorved en fysisk eller juridisk person identificerer sig og opretter en konto hos den myndighed, der er omhandlet i artikel 12, stk. 2, i forordning (EU) 2019/1239

(12) »identifikation«: en elektronisk identifikation som defineret i artikel 3, nr. 1), i forordning (EU) nr. 910/2014

(13) »elektronisk identifikationsmiddel«: et elektronisk identifikationsmiddel som defineret i artikel 3, nr. 2), i forordning (EU) nr. 910/2014

(14) »autentifikation«: autentifikation som defineret i artikel 3, nr. 5), i forordning (EU) nr. 910/2014

(15) »certifikat«: et kvalificeret certifikat for elektronisk segl som defineret i artikel 3, nr. 30), i forordning (EU) nr. 910/2014 udstedt af en kvalificeret tillidstjenesteudbyder som defineret i artikel 3, nr. 20), i forordning (EU) nr. 910/2014

(16) »EORI-nummer«: et identifikationsnummer som defineret i artikel 1, nr. 18), i Kommissionens delegerede forordning (EU) 2015/2446 ([6])

(17) »EMSWe-brugerregister og adgangsadministrationssystem«: et system, der drives af Kommissionen, og som omfatter et centralt register og en central autentifikationstjeneste og sikrer gensidig anerkendelse af elektroniske identifikationsmidler og autentifikation med henblik på sikker grænseoverskridende dataudveksling mellem afsendere og nationale søfartsmiljøer med ét kontaktpunkt via meldegrænseflademodulet

(18) »centralt register«: et register, der drives af Kommissionen, og som indeholder afsenderes registreringsdata, som stilles til rådighed af medlemsstaterne med henblik på at lette autentifikationen af afsendere

(19) »nationalt register«: et register, der drives af en medlemsstat, og som indeholder afsenderes registreringsdata og kan anvendes til at lette autentifikationen af afsendere, hvis registreret overholder den centrale autentifikationstjenestes krav

(20) »central autentifikationstjeneste«: en tjeneste, der drives af Kommissionen, og som kan anvendes til at autentificere afsendere, der anvender meldegrænseflademodulet

(21) »national autentifikationstjeneste«: en tjeneste, der drives af en medlemsstat, og som kan anvendes til at autentificere afsendere, der anvender meldegrænseflademodulet.

Artikel 2

Meldegrænseflademodulet opfylder de funktionsspecifikationer og tekniske specifikationer, der er fastsat i bilagets del I.

For at hjælpe med at integrere meldegrænseflademodulet i de nationale søfartsmiljøer med ét kontaktpunkt skal Kommissionen i nært samarbejde med de nationale koordinatorer for det europæiske søfartsmiljø med ét kontaktpunkt:

— fastlægge retningslinjerne for test og konfigurering af meldegrænseflademoduler med henblik på integration i de respektive nationale søfartsmiljøer med ét kontaktpunkt

— udarbejde og ajourføre vejledningen til gennemførelse af meddelelser, med bistand fra Det Europæiske Agentur for Søfartssikkerhed.

([6]) Kommissionens delegerede forordning (EU) 2015/2446 af 28. juli 2015 til supplering af Europa-Parlamentets og Rådets forordning (EU) nr. 952/2013 med nærmere regler angående visse bestemmelser i EU-toldkodeksen (EUT L 343 af 29.12.2015, s. 1).

Artikel 3

Det centrale register og den centrale autentifikationstjeneste oprettes i overensstemmelse med de tekniske specifikationer, standarder og procedurer, der er fastsat i bilagets del II.

Artikel 4

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den finder anvendelse fra den 15. august 2025.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 14. december 2023.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

DEL I

MELDEGRÆNSEFLADEMODUL

ARKITEKTUR OG ANVENDELSESOMRÅDE

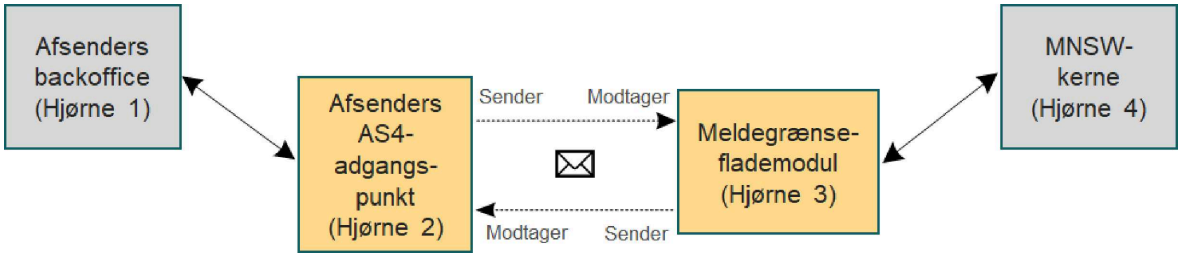
Meldegrænsefladem odulet er en del af en model med fire hjørner til brug for de meddelelser, som udveksles mellem afsendere (hjørne 1) og MNSW-kernen (hjørne 4) og formidles via AS4-adgangspunkter (hjørne 2 og 3) på hver side, der implementerer AS4-protokollen for transport og sikkerhed som følger:

Hjørne 1:afsenders backoffice, som forbereder og sender meddelelser til og modtager dem fra MNSW-kernen

Hjørne 2: afsenders AS4-adgangspunkt

Hjørne 3: meldegrænsefladem odul

Hjørne 4: MNSW-kernen modtager meddelelserne og sender svarmeddelelser til afsenderen.



Figur 1 — Meldegrænsefladem odulets arkitektur på højt niveau

Meldegrænsefladem odulet udfører ingen semantisk validering af meddelelser udover, hvad der er angivet i vejledningen til gennemførelse af meddelelser, og det håndterer heller ikke meddelelsernes rangfølge eller gemmer dem længere, end til overførslen til MNSW-kernen eller afsenderen er afsluttet.

I overensstemmelse med artikel 5, stk. 3, litra c), i forordning (EU) 2019/1239 skal medlemsstaterne, når en meddelelse er overført fra meldegrænsefladem odulet til MNSW-kernen, i givet fald oversætte, validere og overføre formalitetsdataene til de relevante myndigheders systemer i overensstemmelse med disse systemers specifikationer.

FUNKTIONSSPECIFIKATIONER FOR MELDEGRÆNSEFLADEMODULET

ID	Funktion	Beskrivelse
LR1	Logning og overvågning	Funktionen skal sikre logning og opbevaring af hændelser (manglende levering, forsinkelser samt fejl hos modtageren).
LR2	Opbevaring af metadata	Funktionen skal sikre opbevaring af udvekslede meddelelsers metadata.
OA1	Opbevaring af og opslag i tekniske data	Funktionen skal sikre opbevaring af og opslag i tekniske data, som er nødvendige for meldegrænsefladem odulets konfigurering og funktion via en grænseflade (f.eks. tekniske adresser på afsendernes AS4-adgangspunkter, meddelelsesskemaer for vejledningen til gennemførelse af meddelelser, osv.).
OA2	Håndtering af afvigelser	Funktionen skal udløse notifikationer om konstaterede databehandlingsfejl og/eller unormale forhold via en brugergrænseflade.
OA3	Adgang til logning og overvågning af oplysninger og metadata	Funktionen skal give MNSW-kernen adgang til oplysninger om logning og overvågning og til udvekslede meddelelsers metadata via en system-system-grænseflade.

OA4	Autentifikation af afsenderen	Funktionen skal igangsætte processen med autentifikation af en afsender ved hjælp af en central eller national autentifikationstjeneste.
OA5	Validering af meddelelser	Funktionen skal udføre syntaksvalidering og semantisk validering af modtagne meddelelser i overensstemmelse med de tekniske meddelelsesspecifikationer, der er defineret i vejledningen til gennemførelse af meddelelser. I vejledningen til gennemførelse af meddelelser skal det angives nærmere, hvilke valideringer der skal udføres af meldegrænseflademodulet. Meldegrænseflademodulet skal udløse en notifikation ved fejl i overensstemmelse hermed.
MF1	Håndtering af meddelelser	Funktionen skal sikre, at indholdet af de modtagne meddelelser (formalitet eller svar) overføres uden ændringer til det relevante hjørne, hvis valideringerne er gennemført korrekt.

TEKNISKE SPECIFIKATIONER FOR MELDEGRÆNSEFLADEMODULET

Integration

ID	Navn	Beskrivelse
IA1.	Meddelelsesprotokolstandard	Meldegrænseflademodulet skal anvende en AS4-meddelelsesprotokol for at lette interoperabiliteten med afsendernes forskellige teknologier og meldesystemer.

Udveksling af meddelelser

ID	Navn	Beskrivelse
AP1.	Asynkront meddelelsesudvekslingsmønster	Meldegrænseflademodulet skal understøtte asynkron overførsel af meddelelser til og fra (formalitet og svar) MNSW-kernen ved hjælp af en »push and pull«-mekanisme.

Sikkerhed

ID	Navn	Beskrivelse
SA1.	Fortrolighed og sikkerhed i forbindelse med udveksling af oplysninger	Meldegrænseflademodulet skal sikre oplysningernes fortrolighed og beskytte personoplysninger, som udveksles, ved at kryptere de oplysninger, der udveksles mellem afsenderens AS4-adgangspunkt og meldegrænseflademodulet. Meldegrænseflademodulet skal dekryptere de meddelelser, der er sendt af en afsender, og gøre dem tilgængelige for MNSW-kernen. Meldegrænseflademodulet skal anvende Web Service Security (WSS) som standard for at muliggøre sikker udveksling af meddelelser mellem afsenderens AS4-adgangspunkt og meldegrænseflademodulet.
SA2.	Meddelelsers uafviselighed	Kommunikationen og valideringen af meddelelser via meldegrænseflademodulet skal omfatte sikkerhedsforanstaltninger til at sikre meddelelsernes ægthed og undgå, at meddelelser afvises.

SA3.	Integritet	Der skal træffes tekniske foranstaltninger for at sikre integriteten af de data, der udveksles.
SA4.	Applikationssikkerhed	Meldegrænseflademodulet skal bygge på bedste praksis for softwareudvikling, som gør det muligt at afsløre ondsindede aktiviteter, og som muliggør sikker overførsel af følsomme oplysninger.
SA5.	Tjenesternes tilgængelighed	Med henblik på at sikre pålidelig kommunikation og distribution af oplysninger mellem afsendere og nationale søfartsmiljøer med ét kontaktpunkt skal meldegrænseflademodulet have implementeret mekanismer, som sikrer, at meddelelser, der udveksles med meldegrænseflademodulet, ikke går tabt, hvis tjenesten ikke er tilgængelig.

Ydeevne og skalerbarhed

ID	Navn	Beskrivelse
PS1.	Ydeevne og skalerbarhed	Meldegrænseflademodulet skal være i stand til at nå eksisterende og fremtidige mål for ydeevne, herunder svartid, antallet af samtidige afsendere og de udvekslede meddelelsers antal/størrelse.

Portabilitet og udrulning

ID	Navn	Beskrivelse
PD1.	Platformens uafhængighed	Meldegrænseflademodulet skal være kompatibelt med den hardwarearkitektur og de operativsystemer, der er mest almindelige, hvor meldegrænseflademodulet tages i anvendelse. Installation eller konfigurering af meldegrænseflademodulet bør ikke kræve beskyttet hardware eller software.
PD2	Selvinstallerende applikation	Meldegrænseflademodulet skal leveres som en softwarepakke, som omfatter alle de applikationskomponenter, som meldegrænseflademodulet kræver. De leverede og krævede afhængigheder skal angives i hver versionsbeskrivelse for meldegrænseflademodulet.

DEL II

EMSWE-BRUGERREGISTER OG ADGANGSADMINISTRATIONSSYSTEM

DET CENTRALE REGISTER

På anmodning fra afsenderen skal medlemsstater, der ikke stiller et nationalt register til rådighed, som er i overensstemmelse med de i dette bilag anførte specifikationer for det centrale register, registrere EORI-nummeret og afsenderens certifikat i det centrale register og være ansvarlige for verifikationen, nøjagtigheden og administrationen af dataene i overensstemmelse med artikel 12, stk. 2, i forordning (EU) 2019/1239. Det centrale register skal stille en grænseflade til rådighed for medlemsstaterne til at udføre registreringen og administrationen af afsenderne.

DEN CENTRALE AUTENTICERINGSTJENESTE

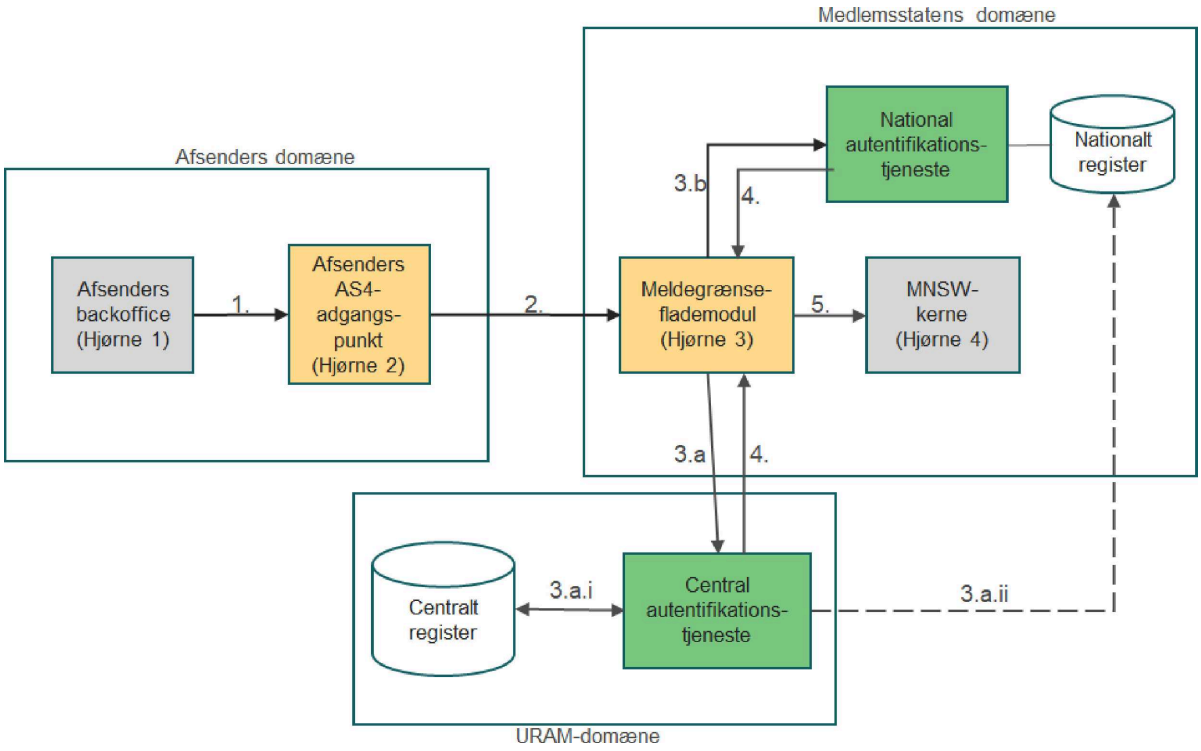
Nedenstående diagram viser de sekventielle trin for autentifikation af en afsender, som udarbejder og sender en meddelelse til meldegrænseflademodulet (trin 1 og 2).

Meldegrænseflademodulet skal udføre funktionen »autentifikation af afsenderen« ([1]) ved hjælp af den centrale autentifikationstjeneste (trin 3.a).

Trin 3.a: Den centrale autentifikationstjeneste skal autentificere afsenderen ved at søge i det centrale register og kontrollere den relevante registrering (trin 3.a.i) eller, hvis afsenderen ikke findes i det centrale register, ved at søge i det nationale register i afsenderens land, hvis dette er tilgængeligt, og kontrollerer den relevante registrering (trin 3.a.ii).

Trin 3.b: Hvis en national autentifikationstjeneste er oprettet og gjort tilgængelig i en medlemsstat, skal meldegrænseflademodulet udføre funktionen »autentifikation af afsenderen« og kun benytte den nationale autentifikationstjeneste til autentifikation af afsendere, der anvender et certifikat udstedt i den pågældende medlemsstat.

Trin 4: Resultatet af autentifikationen skal sendes tilbage til meldegrænseflademodulet. Hvis autentifikationen lykkes, skal meddelelsen gøres tilgængelig for hjørne 4 (MNSW-kernen) (trin 5). Hvis autentifikationen ikke lykkes, skal en fejlmeddelelse sendes tilbage til hjørne 2.



Figur 2

TEKNISKE SPECIFIKATIONER FOR URAM

Integration

ID	Navn	Beskrivelse
URAM.01	Interoperable standarder	URAM-softwaren skal følge standardprotokoller og anvende robuste sikkerhedsfunktioner, når den eksponerer sine grænseflader og integreres med andre komponenter.

([1]) Angivet som OA4 i afsnittet om de funktionsspecifikationer for meldegrænseflademodulet i dette bilags del I.

URAM.02	Efterlevelse af eIDAS-forordningen	URAM-softwaren skal gøre brug af åbne EU-standarder og -løsninger og implementere de nødvendige mekanismer til kontrol af afsenderens certifikater mod de positivlister, medlemsstaterne offentliggør i overensstemmelse med artikel 22 i forordning (EU) nr. 910/2014 og Kommissionens gennemførelsesafgørelse (EU) 2015/1505 ([2]), herunder oplysninger vedrørende kvalificerede tillidstjenesteudbydere, som udsteder certifikater til brug i forbindelse med elektroniske segl.

Sikkerhed

ID	Navn	Beskrivelse
URAM.03	Fortrolighed i forbindelse med udveksling af oplysninger	For at tilgodese sikkerheden i forbindelse med URAM-softwaren og udveksling af personoplysninger skal følgende protokoller og krypteringsmetoder implementeres: — Transport Layer Security (TLS): Al software i URAM skal sikres ved brug af TLS med henblik på kryptering af data og disses integritet på netværksniveau og bidrage til at beskytte data under overførsel, således at uautoriseret adgang og manipulation forhindres. — For at kommunikere med URAM-softwaren skal der foretages en TLS-konfigurering.
URAM.04	Applikationssikkerhed	URAM-softwaren skal garantere opdagelse af ondsindede aktiviteter samt sikker overførsel af følsomme oplysninger.
URAM.05	Beskyttelse af personoplysninger	Medlemsstaternes myndigheder skal tildeles adgangsrettigheder i overensstemmelse med artikel 12, stk. 2, i forordning (EU) 2019/1239 med henblik på at registrere afsendere. URAM-softwaren skal implementere adgangskontrolmekanismer for at sikre beskyttelse af brugeroplysninger, som er personoplysninger, og som udelukkende skal behandles for at oprette brugerkonti og administrere de dertil svarende adgangsrettigheder. Den centrale autentifikationstjeneste skal ikke opbevare afsendernes personoplysninger længere, end hvad der er nødvendigt for at udføre autentifikationen. Det centrale register skal ikke opbevare afsendernes personoplysninger længere, end hvad der er nødvendigt for administrationen af kontoen.

Holdbarhed og flytbarhed

ID	Navn	Beskrivelse
URAM.06	Teknologisk uafhængighed	URAM-softwaren skal muliggøre interaktioner med meldegrænseflademodulet og andre relevante tjenester, uden at der er behov for beskyttet software eller hardware, og URAM-softwaren skal muliggøre integration med meldegrænseflademodulet, uanset hvilket teknologisk miljø meldegrænseflademodulet tages i anvendelse i.

([2]) Kommissionens gennemførelsesafgørelse (EU) 2015/1505 af 8. september 2015 om fastlæggelse af tekniske specifikationer og formater for positivlister i henhold til artikel 22, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 235 af 9.9.2015, s. 26).

URAM.07	Uafhængig udrulning	URAM-softwaren må ikke medføre, at der stilles særlige krav til meldegrænseflademodulet i forbindelse med udrulning. Meldegrænseflademodulet bør kun sikre internetkonnektivitet og efterlevelse af standarder vedrørende URAM-softwarens sikkerhed og protokoller.

Den centrale autentifikationstjenestes funktioner

Den centrale autentifikationstjeneste skal stille følgende tjenester til rådighed for meldegrænseflademodulet:

ID	Navn	Beskrivelse
URAM.08	Autentifikationstjeneste	Den centrale autentifikationstjeneste er ansvarlig for autentifikation af afsendere ved at verificere certifikatets gyldighed, EORI-nummeret og forbindelsen mellem afsenderens EORI-nummer og certifikat. Den centrale autentifikationstjeneste behandler anmodninger fremsendt af meldegrænseflademodulet og afgiver svar, hvoraf det fremgår, om autentifikationen er lykkedes eller ej.

Specifikationer for det centrale register

ID	Navn	Beskrivelse
URAM.09	Registrering af afsendere	Det centrale register skal stille en grafisk brugergrænseflade til rådighed for medlemsstaterne til registrering af afsendernes data. Når en afsender er registreret i det centrale register, skal den pågældende være registreret i alle medlemsstater.
URAM.10	Visning af og søgning efter afsendere	Det centrale register skal gøre det muligt for en medlemsstat at se alle data vedrørende de afsendere, som den tidligere har registreret. Det skal også stille en søgefunktion til rådighed, som gør det muligt at hente data vedrørende de afsendere, medlemsstaten har registreret, på grundlag af forskellige søgekriterier.
URAM.11	Opdatering af afsendere	Det centrale register skal gøre det muligt for en medlemsstat at ændre alle dens tidligere registrerede afsenderes data for at sikre dataenes nøjagtighed og gyldighed.
URAM.12	Deaktivering af afsendere	Det centrale register skal gøre det muligt for en medlemsstat af deaktivere sine tidligere registrerede afsendere.
URAM.13	Revision og rapportering	Det centrale register skal have en rapporteringsmulighed, som sætter en medlemsstat i stand til at analysere sine tidligere registrerede afsenderes data, f.eks. registreringsdato og certifikatgyldighed.
URAM.14	Notifikationer	Det centrale register skal give medlemsstaterne mulighed for at modtage en notifikation fra det centrale register, hver gang en afsender, der tidligere er registreret af den pågældende medlemsstat, registreres, opdateres eller deaktiveres, og hver gang afsenderens certifikat udløber.