

KOMMISJONENS GJENNOMFØRINGSFORORDNING (EU) 2023/2790**av 14. desember 2023****om fastsettelse av funksjonsspesifikasjoner og tekniske spesifikasjoner for rapporteringsgrensesnittmodulen i de nasjonale rapporteringspunktene for sjøfart**

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsforordning (EU) 2019/1239 av 20. juni 2019 om opprettelse av et europeisk miljø for rapportering fra skip og om oppheving av direktiv 2010/65/EU⁽¹⁾, særlig artikkel 6 nr. 1 og artikkel 12 nr. 4,

etter samråd med komiteen for digital tilrettelegging for transport og handel og

ut fra følgende betraktninger:

- 1) Spesifikasjonene for rapporteringsgrensesnittmodulen bør bygge på en teknologi som er lett tilgjengelig, lett å installere og lett å integrere i alle nasjonale rapporteringspunkter for sjøfart, og bør muliggjøre jevn integrering og vedlikehold i framtiden.
- 2) Funksjonsspesifikasjonene og de tekniske spesifikasjonene for rapporteringsgrensesnittmodulen bør bygge på retningslinjene for HL SAT (High Level Interoperability Requirements Solution Architecture Template) for å muliggjøre sporbarhet mellom høye og detaljerte interoperabilitetskrav.
- 3) Tatt i betraktning at avsendere bruker forskjellige rapporteringssystemer, og at de nasjonale rapporteringspunktene for sjøfart gjennomføres ved hjelp av forskjellige teknologier, bør rapporteringsgrensesnittmodulen bygge på teknologier som gjør det mulig å utveksle informasjon mellom forskjellige informasjonssystemer som bruker en standardisert protokoll, noe som muliggjør større interoperabilitet.
- 4) Rapporteringspliktene oppført i vedlegget til forordning (EU) 2019/1239 kan kreve at deklaranten sender inn personopplysninger gjennom rapporteringsgrensesnittmodulen, som skal utveksle informasjonen på en slik måte at personopplysninger behandles i samsvar med europaparlaments- og rådsforordning (EU) 2018/1725⁽²⁾ og europaparlaments- og rådsforordning (EU) 2016/679⁽³⁾.
- 5) Etter hvert som rapporteringsgrensesnittmodulen utvikles og oppdateres av Kommisjonen og distribueres til medlemsstatene for integrering, bør distribusjon av nye versjoner av rapporteringsgrensesnittmodulen, overvåking av korrekt installering av programvaren og oppdatering av meldingsimplementeringsveiledningen bør administreres sentralt, idet det tas hensyn til IT-sikkerhetskravene til de nasjonale rapporteringspunktene for sjøfart der det er mulig.
- 6) For å sikre rapporteringsgrensesnittmodulens stabilitet, sikkerhet og ytelse bør medlemsstatene kunne overvåke nettverkstrafikk og analysere systemhendelser, -feil og -unntak samt integrere denne informasjonen i sine eksisterende overvåkingssystemer og -prosesser. For å oppnå dette bør rapporteringsgrensesnittmodulen sørge for egnet funksjonalitet som gjør det mulig å logge og lagre hendelser samt gi informasjon om nettverkstrafikken til medlemsstatene.

⁽¹⁾ EUT L 198 av 25.7.2019, s. 64.

⁽²⁾ Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger samt om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

⁽³⁾ Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

- 7) For å sikre sikker informasjonsutveksling gjennom rapporteringsgrensesnittmodulen må avsenderne autentiseres. For dette formålet bør det felles brukerregisteret og tilgangsadministrasjonssystemet ha en sentral autentiseringstjeneste og et sentralt register som nøkkelkomponenter. Disse komponentene bør sammen bidra til å muliggjøre avsenderautentisering på tvers av alle rapporteringsgrensesnittmoduler, noe som gir en enhetlig autentiseringsmekanisme.
- 8) For å utveksle informasjon på en sikker måte ved bruk av rapporteringsgrensesnittmodulen og sikre at brukerne gjenkjennes på EU-nivå når de får tilgang til noen av rapporteringsgrensesnittmodulene, bør avsendere innhente et kvalifisert sertifikat for elektroniske segl som overholder kravene fastsatt i europaparlaments- og rådsforordning (EU) nr. 910/2014⁽⁴⁾.
- 9) For å sikre at avsendere kan utveksle informasjon gjennom de harmoniserte rapporteringsgrensesnittene i ulike medlemsstater med bare én registrering, bør medlemsstatene kunne registrere avsendere i det sentrale registeret. Dette bør redusere byrden med flere registreringer for grensekryssende virksomhet i flere nasjonale rapporteringspunkter for sjøfart. Alle personopplysninger i sentralregisteret skal behandles i samsvar med forordning (EU) 2018/1725 og (EU) 2016/679.
- 10) For å minimere medlemsstatenes avhengighet av sentrale tjenester, og med tanke på at nasjonale rapporteringspunkter for sjøfart allerede kan støttes av nasjonale autentiseringstjenester, bør medlemsstatene også kunne gjenbruke sine egne nasjonale autentiseringstjenester og nasjonale registre for å autentisere avsendere som ønsker å bruke rapporteringsgrensesnittmodulen, som et alternativ til brukerregisteret og tilgangsadministrasjonssystemet i det europeiske miljøet for rapportering fra skip.
- 11) For at medlemsstatene skal kunne integrere rapporteringsgrensesnittmodulen, brukerregisteret og tilgangsadministrasjonssystemet på riktig måte med de nasjonale rapporteringspunktene for sjøfart, bør denne forordningen få anvendelse fra samme dato som forordning (EU) 2019/1239.
- 12) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 42 nr. 1 i forordning (EU) 2018/1725 og avga uttalelse 18. oktober 2023.

VEDTATT DENNE FORORDNINGEN:

Artikkel 1

Definisjoner

I denne forordningen menes med

- 1) «rapporteringsgrensesnittmodul» en mellomvarekomponent i det nasjonale rapporteringspunktet for sjøfart nevnt i artikkel 2 nr. 4 i forordning (EU) 2019/1239,
- 2) «avsender» en deklarant eller datatjenesteleverandør som driver IT-systemet som sender elektroniske meldinger til det nasjonale rapporteringspunktet for sjøfart eller mottar dem via rapporteringsgrensesnittmodulen,
- 3) «formalitet» en formalitet som definert i artikkel 1 i Kommisjonens gjennomføringsforordning (EU) 2023/204⁽⁵⁾,
- 4) «AS4» en meldingsprotokoll basert på netjtjenester for sikker utveksling av meldinger mellom to parter,
- 5) «melding» en digital representasjon av formaliteter eller svarmeldinger som brukes til utveksling mellom avsenderen og det nasjonale rapporteringspunktet for sjøfart,
- 6) «AS4-tilgangspunkt» en server som kjører programvare som er kompatibel med meldingsprotokollen AS4 og kravene til rapporteringsgrensesnittmodulen, slik at det er mulig å sende og motta informasjon på vegne av en avsender fra og til rapporteringsgrensesnittmodulen,

⁽⁴⁾ Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF (EUT L 257 av 28.8.2014, s. 73).

⁽⁵⁾ Kommisjonens gjennomføringsforordning (EU) 2023/204 av 28. oktober 2022 om fastsettelse av tekniske spesifikasjoner, standarder og prosedyrer for det europeiske miljøet for rapportering fra skip i samsvar med europaparlaments- og rådsforordning (EU) 2019/1239 (EUT L 33 av 3.2.2023, s. 1).

- 7) «kjerne i det nasjonale rapporteringspunktet for sjøfart» en teknisk komponent for det nasjonale rapporteringspunktet for sjøfart som rapporteringsgrensesnittmodulen er integrert med,
- 8) «syntaksvalidering» prosessen med å kontrollere om en elektronisk melding er fri for programmerings-, struktur- eller stilfeil,
- 9) «semantisk validering» en prosess der det kontrolleres at data overholder spesifikke dataregler innenfor en formalitet,
- 10) «meldingsimplementeringsveiledning» en funksjonsspesifikasjon som fastsetter standarder og meldinger som skal utveksles mellom avsendere og nasjonale rapporteringspunkter for sjøfart gjennom rapporteringsgrensesnittmodulen,
- 11) «registrering» en prosess der en fysisk eller juridisk person identifiserer seg og oppretter en konto hos myndigheten nevnt i artikkel 12 nr. 2 i forordning (EU) 2019/1239,
- 12) «identifikasjon» elektronisk identifikasjon som definert i artikkel 3 nr. 1 i forordning (EU) 910/2014,
- 13) «elektronisk identifikasjonsmiddel» elektronisk identifikasjon som definert i artikkel 3 nr. 2 i forordning (EU) 910/2014,
- 14) «autentisering» autentisering som definert i artikkel 3 nr. 5 i forordning (EU) nr. 910/2014,
- 15) «sertifikat» et kvalifisert sertifikat for elektronisk segl som definert i artikkel 3 nr. 30 i forordning (EU) nr. 910/2014 utstedt av en kvalifisert tilbyder av tillitstjenester som definert i artikkel 3 nr. 20 i forordning (EU) nr. 910/2014,
- 16) «EORI-nummer» et identifikasjonsnummer som definert i artikkel 1 nr. 18 i delegert kommisjonsforordning (EU) 2015/2446⁽⁶⁾,
- 17) «brukerregisteret og tilgangsadministrasjonssystemet i det europeiske miljøet for rapportering fra skip» et system som drives av Kommisjonen, og som omfatter et sentralt register og en sentral autentiseringstjeneste, som sikrer gjensidig anerkjennelse av elektroniske identifikasjonsmidler og autentisering for sikker grensekryssende datautveksling mellom avsendere og nasjonale rapporteringspunkter for sjøfart gjennom rapporteringsgrensesnittmodulen,
- 18) «sentralt register» et register som drives av Kommisjonen og inneholder avsenderregistreringsdata fra medlemsstatene med det formål å lette autentiseringen av avsenderne,
- 19) «nasjonalt register» et register som drives av en medlemsstat, og som inneholder avsendernes registreringsdata og kan brukes til å lette autentiseringen av avsenderne, forutsatt at det oppfyller kravene i den sentrale autentiseringstjenesten,
- 20) «sentral autentiseringstjeneste» en tjeneste som drives av Kommisjonen, og som autentiserer avsendere som bruker rapporteringsgrensesnittmodulen,
- 21) «nasjonal autentiseringstjeneste» en tjeneste som drives av en medlemsstat, og som kan brukes til å autentisere avsendere som bruker rapporteringsgrensesnittmodulen.

Artikkel 2

Rapporteringsgrensesnittmodulen skal overholde funksjonsspesifikasjonene og de tekniske spesifikasjonene som er fastsatt i del I i vedlegget.

For å bidra til å integrere rapporteringsgrensesnittmodulen i de nasjonale rapporteringspunktene for sjøfart skal Kommisjonen, i nært samarbeid med de nasjonale koordinatorene for det europeiske miljøet for rapportering fra skip,

- fastsette retningslinjer for testing og konfigurering av rapporteringsgrensesnittmodulen for integrering i de respektive nasjonale rapporteringspunktene for sjøfart,
- fastsette og vedlikeholde, med bistand fra Det europeiske sjøsikkerhetsbyrå, meldingsimplementeringsveiledningen.

⁽⁶⁾ Delegert kommisjonsforordning (EU) 2015/2446 av 28. juli 2015 om utfylling av europaparlaments- og rådsforordning (EU) nr. 952/2013 med hensyn til nærmere regler for visse bestemmelser i Unionens tollkodeks (EUT L 343 av 29.12.2015, s. 1).

Artikkel 3

Det sentrale registeret og den sentrale autentiseringstjenesten skal opprettes i samsvar med de tekniske spesifikasjonene, standardene og framgangsmåtene som er fastsatt i del II i vedlegget.

Artikkel 4

Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Den får anvendelse fra 15. august 2025.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 14. desember 2023.

For Kommisjonen

Ursula VON DER LEYEN

President

VEDLEGG

DEL I

RAPPORTERINGSGRENSESNITTMODUL**ARKITEKTUR OG BRUKSOMRÅDE**

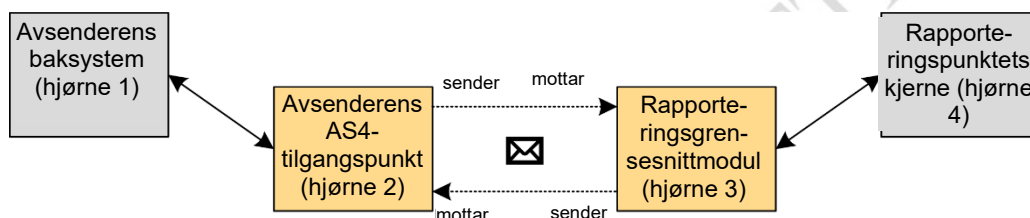
Rapporteringsgrensesnittmodulen er en del av en modell med fire hjørner for meldingene som utveksles mellom avsenderne (hjørne 1) og rapporteringspunktets kjerne (hjørne 4) og formidles gjennom AS4-tilgangspunkter (hjørne 2 og 3) på hver side, idet AS4-protokollen for transport og sikkerhet implementeres som følger:

Hjørne 1: Avsenderens baksystem forbereder, sender og mottar meldingene fra og til rapporteringspunktets kjerne.

Hjørne 2: Avsenderens AS4-tilgangspunkt.

Hjørne 3: Rapporteringsgrensesnittmodul

Hjørne 4: Rapporteringspunktets kjerne som mottar meldingene og sender svarmeldinger til avsenderen.



Figur 1 – Høynivåarkitektur for rapporteringsgrensesnittmodul

Rapporteringsgrensesnittmodulen skal ikke utføre semantisk validering av meldinger utover spesifikasjonene i meldingsimplementeringsveiledningen, håndtere deres sekvens eller lagre meldinger etter at de har blitt korrekt overført til rapporteringspunktets kjerne eller avsenderen.

I samsvar med artikkel 5 nr. 3 bokstav c) i forordning (EU) 2019/1239 skal medlemsstatene eventuelt, når meldingen er overført fra rapporteringsgrensesnittmodulen til rapporteringspunktets kjerne, oversette, validere og overføre formalitetsdataene til de relevante myndighetenes systemer i samsvar med spesifikasjonene for disse systemene.

FUNKSJONSSPESIFIKASJONER FOR RAPPORTERINGSGRENSESNITTMODULEN

ID	Stilling	Beskrivelse
LR1	Logging og overvåking	Funksjonen skal sikre logging og lagring av hendelser (leveringsfeil, forsinkelser og mottakerfeil).
LR2	Lagring av metadata	Funksjonen skal sikre lagring av metadata for utvekslede meldinger.
OA1	Lagring av og oppslag i tekniske data	Funksjonen skal sikre lagring av og oppslag i tekniske data som kreves for at rapporteringsgrensesnittmodulen skal kunne konfigureres og fungere gjennom et grensesnitt (f.eks. tekniske adresser til avsenderens AS4-tilgangspunkter, meldingsskjemaer for meldingsimplementeringsveiledningen osv.).
OA2	Håndtering av unntak	Funksjonen skal gi varsler om fastslåtte behandlingsfeil og/eller uregelmessige forhold gjennom et brukergrensesnitt.
OA3	Tilgang til loggings- og overvåkingsinformasjon og metadata	Funksjonen skal gi rapporteringspunktets kjerne tilgang til loggings- og overvåkingsinformasjon og metadata for utvekslede meldinger gjennom et system-til-system-grensesnitt.

OA4	Autentisering av avsender	Funksjonen skal utløse autentiseringsprosessen for en avsender ved hjelp av en sentral eller nasjonal autentiseringstjeneste.
OA5	Meldingsvalidering	Funksjonen skal utføre syntaksvalidering og semantisk validering av mottatte meldinger i samsvar med de tekniske meldingsspesifikasjonene som er definert i meldingsimplementeringsveiledningen. Meldingsimplementeringsveiledningen skal angi hvilke valideringer som skal utføres av rapporteringsgrensesnittmodulen. Rapporteringsgrensesnittmodulen skal varsle om feil i tråd med dette.
MF1	Meldingshåndtering	Funksjonen skal sikre at innholdet i de mottatte meldingene (formalitet eller svar) overføres uten endringer til relevant hjørne dersom valideringene har vært vellykket.

TEKNISKE SPESIFIKASJONER FOR RAPPORTERINGSGRENSENITTMODULEN

Integrering

ID	Navn	Beskrivelse
IA1.	Standard for meldingsprotokoll	Rapporteringsgrensesnittmodulen skal bruke meldingsprotokollen AS4 for å lette interoperabiliteten med ulike teknologier og rapporteringssystemer for avsendere.

Meldingsutveksling

ID	Navn	Beskrivelse
AP1.	Asynkront meldingsutvekslingsmønster	Rapporteringsgrensesnittmodulen skal støtte asynkron overføring av meldinger til og fra (formalitet og svar) rapporteringssystemets kjerne med push-and-pull-mekanismen.

Sikkerhet

ID	Navn	Beskrivelse
SA1.	Fortrolighet og sikkerhet ved informasjonsutveksling	Rapporteringsgrensesnittmodulen skal sikre informasjonsfortrolighet og beskytte personopplysninger som utveksles, ved å kryptere informasjonen som utveksles mellom avsenderens AS4-tilgangspunkt og rapporteringsgrensesnittmodulen. Rapporteringsgrensesnittmodulen skal dekryptere de meldingene en avsender sender, og gjøre dem tilgjengelige for rapporteringssystemets kjerne. Rapporteringsgrensesnittmodulen skal bruke en WSS-standard (Web Service Security) for å muliggjøre sikker utveksling av meldinger mellom avsenderens AS4-tilgangspunkt og rapporteringsgrensesnittmodulen.
SA2.	Meldingers uavviselighet	Kommunikasjon og validering av meldinger via rapporteringsgrensesnittmodulen skal inkludere sikkerhetstiltak for å sikre meldingens autentisitet og unngå at meldinger avvises.

SA3.	Integritet	Det skal innføres tekniske tiltak for å sikre integriteten til dataene som utveksles.
SA4.	Applikasjonssikkerhet	Rapporteringsgrensesnittmodulen skal bygge på beste praksis for programvareutvikling som gjør det mulig å oppdage skadelige aktiviteter, og på sikker overføring av sensitiv informasjon.
SA5.	Tjenestenes tilgjengelighet	For pålitelig kommunikasjon og distribusjon av informasjon mellom avsendere og nasjonale rapporteringspunkter for sjøfart skal rapporteringsgrensesnittmodulen implementere mekanismer som sikrer at meldinger som utveksles med rapporteringsgrensesnittmodulen, ikke går tapt ved manglende tjenestetilgjengelighet.

Ytelse og skalerbarhet

ID	Navn	Beskrivelse
PS1.	Ytelse og skalerbarhet	Rapporteringsgrensesnittmodulen skal kunne nå eksisterende og framtidige ytelsesmål som responstid, antall samtidige avsendere og mengde/størrelse på utvekslede meldinger.

Overførbarhet og ibruktaking

ID	Navn	Beskrivelse
PD1.	Plattformuavhengighet	Rapporteringsgrensesnittmodulen skal være kompatibel med den vanligste maskinvarearkitekturen og de vanligste operativsystemene der rapporteringsgrensesnittmodulen skal distribueres. Rapporteringsgrensesnittmodulen bør ikke kreve proprietær maskinvare eller programvare for installering eller konfigurering.
PD2	Selvinstallerende applikasjon	Rapporteringsgrensesnittmodulen skal leveres som en programvarepakke som inneholder alle de programkomponentene som rapporteringsgrensesnittmodulen krever. De leverte og påkrevde avhengighetene skal angis i hver versjonsbeskrivelse for rapporteringsgrensesnittmodulen.

DEL II

SYSTEM FOR BRUKERREGISTER OG TILGANGSADMINISTRASJON FOR DET EUROPEISKE MILJØET FOR RAPPORTERING AV SKIP

SENTRALT REGISTER

På anmodning fra avsenderen skal medlemsstater som ikke har et nasjonalt register som er i samsvar med spesifikasjonene for det sentrale registret i dette vedlegget, registrere EORI-nummeret og avsenderens sertifikat i det sentrale registret, og de er ansvarlige for verifisering, nøyaktighet og administrasjon av data i samsvar med artikkel 12 nr. 2 i forordning (EU) 2019/1239. Det sentrale registeret skal gi medlemsstatene et grensesnitt for å utføre registrering og administrasjonen av avsendere.

SENTRAL AUTENTISERINGSTJENESTE

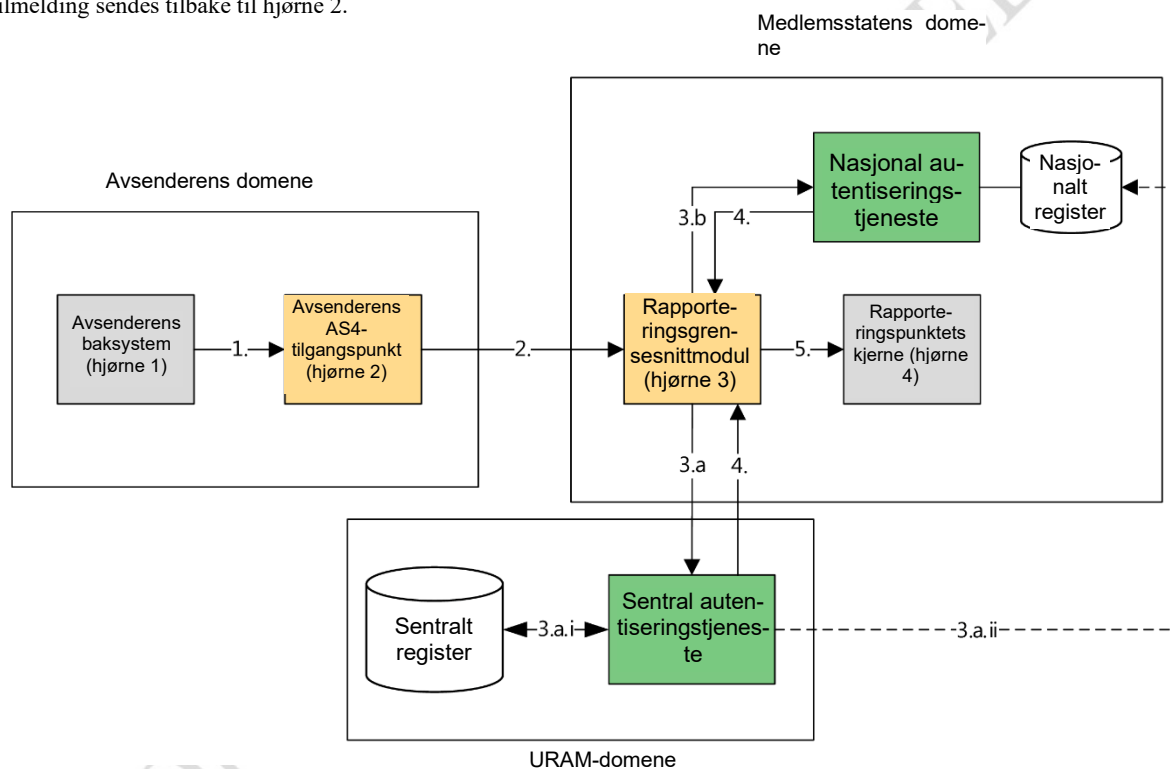
Diagrammet nedenfor illustrerer sekvensen av trinn for å autentisere en avsender som utarbeider og sender en melding til rapporteringsgrensesnittmodulen (trinn 1, 2).

Rapporteringsgrensesnittmodulen skal utøve funksjonen «avsenderautentisering»⁽¹⁾ ved bruk av den sentrale autentiseringstjenesten (trinn 3.a).

Trinn 3a: Den sentrale autentiseringstjenesten skal autentisere avsenderen ved å søke i det sentrale registret og kontrollere den relevante posten (3.a.i) eller, dersom avsenderen ikke finnes i det sentrale registret, ved å søke i det nasjonale registret i avsenderens land, dersom det er tilgjengelig, og kontrollere den relevante posten (trinn 3.a.ii).

Trinn 3.b: Dersom en nasjonal autentiseringstjeneste er etablert og gjort tilgjengelig i en medlemsstat, skal rapporteringsgrensesnittmodulen utøve funksjonen «avsenderautentisering» ved bruk av denne nasjonale autentiseringstjenesten bare for autentisering av avsendere ved bruk av et sertifikat utstedt i denne medlemsstaten.

Trinn 4: Resultatet av autentiseringen skal sendes tilbake til rapporteringsgrensesnittmodulen. Ved vellykket autentisering skal meldingen gjøres tilgjengelig i hjørne 4 (rapporteringpunktets kjerne) (trinn 5). Dersom autentiseringen mislykkes, skal en feilmelding sendes tilbake til hjørne 2.



Figur 2

TEKNISKE SPESIFIKASJONER FOR URAM

Integrering

ID	Navn	Beskrivelse
URAM.01	Interoperabilitetsstandarder	URAM-programvaren skal overholde standardprotokoller og bruke robuste sikkerhetsfunksjoner når grensesnittene eksponeres og integreres med andre komponenter.

⁽¹⁾ Identifisert som OA4 i avsnittet om funksjonsspesifikasjoner for rapporteringsgrensesnittmodulen i del I i dette vedlegget.

URAM.02	eIDAS-samsvar	URAM-programvaren skal gjøre bruk av åpne EU-standarder og -løsninger og skal gjennomføre nødvendige kontrollmekanismer for å kontrollere avsendersertifikater mot klarerte lister offentliggjort av medlemsstatene i samsvar med artikkel 22 i forordning (EU) nr. 910/2014 og Kommisjonens gjennomføringsbeslutning (EU) 2015/1505 ⁽²⁾ , herunder informasjon knyttet til kvalifiserte tilbydere av tillitstjenester som utsteder sertifikater som brukes for elektroniske segl.
----------------	---------------	---

Sikkerhet

ID	Navn	Beskrivelse
URAM.03	Fortrolighet ved informasjonsutveksling	For å sikre sikkerheten til URAM-programvaren og utvekslingen av personopplysninger skal følgende protokoller og krypteringsmetoder implementeres: — Transport Layer Security (TLS): All programvare i URAM skal sikres ved hjelp av TLS for å besørge kryptering på nettverksnivå og dataintegritet for å bidra til å beskytte data under overføring, slik at uautorisert tilgang og manipulering forhindres. — For å kommunisere med URAM-programvaren skal en TLS-konfigurasjon implementeres.
URAM.04	Applikasjonssikkerhet	URAM-programvaren skal sikre deteksjon av skadelige aktiviteter og sikker overføring av sensitiv informasjon.
URAM.05	Vern av personopplysninger	Myndighetene i medlemsstatene gis tilgangsstett i henhold til artikkel 12 nr. 2 i forordning (EU) 2019/1239 for å registrere avsendere. URAM-programvaren skal implementere tilgangskontrollmekanismer for å sikre vern av brukerinformasjon som er personopplysninger, som skal behandles utelukkende for det formålet å opprette brukerkontoer og administrere de tilsvarende tilgangsrettighetene. Den sentrale godkjenningstjenesten skal ikke oppbevare personopplysninger om avsendere lenger enn det som er nødvendig for autentisering. Det sentrale registeret skal ikke oppbevare personopplysninger om avsendere lenger enn det som er nødvendig for administrasjon av kontoen.

Bærekraft og overførbarhet

ID	Navn	Beskrivelse
URAM.06	Teknologiavhengighet	URAM-programvaren skal muliggjøre samhandling med rapporteringsgrensesnittmodulen og andre relevante tjenester uten behov for proprietær programvare eller maskinvare, og skal muliggjøre integrasjon med rapporteringsgrensesnittmodulen uavhengig av det teknologiske miljøet der rapporteringsgrensesnittmodulen brukes.

⁽²⁾ Kommisjonens gjennomføringsbeslutning (EU) 2015/1505 av 8. september 2015 om fastsettelse av tekniske spesifikasjoner og formater for tillitslister i henhold til artikkel 22 nr. 5 i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (EUT L 235 av 9.9.2015, s. 26).

URAM.07	Uavhengig bruk	URAM-programvaren skal ikke kreve at rapporteringsgrensesnittmodulen brukes i et spesifikt miljø. Rapporteringsgrensesnittmodulen skal bare sikre internettforbindelsen og overholdelse av standarder for sikkerhet og protokoller for URAM-programvaren.
----------------	----------------	---

Den sentrale autentiseringstjenestens funksjoner

Følgende tjenester skal være tilgjengelige for rapporteringsgrensesnittmodulen fra den sentrale autentiseringstjenesten:

ID	Navn	Beskrivelse
URAM.08	Autentiseringstjeneste	Den sentrale autentiseringstjenesten er ansvarlig for autentisering av avsendere ved å verifisere gyldigheten til sertifikatet, EORI-nummeret og forbindelsen mellom avsenders EORI-nummer og vedkommendes sertifikat. Den skal behandle autentiseringsforespørsler sendt av RIM og gi svar som angir vellykket eller mislykket autentisering.

Spesifikasjoner for sentralt register

ID	Navn	Beskrivelse
URAM.09	Avsenderregistrering	Det sentrale registeret skal gi medlemsstatene et grafisk brukergrensesnitt for registrering av avsenderdata. Når avsenderen er registrert i det sentrale registeret, skal vedkommende være registrert i alle medlemsstatene.
URAM.10	Visning av og søk etter avsendere	Det sentrale registeret skal gi en medlemsstat mulighet til å se alle data om avsendere som den tidligere har registrert. Det skal også ha en søkefunksjonalitet for å henting av registrerte avsenders data på grunnlag av ulike søkekriterier.
URAM.11	Avsenderoppdatering	Det sentrale registeret skal gi en medlemsstat mulighet til å endre data om alle dens tidligere registrerte avsendere for å sikre at dataene er nøyaktige og gyldige.
URAM.12	Avsenderdeaktivering	Det sentrale registeret skal gi en medlemsstat mulighet til å deaktivere tidligere registrerte avsendere.
URAM.13	Revisjon og rapportering	Det sentrale registeret skal tilby rapporteringsmuligheter som gjør det mulig for en medlemsstat å analysere data om dens tidligere registrerte spesifikke avsendere, for eksempel registreringsdato og sertifikatgyldighet.
URAM.14	Meldinger	Det sentrale registeret skal gi medlemsstatene mulighet til å motta en melding fra det sentrale registeret hver gang en avsender som tidligere er registrert i medlemsstaten, registreres, oppdateres eller deaktiveres, samt når sertifikatet utløper.