2025/908

23.5.2025

AFGØRELSE nr. 1/2024 TRUFFET AF DET FÆLLES UDVALG, DER ER NEDSAT VED AFTALEN MELLEM DEN EUROPÆISKE UNION OG DET SCHWEIZISKE FORBUND OM SAMMENKOBLING AF DERES SYSTEMER FOR HANDEL MED DRIVHUSGASEMISSIONER

af 4. december 2024

for så vidt angår ændringen af bilag II til aftalen og af de fælles driftsprocedurer og de tekniske standarder for sammenkobling [2025/908]

DET FÆLLES UDVALG HAR —

under henvisning til aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner ([1]) (»aftalen«), særlig artikel 9 og artikel 13, stk. 2, og

ud fra følgende betragtninger:

(1) Det fælles udvalgs afgørelse nr. 2/2019 ([2]) indeholdt en foreløbig løsning med henblik på at gøre sammenkoblingen mellem EU ETS og Schweiz' ETS operationel.

(2) På sit tredje møde nåede det fælles udvalg til enighed om behovet for at analysere omkostningseffektiviteten af en permanent forbindelse mellem EU-registret og det schweiziske register.

(3) På sit femte møde nåede det fælles udvalg til enighed om rapporten fra den arbejdsgruppe, der blev nedsat ved det fælles udvalgs afgørelse nr. 1/2020 ([3]) og nr. 2/2020 ([4]). I denne rapport analyserede og anbefalede arbejdsgruppen en tilgang for at gennemføre den permanente forbindelse mellem EU-registret og det schweiziske register.

(4) For at afspejle de tekniske krav til den permanente forbindelse mellem EU-registret og det schweiziske register og for at strømline bestemmelserne i bilag II til aftalen i lyset af den teknologiske udvikling bør bilag II til aftalen ændres.

(5) For at sikre sammenhæng mellem de fælles driftsprocedurer og de tekniske standarder for sammenkobling og bilag II bør de pågældende dokumenter også ændres —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. Bilag II til aftalen erstattes af teksten i bilag I til denne afgørelse.

2. De fælles driftsprocedurer, der er omhandlet i aftalens artikel 3, stk. 6, er fastlagt i bilag II til denne afgørelse. De erstatter de fælles driftsprocedurer i bilaget til afgørelse nr. 1/2020.

([1]) EUT L 322 af 7.12.2017, s. 3.

([2]) Afgørelse nr. 2/2019 truffet af det fælles udvalg, der er nedsat ved aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner af 5. december 2019 om ændring af bilag I og II til aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner [2020/1359] (EUT L 314 af 29.9.2020, s. 68).

([3]) Afgørelse nr. 1/2020 truffet af det fælles udvalg, der er oprettet ved samarbejdsaftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner af 5. november 2020 om vedtagelsen af fælles driftsprocedurer [2021/1033] (EUT L 226 af 25.6.2021, s. 2).

([4]) Afgørelse nr. 2/2020 truffet af det fælles udvalg, der er oprettet ved samarbejdsaftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner af 5. november 2020 om ændring af bilag I og II til aftalen og vedtagelse af tekniske standarder for sammenkobling [2021/1034] (EUT L 226 af 25.6.2021, s. 16).

3. De tekniske standarder for sammenkobling, der er omhandlet i aftalens artikel 3, stk. 7, er fastsat i bilag III til denne afgørelse. De erstatter de tekniske standarder for sammenkobling i bilaget til afgørelse nr. 2/2020.

Artikel 2

Denne afgørelse træder i kraft på dagen for vedtagelsen.

Udfærdiget i Bruxelles, den 4. december 2024.

På det fælles udvalgs vegne

Ruben VERMEEREN	*Beatriz YORDI*	*Thomas MEIER*
Sekretær for Den Europæiske Union	Formand	Sekretær for Schweiz

BILAG I

»*BILAG II*

TEKNISKE STANDARDER FOR SAMMENKOBLING

For at gennemføre sammenkoblingen af EU ETS og Schweiz' ETS blev der gennemført en foreløbig løsning i 2020. Fra og med 2023 vil registerforbindelsen mellem de to ETS'er gradvis blive udviklet hen imod en permanent registerforbindelse, der forventes at blive gennemført senest i 2024, og som gør det muligt for de forbundne markeder at fungere, for så vidt angår fordelene ved markedslikviditet og gennemførelse af transaktioner mellem de to forbundne systemer på en måde, der svarer til et marked bestående af to systemer, og som gør det muligt for markedsdeltagerne at handle, som om de befandt sig på ét marked, kun med det forbehold, at de er underlagt parternes individuelle forskrifter.

I de tekniske standarder for sammenkobling beskrives:

— kommunikationsforbindelsens arkitektur

— kommunikationen mellem SSTL og EUTL

— sikkerheden ved dataoverførsel

— listen over funktioner (transaktioner, afstemning osv.)

— definitionen af transportlaget

— kravene til journalføring af data

— de operationelle arrangementer (calldesk og support)

— planen for aktivering af kommunikation og testproceduren

— proceduren for sikkerhedstest.

I de tekniske standarder for sammenkobling angives det, at administratorerne skal træffe rimelige foranstaltninger for at sikre, at SSTL og EUTL samt forbindelsen er i drift 24 timer om dagen, syv dage om ugen, og at eventuelle driftsafbrydelser for SSTL og EUTL samt forbindelsen holdes på et minimum.

I de tekniske standarder for sammenkobling angives yderligere sikkerhedskrav for det schweiziske register, SSTL, EU-registret og EUTL, som dokumenteres i en plan for sikkerhedsstyring. I de tekniske standarder for sammenkobling angives det navnlig, at:

— begge parter, hvis der er mistanke om, at sikkerheden for det schweiziske register, SSTL, EU-registret eller EUTL er blevet kompromitteret, straks skal underrette den anden part og suspendere forbindelsen mellem SSTL og EUTL

— parterne, i tilfælde af et brud på sikkerheden, forpligter sig til omgående at dele oplysningerne med hinanden. Hvis de tekniske oplysninger foreligger, deles en rapport, der beskriver hændelsen (dato, årsag, virkning og afhjælpning), mellem administratoren af det schweiziske register og Unionens centrale administrator senest 24 timer, efter at en sikkerhedshændelse er identificeret som et sikkerhedsbrud.

Den procedure for sikkerhedstest, der er beskrevet i de tekniske standarder for sammenkobling, udføres, inden kommunikationsforbindelsen mellem SSTL og EUTL etableres, og når en ny version eller frigivelse af SSTL eller EUTL er påkrævet.

De tekniske standarder for sammenkobling skal omhandle to testmiljøer ud over produktionsmiljøet: et testmiljø for udviklere og et godkendelsesmiljø.

Parterne dokumenterer gennem administratoren af det schweiziske register og Unionens centrale administrator, at der er udført en uafhængig sikkerhedsvurdering af deres systemer inden for de foregående 12 måneder i overensstemmelse med de sikkerhedskrav, der er anført i de tekniske standarder for sammenkobling. Sikkerhedstest og navnlig penetrationstest gennemføres for alle nye og større softwarefrigivelser i overensstemmelse med de sikkerhedskrav, der er anført i de tekniske standarder for sammenkobling. Penetrationstesten udføres ikke af softwareudvikleren eller af softwareudviklerens underkontrahent.«

BILAG II

FÆLLES DRIFTSPROCEDURER (FDP) I HENHOLD TIL ARTIKEL 3, STK. 6, I AFTALEN MELLEM DEN EUROPÆISKE UNION OG DET SCHWEIZISKE FORBUND OM SAMMENKOBLING AF DERES SYSTEMER FOR HANDEL MED DRIVHUSGASEMISSIONER

Procedurer for permanent registerforbindelse

Indhold

1. ORDLISTE 7
2. INDLEDNING 7
2.1. Anvendelsesområde 8
2.2. Adressater 8
3. FREMGANGSMÅDE OG STANDARDER 8
4. HÆNDELSESSTYRING 9
4.1. Opdagelse og registrering af hændelser 9
4.2. Klassificering og indledende support 9
4.3. Undersøgelse og diagnosticering 10
4.4. Løsning og genopretning 10
4.5. Lukning af hændelser 10
5. PROBLEMSTYRING 11
5.1. Problemidentifikation og -løsning 11
5.2. Prioritering af problemer 11
5.3. Undersøgelse og diagnosticering af problemer 11
5.4. Løsning 11
5.5. Lukning af problemer 11
6. OPFYLDELSE AF ANMODNINGER 11
6.1. Oprettelse af anmodning 11
6.2. Registrering og analyse af anmodning 12
6.3. Godkendelse af anmodning 12
6.4. Opfyldelse af anmodninger 12
6.5. Eskalering af anmodning 12
6.6. Gennemgang af opfyldelsen af anmodning 12
6.7. Lukning af anmodning 12
7. ÆNDRINGSSTYRING 12
7.1. Ændringsanmodning 13
7.2. Evaluering og planlægning af ændring 13
7.3. Godkendelse af ændring 13
7.4. Gennemførelse af ændring 13
8. FRIGIVELSESSTYRING 13
8.1. Planlægning af frigivelse 14
8.2. Udvikling og test af frigivelsespakke 14
8.3. Forberedelse af ibrugtagning 14
8.4. Rollback af frigivelsen 15

8.5. Gennemgang og lukning af frigivelsen 15
9. STYRING AF SIKKERHEDSHÆNDELSER 15
9.1. Kategorisering af informationssikkerhedshændelser 15
9.2. Håndtering af informationssikkerhedshændelser 15
9.3. Identifikation af sikkerhedshændelser 16
9.4. Analyse af sikkerhedshændelser 16
9.5. Vurdering, eskalering og rapportering af sikkerhedshændelser 16
9.6. Rapportering om håndteringen af sikkerhedshændelsen 16
9.7. Overvågning, kapacitetsopbygning og løbende forbedringer 16
10. INFORMATIONSSIKKERHEDSSTYRING 17
10.1. Identifikation af følsomme oplysninger 17
10.2. Følsomhedsniveauer for informationsaktiver 17
10.3. Tildeling af ejer af informationsaktiver 17
10.4. Registrering af følsomme oplysninger 17
10.5. Håndtering af følsomme oplysninger 18
10.6. Adgangsstyring 18
10.7. Certifikat-/nøglestyring 18

1. **ORDLISTE**

Tabel 1-1

Akronymer og definitioner

Akronym/begreb	Definition
Certifikatmyndighed	Enhed, der udsteder digitale certifikater
CH	Det Schweiziske Forbund
ETS	Emissionshandelssystem
EU	Den Europæiske Union
IMT	Hændelsesstyringsteam
Informationsaktiv	En oplysning, der er værdifuld for en virksomhed eller organisation
IT	Informationsteknologi
ITIL	IT-infrastrukturbibliotek
ITSM	IT-servicemanagement
LTS	Tekniske standarder for sammenkobling
Register	Et regnskabssystem for kvoter udstedt under det ETS, som holder styr på ejerskabet af kvoter, der opbevares på elektroniske konti
RFC	Ændringsanmodning
SIL	Liste over følsomme oplysninger
SR	Serviceanmodning
Wiki	Websted, hvor brugerne kan udveksle information og viden ved at tilføje eller tilpasse indhold direkte via en webbrowser

2. **INDLEDNING**

Aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner af 23. november 2017 (»aftalen«) indeholder bestemmelser om gensidig anerkendelse af emissionskvoter, der kan anvendes til at opfylde kravene i Den Europæiske Unions emissionshandelssystem (»EU ETS«) eller Schweiz' emissionshandelssystem (»Schweiz' ETS«). Med henblik på at gennemføre sammenkoblingen af EU ETS og Schweiz' ETS vil der blive etableret en direkte forbindelse mellem EU-registrets EU-transaktionsjournal (EUTL) og det schweiziske registers supplerende transaktionsjournal (SSTL), som vil muliggøre overdragelse af emissionskvoter udstedt i et af ETS'erne mellem registrene (aftalens artikel 3, stk. 2). For at gennemføre sammenkoblingen af EU ETS og Schweiz' ETS blev der gennemført en foreløbig løsning i 2020. Fra og med 2023 vil registerforbindelsen mellem de to ETS'er gradvis blive udviklet hen imod en permanent registerforbindelse, der forventes at blive gennemført senest i 2024, og som gør det muligt for de forbundne markeder at fungere, for så vidt angår fordelene ved markedslikviditet og gennemførelse af transaktioner mellem de to forbundne systemer på en måde, der svarer til et marked bestående af to systemer, og som gør det muligt for markedsdeltagerne at handle, som om de befandt sig på ét marked, kun med det forbehold, at de er underlagt parternes individuelle forskrifter (bilag II til aftalen).

I henhold til aftalens artikel 3, stk. 6, fastlægger administratoren af det schweiziske register og Unionens centrale administrator fælles driftsprocedurer (FDP) for tekniske og andre forhold, som er nødvendige for driften af forbindelsen, under hensyntagen til prioriteter i den nationale lovgivning. De FDP'er, der udvikles af administratorerne, træder i kraft, når de er vedtaget ved afgørelse i det fælles udvalg.

FDP'erne blev vedtaget af det fælles udvalg ved afgørelse nr. 1/2020. De opdaterede FDP, der fremgår af dette dokument, vil blive vedtaget af det fælles udvalg ved afgørelse nr. 1/2024. I overensstemmelse med nærværende afgørelse og efter anmodninger fra det fælles udvalg har administratoren af det schweiziske register og Unionens centrale administrator udviklet yderligere tekniske retningslinjer for at gennemføre sammenkoblingen og sikre, at disse løbende tilpasses til den tekniske udvikling og nye krav til sammenkoblingens sikkerhed og sikring og dens effektive drift.

2.1. **Anvendelsesområde**

Dette dokument repræsenterer den fælles forståelse mellem aftalens parter om oprettelse af det proceduremæssige grundlag for forbindelse mellem registrene i EU ETS og Schweiz' ETS. Det skitserer de overordnede proceduremæssige krav med hensyn til driften, men der vil være behov for yderligere tekniske retningslinjer for at gennemføre forbindelsen.

For at sikre, at forbindelsen fungerer korrekt, vil det kræve tekniske specifikationer for yderligere at gennemføre sammenkoblingen. I henhold til aftalens artikel 3, stk. 7, er disse spørgsmål beskrevet i de tekniske standarder for sammenkobling, der skal vedtages separat ved afgørelse i det fælles udvalg.

Formålet med FDP er at sikre, at de IT-tjenester, der er knyttet til driften af forbindelsen mellem registrene i EU ETS og Schweiz' ETS, leveres effektivt, navnlig for at kunne imødekomme serviceanmodninger, løse servicefejl, løse problemer og udføre rutinemæssige operationelle opgaver i overensstemmelse med internationale standarder for IT-servicemanagement.

For den permanente registerforbindelse vil der kun være behov for følgende FDP, som indgår i dette dokument:

— Hændelsesstyring

— Problemstyring

— Opfyldelse af anmodninger

— Ændringsstyring

— Frigivelsesstyring

— Styring af sikkerhedshændelser

— Informationssikkerhedsstyring.

2.2. **Adressater**

Målgrupperne for disse FDP er EU's og de schweiziske supportteams for registrene.

3. **FREMGANGSMÅDE OG STANDARDER**

Følgende princip gælder for alle FDP:

— EU og CH er enige om at definere FDP på grundlag af ITIL (IT-infrastrukturbibliotek, version 4). Praksis fra denne standard genbruges og tilpasses de særlige behov i relation til den permanente registerforbindelse.

— Den kommunikation og koordinering, der er nødvendig for behandlingen af FDP mellem de to parter, foregår via servicedeskene under CH's og EU's registre. Opgaverne tildeles altid inden for den ene part.

— Hvis der er uenighed om håndteringen af en fælles driftsprocedure, vil dette blive analyseret og løst mellem de to servicedeske. Hvis det ikke er muligt at nå til enighed, eskaleres problemstillingen til det næste niveau.

Eskaleringsniveauer	EU	CH
1. niveau	EU's servicedesk	CH's servicedesk
2. niveau	EU's driftsleder	Den ansvarlige for CH's registerapplikation
3. niveau	Det fælles udvalg (som kan uddelegere dette ansvar under hensyntagen til aftalens artikel 12, stk. 5)	
4. niveau	Det fælles udvalg, hvis 3. niveau uddelegeres	

— Hver part kan fastsætte procedurer for driften af sit eget registersystem under hensyntagen til krav og grænseflader i forbindelse med disse FDP'er.

— Der anvendes et værktøj til ITSM (IT-servicemanagement) til støtte for FDP'en, herunder navnlig hændelsesstyring, problemstyring og opfyldelse af anmodninger, samt kommunikation mellem parterne.

— Desuden tillades udveksling af oplysninger via e-mail.

— Begge parter sikrer, at kravene til informationssikkerhed opfyldes i overensstemmelse med håndteringsinstrukserne.

4. HÆNDELSESSTYRING

Formålet med hændelsesstyringsprocessen er at sikre, at IT-tjenester efter en hændelse kan vende tilbage til det normale serviceniveau så hurtigt som muligt og med minimale afbrydelser af driften.

Hændelsesstyringen bør også omfatte et register over hændelser med henblik på indberetning og integration med andre processer for at sikre løbende forbedringer.

Fra et overordnet perspektiv omfatter hændelsesstyring følgende aktiviteter:

— Opdagelse og registrering af hændelser

— Klassificering og indledende support

— Undersøgelse og diagnosticering

— Løsning og genopretning

— Lukning af hændelser.

I løbet af en hændelses livscyklus sikrer hændelsesstyringsprocessen den løbende håndtering af ejerskab, overvågning, sporing og kommunikation.

4.1. Opdagelse og registrering af hændelser

En hændelse kan opdages af en supportgruppe, af automatiserede overvågningsværktøjer eller af teknisk personale, der udfører rutinemæssig overvågning.

Når en hændelse opdages, skal den registreres og tildeles en entydig identifikator, der muliggør korrekt sporing og overvågning. Den entydige identifikator for en hændelse er den identifikator, der er tildelt i det fælles sagsstyringssystem i servicedesken for den part (enten EU eller CH), der konstaterede hændelsen, og den skal anvendes i alle meddelelser vedrørende denne hændelse.

For alle hændelser bør kontaktpunktet være servicedesken for den part, der har åbnet sagen.

4.2. Klassificering og indledende support

Klassificeringen af hændelser har til formål at forstå og identificere, hvilket system og/eller hvilke tjenester, der er berørt af en hændelse, og i hvilket omfang. For at være effektiv bør klassificeringen sikre, at hændelsen henvises til den korrekte ressource i første forsøg for at fremskynde løsningen af hændelsen.

I klassificeringsfasen kategoriseres og prioriteres hændelsen afhængigt af, hvilken virkning den har, og hvor meget den haster, så den kan behandles inden for den tidshorisont, der er relevant i forhold til prioriteringen.

Hvis hændelsen har en potentiel indvirkning på følsomme datas fortrolighed eller integritet og/eller på systemets tilgængelighed, skal hændelsen også angives som en sikkerhedshændelse og derefter håndteres i henhold til den proces, der er defineret i kapitlet »Styring af sikkerhedshændelser« i dette dokument.

Om muligt udfører den servicedesk, der åbnede sagen, en indledende diagnose. Her vil servicedesken undersøge, om hændelsen er en kendt fejl. Hvis dette er tilfældet, er det allerede kendt og dokumenteret, hvordan man løser problemet eller laver en workaround.

Hvis servicedesken løser hændelsen, vil den rent faktisk lukke hændelsen på dette tidspunkt, da det primære formål med hændelsesstyring er blevet opfyldt (dvs. hurtig genoptagelse af service for slutbrugeren). Hvis dette ikke er tilfældet, vil servicedesken eskalere hændelsen til et relevant team, der kan undersøge og diagnosticere problemet nærmere.

4.3. **Undersøgelse og diagnosticering**

Undersøgelse og diagnosticering af hændelser bruges, når en hændelse ikke kan afhjælpes af servicedesken som en del af den indledende diagnose og derfor er blevet eskaleret. Eskalering af hændelser er en del af undersøgelses- og diagnosticeringsprocessen.

En almindelig praksis i undersøgelses- og diagnosticeringsfasen er at forsøge at genskabe hændelsen under kontrollerede forhold. Det er i forbindelse med undersøgelse og diagnosticering af hændelser vigtigt, at man forstår rækkefølgen af de handlinger, der førte til hændelsen.

Eskalering er en anerkendelse af, at en hændelse ikke kan afhjælpes på det nuværende supportniveau og skal overdrages til en supportgruppe på et højere plan eller til den anden part. Eskaleringen kan følge to veje: horisontalt (funktionelt) eller vertikalt (hierarkisk).

Den servicedesk, der registrerede og udløste hændelsen, er ansvarlig for at eskalere hændelsen til den relevante ressource og for at følge den overordnede status for og placering af hændelsen.

Den part, som har fået tildelt hændelsen, er ansvarlig for at sikre, at de ønskede handlinger udføres rettidigt, samt for at give feedback til sin egen parts servicedesk.

4.4. **Løsning og genopretning**

Løsning af hændelser og genopretning foretages, når man ved, hvad der forårsagede hændelsen. At finde en løsning på en hændelse betyder, at man har fundet en metode til afhjælpning af problemet. Det at gennemføre løsningen er genopretningsfasen.

Når de passende ressourcer har løst problemet, henvises hændelsen tilbage til den relevante servicedesk, som har registreret hændelsen, og samme servicedesk bekræfter over for den, der konstaterede hændelsen, at fejlen er rettet, og at hændelsen kan lukkes. Resultaterne af behandlingen af hændelsen skal registreres til fremtidig brug.

Genopretning kan foretages af IT-supportere eller ved at give slutbrugeren en række instrukser, der skal følges.

4.5. **Lukning af hændelser**

Lukning er det sidste trin i hændelsesstyringsprocessen lige efter, at der er fundet en løsning.

Tjeklisten over handlinger, der skal foretages i denne fase, omfatter bl.a.:

— Kontrol af den oprindelige kategorisering, der blev tildelt hændelsen

— Korrekt indsamling af alle oplysninger om hændelsen

— Behørig dokumentation af hændelsen og opdatering af videnbasen

— Passende kommunikation til alle interessenter, der er direkte eller indirekte berørt af hændelsen.

En hændelse lukkes formelt, når servicedesken har afsluttet lukningen af hændelsen og meddelt det til den anden part.

Når en hændelse er lukket, genåbnes den ikke. Hvis en hændelse sker igen inden for kort tid, skal den oprindelige hændelse ikke genåbnes, men der skal åbnes en ny hændelse.

Hvis hændelsen behandles af både EU's og CH's servicedesk, ligger ansvaret for lukning af sagen hos den servicedesk, der åbnede sagen.

5. PROBLEMSTYRING

Denne procedure bør følges, hver gang der konstateres et problem, som udløser problemstyringsprocessen. Problemstyring fokuserer på at forbedre kvaliteten og reducere antallet af hændelser, der rettes til servicedesken. Et problem kan være årsagen til en eller flere hændelser. Når en hændelse rapporteres, er formålet med hændelsesstyring at genoprette tjenesten så hurtigt som muligt, eventuelt gennem en workaround. Når et problem oprettes, er formålet at undersøge den grundlæggende årsag til problemet for at finde frem til en ændring, der vil sikre, at problemet og de dermed forbundne hændelser ikke vil ske igen.

5.1. Problemidentifikation og -løsning

Afhængigt af hvilken part, der har åbnet sagen, vil enten EU's eller CH's servicedesk være kontaktpunkt for spørgsmål vedrørende problemet.

Den entydige identifikator for et problem er den identifikator, der er tildelt af IT-servicemanagement (ITSM). Den skal fremgå af alle meddelelser vedrørende dette problem.

Et problem kan udløses af en hændelse eller kan åbnes på eget initiativ for at løse problemer, der opdages i systemet på et hvilket som helst tidspunkt.

5.2. Prioritering af problemer

Problemer kan ligesom hændelser kategoriseres efter alvorsgrad og prioritering for at gøre det nemmere at spore dem, hvor konsekvenserne af de tilknyttede hændelser og deres hyppighed tages i betragtning.

5.3. Undersøgelse og diagnosticering af problemer

Hver part kan gøre opmærksom på et problem, og den pågældende parts servicedesk vil være ansvarlig for at registrere problemet, tildele passende ressourcer og følge den overordnede status for problemet.

Den gruppe, som problemet blev eskaleret til, er ansvarlig for at løse problemet hurtigt og kommunikere med servicedesken.

Efter anmodning er begge parter ansvarlige for at sikre, at de anviste foranstaltninger gennemføres, og for at give feedback til sin egen parts servicedesk.

5.4. Løsning

Den gruppe, som problemet er blevet henvist til, er ansvarlig for at løse problemet og give relevante oplysninger til sin egen parts servicedesk.

Resultaterne af behandlingen af problemet skal registreres til fremtidig brug.

5.5. Lukning af problemer

Et problem lukkes formelt, når problemet er blevet løst ved at gennemføre ændringen. Denne fase gennemføres af den servicedesk, der registrerede problemet og informerede den anden parts servicedesk.

6. OPFYLDELSE AF ANMODNINGER

Opfyldelse af anmodninger er håndtering fra start til slut af en anmodning om en ny eller eksisterende tjeneste fra det øjeblik, hvor den registreres og godkendes, og indtil den lukkes. Serviceanmodninger er normalt små, foruddefinerede, repeterbare, hyppige, forhåndsgodkendte og proceduremæssige anmodninger.

De vigtigste trin, der skal følges, er beskrevet nedenfor:

6.1. Oprettelse af anmodning

Oplysningerne vedrørende en serviceanmodning gives til EU's eller CH's servicedesk pr. e-mail, telefon eller via ITSM-værktøjet eller en anden aftalt kommunikationskanal.

6.2. **Registrering og analyse af anmodning**

For alle serviceanmodninger bør kontaktpunktet være EU's eller CH's servicedesk, afhængigt af hvilken part serviceanmodningen kommer fra. Denne servicedesk vil være ansvarlig for at registrere og analysere serviceanmodningen med den fornødne omhu.

6.3. **Godkendelse af anmodning**

Medarbejderen i servicedesken for den part, serviceanmodningen kom fra, kontrollerer, om der kræves godkendelser fra den anden part, og indhenter dem i så fald. Hvis serviceanmodningen ikke godkendes, ajourfører og lukker servicedesken sagen.

6.4. **Opfyldelse af anmodninger**

I dette trin sikres effektiv og virkningsfuld behandling af serviceanmodninger. Der skal skelnes mellem følgende tilfælde:

— Opfyldelsen af serviceanmodningen berører kun den ene part. I dette tilfælde udsteder denne part arbejdsordrerne og koordinerer udførelsen.

— Opfyldelsen af serviceanmodningen berører både EU og CH. I dette tilfælde udsteder begge servicedeske arbejdsordrerne inden for deres ansvarsområde. Behandlingen af serviceanmodningen koordineres mellem de to servicedeske. Det overordnede ansvar ligger hos den servicedesk, som modtog og igangsatte serviceanmodningen.

Når serviceanmodningen er blevet opfyldt, skal den have status som »løst« (»Resolved«).

6.5. **Eskalering af anmodning**

Servicedesken kan om nødvendigt eskalere den udestående serviceanmodning til den relevante ressource (tredjepart).

Eskalering sker til de respektive tredjeparter, dvs. at EU's servicedesk skal gå gennem CH's servicedesk for at eskalere til en tredjepart i CH og omvendt.

Den tredjepart, som serviceanmodningen blev eskaleret til, er ansvarlig for at behandle serviceanmodningen rettidigt og kommunikere med den servicedesk, der har eskaleret anmodningen.

Den servicedesk, der registrerede serviceanmodningen, er ansvarlig for at følge den overordnede status og placering af en serviceanmodning.

6.6. **Gennemgang af opfyldelsen af anmodning**

Den ansvarlige servicedesk fremsender serviceanmodningen til en endelig kvalitetskontrol, inden den lukkes. Formålet er at sikre, at serviceanmodningen faktisk behandles, og at alle de oplysninger, der er nødvendige for at beskrive anmodningens livscyklus, leveres med tilstrækkelige detaljer. Derudover skal resultaterne af behandlingen af anmodningen registreres til fremtidig brug.

6.7. **Lukning af anmodning**

Hvis de deltagende parter er enige om, at serviceanmodningen er blevet opfyldt, og rekvirenten mener, at sagen er løst, er den næste status, der skal angives, »lukket« (»Closed«).

En serviceanmodning lukkes formelt, når den servicedesk, der registrerede serviceanmodningen, har gennemført lukningen og underrettet den anden parts servicedesk.

7. **ÆNDRINGSSTYRING**

Formålet er at sikre, at der anvendes standardiserede metoder og procedurer til effektiv og hurtig håndtering af alle ændringer i kontrolinfrastrukturen for at minimere antallet og virkningen af relaterede hændelser ved service. Ændringer i IT-infrastruktur kan ske som reaktion på problemer eller krav udefra, f.eks. lovgivningsmæssige ændringer, eller som et proaktivt forsøg på at opnå større effektivitet eller virkningsfuldhed eller for at kunne gennemføre eller afspejle forretningsmæssige initiativer.

Ændringsstyringsprocessen omfatter forskellige trin, der omfatter alle detaljer af en ændringsanmodning med henblik på fremtidig sporing. Disse processer sikrer, at ændringen valideres og testes, før den tages i brug. Ibrugtagningen gennemføres under frigivelsesstyringens ansvar.

7.1. **Ændringsanmodning**

En ændringsanmodning indgives til ændringsstyringsteamet med henblik på validering og godkendelse. For alle ændringsanmodninger bør kontaktpunktet være EU's eller CH's servicedesk, afhængigt af hvilken part der har fremsat anmodningen. Denne servicedesk vil være ansvarlig for at registrere og analysere anmodningen med fornøden omhu.

Ændringsanmodninger kan stamme fra:

— En hændelse, der medfører en ændring

— Et eksisterende problem, der medfører en ændring

— En slutbruger, der anmoder om en ny ændring

— Ændring som følge af løbende vedligeholdelse

— Lovgivningsmæssig ændring.

7.2. **Evaluering og planlægning af ændring**

På dette trin sker vurderingen og planlægningen af ændringer. Det omfatter prioritering og planlægning af aktiviteter med henblik på at minimere risici og virkninger.

Hvis gennemførelsen af ændringsanmodningen berører både EU og CH, verificerer den part, der har registreret ændringsanmodningen, evalueringen og planlægningen med den anden part.

7.3. **Godkendelse af ændring**

Alle registrerede ændringsanmodninger skal godkendes af det relevante eskaleringsniveau.

7.4. **Gennemførelse af ændring**

Gennemførelsen af ændringer sker i forbindelse med frigivelsesstyringsprocessen. Parternes teams følger deres egne processer, der omfatter planlægning og test. Ændringen vurderes derefter, når den er gennemført. For at sikre, at alt er forløbet efter planen, gennemgås den eksisterende ændringsstyringsproces hele tiden og ajourføres, hvis det er nødvendigt.

8. **FRIGIVELSESSTYRING**

En frigivelse er en eller flere ændringer i en IT-tjeneste, der er samlet i en frigivelsesplan, og som skal godkendes, forberedes, udvikles, testes og anvendes sammen. En frigivelse kan f.eks. være en fejlrettelse, en ændring af hardware eller andre komponenter, ændringer i software, opgradering af applikationsversioner, ændringer af dokumentation og/eller processer. Indholdet af hver enkelt frigivelse styres, testes og anvendes som én enkelt enhed.

Frigivelsesstyring har til formål at planlægge, udvikle, teste og validere og levere kapacitet til at udføre den ønskede service, som vil opfylde de berørte parters behov samt de tilsigtede mål. Acceptkriterier for alle serviceændringer vil blive fastlagt og dokumenteret i forbindelse med designkoordinering og leveres til de relevante teams.

Frigivelsen vil typisk bestå af en række problemrettelser og forbedringer af en service. Den indeholder det nye eller ændrede software, der kræves, og det nye eller ændrede hardware, der er nødvendigt for at gennemføre de godkendte ændringer.

8.1. **Planlægning af frigivelse**

I det første trin i processen fordeles godkendte ændringer på frigivelsespakker, og frigivelsens omfang og indhold bestemmes. På grundlag af disse oplysninger vil der i planlægningen af frigivelsen blive udarbejdet en tidsplan for udvikling, test og ibrugtagning af frigivelsen.

Planlægningen bør omfatte:

— Frigivelsens omfang og indhold

— Risikovurdering og risikoprofil for frigivelsen

— Kunder/brugere, der berøres af frigivelsen

— Det team, der er ansvarligt for frigivelsen

— Strategi for levering og ibrugtagning

— Ressourcer til frigivelsen og dens ibrugtagning.

Begge parter informerer hinanden om deres vinduer for planlægning og vedligeholdelse af frigivelser. Hvis en frigivelse berører både EU og CH, koordinerer de planlægningen og definerer et fælles vindue for vedligeholdelse.

8.2. **Udvikling og test af frigivelsespakke**

I udviklings- og testfasen fastlægges det, hvordan frigivelsen eller pakken skal behandles, og hvordan de kontrollerede miljøer, inden produktionen ændres, kan opretholdes, samt test af alle ændringer i alle miljøer.

Hvis en frigivelse berører både EU og CH, koordinerer de leveringsplaner og test. Dette omfatter følgende aspekter:

— Hvordan og hvornår de enkelte dele af en frigivelse og servicekomponenter vil blive leveret

— Hvad produktionstiden normalt er, og hvad der sker i tilfælde af en forsinkelse

— Hvordan man kan følge med i, hvordan leveringen skrider frem, og få det bekræftet

— Parametre for overvågning og bestemmelse af, om ibrugtagningen af frigivelsen sker korrekt

— Fælles testcases for relevante funktioner og ændringer.

Ved afslutningen af denne delproces er alle de krævede frigivelseskomponenter klar til ibrugtagning.

8.3. **Forberedelse af ibrugtagning**

Forberedelsesprocessen sikrer, at kommunikationsplanerne defineres korrekt, at meddelelser er klar til at blive sendt til alle berørte interessenter og slutbrugere, og at frigivelsen integreres i ændringsstyringsprocessen for at sikre, at alle ændringer udføres på en kontrolleret måde og godkendes i de krævede fora.

Hvis en frigivelse berører både EU og CH, skal de koordinere følgende aktiviteter:

— Registrering af ændringsanmodning og forberedelse af ibrugtagning i produktionsmiljø

— Udarbejdelse af en gennemførelsesplan

— Rollback-metode, så det er muligt at vende tilbage til den tidligere tilstand, hvis ibrugtagning af frigivelsen mislykkes

— Meddelelser til alle de nødvendige parter

— Krav om godkendelse af gennemførelsen af frigivelsen fra det relevante eskaleringsniveau.

8.4. **Rollback af frigivelsen**

Hvis der har været fejl i ibrugtagningen, eller det viste sig i testen, at ibrugtagningen ikke lykkedes, eller ikke opfyldte de aftalte godkendelses-/kvalitetskriterier, vil begge parters teams skulle rulle tilbage til den tidligere tilstand. Alle berørte interessenter skal informeres, herunder berørte og tilsigtede slutbrugere. Mens der afventes godkendelse, kan processen genoptages på ethvert af de foregående trin.

8.5. **Gennemgang og lukning af frigivelsen**

Ved gennemgangen af en ibrugtagning bør følgende aktiviteter være omfattet:

— Indhente feedback om kundens, brugerens og de pågældende medarbejderes tilfredshed med ibrugtagningen (indsamle feedback og overveje løbende at forbedre servicen)

— Gennemgå alle kvalitetskriterier, der ikke er opfyldt

— Kontrollere, at eventuelle handlinger, nødvendige rettelser og ændringer er fuldstændige

— Sikre, at der ikke er nogen problemer med hensyn til funktioner, ressourcer, kapacitet eller resultater efter ibrugtagningen af frigivelsen

— Kontrollere, at eventuelle problemer, kendte fejl og workarounds er dokumenteret og accepteret af kunden, slutbrugerne, driftssupport og andre berørte parter

— Overvåge hændelser og problemer som følge af ibrugtagning (yde tidlig support til driftsteams, hvis frigivelsen har medført en forøgelse af arbejdsmængden)

— Ajourføre supportdokumentation (dvs. tekniske dokumenter)

— Formelt overdrage den ibrugtagede frigivelse til driften

— Dokumentere de indhøstede erfaringer

— Indhente en oversigt over frigivelsen fra de teams, der har gennemført den

— Formelt lukke frigivelsen efter kontrol af ændringsanmodninger.

9. **STYRING AF SIKKERHEDSHÆNDELSER**

Styring af sikkerhedshændelser er en proces for håndtering af sikkerhedshændelser med henblik på at muliggøre kommunikation om hændelser til potentielt berørte interessenter, evaluering og prioritering af hændelser samt håndtering af hændelser med henblik på at løse eventuelle faktiske, formodede eller potentielle brud på fortroligheden, tilgængeligheden eller integriteten af følsomme informationsaktiver.

9.1. **Kategorisering af informationssikkerhedshændelser**

Alle hændelser, der påvirker forbindelsen mellem EU-registret og det schweiziske register, analyseres for at fastslå et eventuelt brud på fortroligheden, integriteten eller tilgængeligheden af følsomme oplysninger, der er registreret på listen over følsomme oplysninger (SIL).

Hvis dette er tilfældet, skal hændelsen kategoriseres som en informationssikkerhedshændelse, straks registreres i ITSM-værktøjet og behandles som sådan.

9.2. **Håndtering af informationssikkerhedshændelser**

Sikkerhedshændelser placeres under det 3. eskaleringsniveau, og løsningen af hændelser vil blive varetaget af et særligt team til styring af hændelser (Incident Management Team (IMT)).

Teamet er ansvarligt for:

— Den første analyse, kategorisering og vurdering af hændelsens alvor

— Koordinering af foranstaltninger mellem alle interessenter, herunder den fulde dokumentation af analysen af hændelsen, de beslutninger, der træffes for at håndtere hændelsen, og mulige identificerede svagheder

— Rettidig eskalering af hændelsen til rette niveau til orientering og/eller afgørelse, afhængigt af hvor alvorlig sikkerhedshændelsen er.

I informationsstyringsprocessen klassificeres alle oplysninger vedrørende hændelser på det højeste følsomhedsniveau, men under ingen omstændigheder lavere end SENSITIVE: *ETS*.

I forbindelse med en igangværende undersøgelse og/eller en svaghed, der kan udnyttes, og indtil den afhjælpes, klassificeres oplysningerne som SPECIAL HANDLING: *ETS Critical*.

9.3. **Identifikation af sikkerhedshændelser**

Afhængigt af typen af sikkerhedshændelse fastsætter den informationssikkerhedsansvarlige de relevante organisationer, der skal inddrages, og som skal indgå i IMT.

9.4. **Analyse af sikkerhedshændelser**

IMT samarbejder med alle involverede organisationer og de relevante medlemmer af deres teams, alt efter hvad der er relevant, for at gennemgå hændelsen. Under analysen afdækkes det, i hvilket omfang et aktivs fortrolighed, integritet eller tilgængelighed er berørt, og konsekvenserne for alle berørte organisationer vurderes. Dernæst defineres indledende og opfølgende foranstaltninger til at afhjælpe hændelsen og styre dens virkninger, herunder de ressourcemæssige konsekvenser af disse foranstaltninger.

9.5. **Vurdering, eskalering og rapportering af sikkerhedshændelser**

IMT vurderer, hvor alvorlig en ny sikkerhedshændelse er, efter at den er blevet konstateret, og begynder omgående at træffe de nødvendige foranstaltninger afhængigt af hændelsens alvor.

9.6. **Rapportering om håndteringen af sikkerhedshændelsen**

IMT udarbejder en rapport om håndteringen af sikkerhedshændelsen med oplysninger om, hvordan den er blevet inddæmmet, og den efterfølgende genopretning. Rapporten sendes til det 3. eskaleringsniveau pr. sikker e-mail eller andre gensidigt accepterede sikre kommunikationsmidler.

Den ansvarlige part gennemgår resultaterne af inddæmningen og genopretningen og:

— Tilkobler registret igen, hvis det er blevet afkoblet

— Oplyser registerteams om hændelsen

— Lukker hændelsen.

IMT bør — på en sikker måde — medtage relevante oplysninger i rapporten om sikkerhedshændelsen for at sikre konsekvent registrering og kommunikation og gøre det muligt at træffe hurtige og hensigtsmæssige foranstaltninger til at inddæmme hændelsen. Efter færdiggørelsen forelægger IMT den endelige rapport om sikkerhedshændelsen inden for rimelig tid.

9.7. **Overvågning, kapacitetsopbygning og løbende forbedringer**

IMT leverer rapporter om alle sikkerhedshændelser til det 3. eskaleringsniveau. Rapporterne vil blive anvendt af dette eskaleringsniveau til at fastslå følgende:

— Svage punkter i sikkerhedskontrollen og/eller driften, der skal styrkes

— Eventuelle behov for at forbedre denne procedure for at forbedre effektiviteten af reaktionen på hændelser

— Uddannelses- og kapacitetsopbygningsmuligheder for yderligere at styrke registersystemers modstandsdygtighed over for informationssikkerhedshændelser, mindske risikoen for fremtidige hændelser og minimere deres virkning.

10. **INFORMATIONSSIKKERHEDSSTYRING**

Informationssikkerhedsstyring har til formål at sikre fortrolighed, integritet og tilgængelighed af en organisations fortrolige oplysninger, data og IT-tjenester. Ud over de tekniske komponenter, herunder design og test (se de tekniske standarder for sammenkobling), er følgende fælles driftsprocedurer nødvendige for at opfylde sikkerhedskravene til den permanente registerforbindelse.

10.1. **Identifikation af følsomme oplysninger**

En oplysnings følsomhed vurderes ved at bestemme virkningerne for virksomheden (f.eks. økonomiske tab, skade på image, overtrædelse af lovgivningen osv.) af et brud på sikkerheden i forbindelse med disse oplysninger.

De følsomme informationsaktiver skal identificeres på grundlag af deres indvirkning på forbindelsen.

Disses følsomhed vurderes i henhold til den følsomhedsskala, der gælder for denne forbindelse, og som er beskrevet i afsnittet »Håndtering af informationssikkerhedshændelser« i dette dokument.

10.2. **Følsomhedsniveauer for informationsaktiver**

Når et informationsaktiv er identificeret, klassificeres det efter følgende regler:

— Ved mindst ét højt niveau med hensyn til fortrolighed, integritet eller tilgængelighed klassificeres aktivet som SPECIAL HANDLING: *ETS Critical*.

— Ved mindst ét mellemhøjt niveau med hensyn til fortrolighed, integritet eller tilgængelighed klassificeres aktivet som SENSITIVE: *ETS*.

— Ved kun lave niveauer med hensyn til fortrolighed, integritet eller tilgængelighed klassificeres aktivet som EU: SENSITIVE: *ETS Joint Procurement*. Klassificering Schweiz: LIMITED: *ETS*.

10.3. **Tildeling af ejer af informationsaktiver**

Alle informationsaktiver bør få tildelt en ejer. Informationsaktiver i ETS, som tilhører eller er forbundet med forbindelsen mellem EUTL og SSTL, bør medtages i en fælles liste over aktiver, der føres af begge parter. Informationsaktiver i ETS, som er uden for forbindelsen mellem EUTL og SSTL, bør medtages i en fælles liste over aktiver, der føres af den respektive part.

Parterne skal aftale, hvem der ejer hvert enkelt informationsaktiv, der tilhører eller er forbundet med forbindelsen mellem EUTL og SSTL. Ejeren af et informationsaktiv er ansvarlig for at vurdere dets følsomhed.

Ejeren bør have de beføjelser, der passer til værdien af de tildelte aktiver. Ejerens ansvar for aktivet/aktiverne og vedkommendes forpligtelse til at opretholde den nødvendige fortrolighed, integritet og tilgængelighed bør aftales og formaliseres.

10.4. **Registrering af følsomme oplysninger**

Alle følsomme oplysninger registreres i listen over følsomme oplysninger (SIL).

Hvis det er relevant, skal der tages højde for, at flere følsomme oplysninger tilsammen kan have en større virkning end virkningen af én enkelt oplysning, og dette skal registreres i listen (f.eks. oplysninger lagret i systemdatabasen).

Listen er ikke statisk. Trusler, sårbarheder, sandsynlighed eller konsekvenser af sikkerhedshændelser i forbindelse med aktiverne kan ændre sig uden forvarsel, og der kan indføres nye aktiver i driften af registersystemerne.

Derfor skal listen regelmæssigt tages op til revision, og nye oplysninger, der kategoriseres som følsomme, skal straks registreres i listen.

Listen skal mindst indeholde følgende oplysninger:

— Beskrivelse af oplysningerne

— Oplysningens ejer

— Følsomhedsniveau

— Angivelse af, om oplysningerne omfatter personoplysninger

— Eventuelle yderligere oplysninger.

10.5. **Håndtering af følsomme oplysninger**

Når følsomme oplysninger behandles uden for forbindelsen mellem EU-registret og det schweiziske register, skal de behandles i overensstemmelse med håndteringsinstrukserne.

Følsomme oplysninger, der behandles via en forbindelse mellem EU-registret og det schweiziske register, behandles i overensstemmelse med parternes sikkerhedskrav.

10.6. **Adgangsstyring**

Formålet med adgangsstyring er at give autoriserede brugere ret til at benytte en service og samtidig forhindre adgang for uautoriserede brugere. Adgangsstyring omtales undertiden også som »rettighedsstyring« eller »identitetsstyring«.

I forbindelse med den permanente registerforbindelse og dens drift har begge parter behov for adgang til følgende komponenter:

— Wiki: Et samarbejdsmiljø for udveksling af fælles oplysninger som f.eks. planlægning af frigivelser

— ITSM-værktøj til styring af hændelser og problemer (se kapitel 3, »Fremgangsmåde og standarder«)

— System til udveksling af meddelelser: Hver part skal have et sikkert system til udveksling af meddelelser, der indeholder transaktionsdata.

Administratoren af det schweiziske register og Unionens centrale administrator sørger for, at adgangsrettighederne er ajourført, og fungerer som kontaktpunkter for parternes adgangsstyringsaktiviteter. Anmodninger om adgang behandles i henhold til procedurerne for opfyldelse af anmodninger.

10.7. **Certifikat-/nøglestyring**

Hver part er ansvarlig for sin egen certifikat-/nøglestyring (generering, registrering, lagring, installation, anvendelse, fornyelse, tilbagekaldelse, sikkerhedskopiering og tilbagelevering af certifikater/nøgler). Som beskrevet i de tekniske standarder for sammenkobling må der kun bruges digitale certifikater udstedt af en certificeringsmyndighed, som begge parter har tillid til. Håndtering og opbevaring af certifikater/nøgler skal følge de bestemmelser, der er fastsat i håndteringsinstrukserne.

Tilbagekaldelse og/eller fornyelse af certifikater og nøgler koordineres af begge parter. Dette sker i overensstemmelse med procedurerne for opfyldelse af anmodninger.

Administratoren af det schweiziske register og Unionens centrale administrator udveksler certifikater/nøgler via sikre kommunikationsmidler i overensstemmelse med de bestemmelser, der er fastlagt i håndteringsinstrukserne.

Enhver verifikation af certifikater/nøgler på en hvilken som helst måde mellem parterne sker via en anden kanal.

BILAG III

TEKNISKE STANDARDER FOR SAMMENKOBLING I HENHOLD TIL ARTIKEL 3, STK. 7, I AFTALEN MELLEM DEN EUROPÆISKE UNION OG DET SCHWEIZISKE FORBUND OM SAMMENKOBLING AF DERES SYSTEMER FOR HANDEL MED DRIVHUSGASEMISSIONER

Standarder for permanent registerforbindelse

Indhold

1. ORDLISTE 21
2. INDLEDNING 22
2.1. Anvendelsesområde 22
2.2. Adressater 23
3. ALMINDELIGE BESTEMMELSER 23
3.1. Kommunikationsforbindelsens arkitektur 23
3.1.1. Udveksling af meddelelser 23
3.1.2. XML-meddelelse – beskrivelse på højt plan 23
3.1.3. Datafangstvinduer 24
3.1.4. Transaktionsmeddelelsesstrømme 24
3.2. Sikker dataoverførsel 26
3.2.1. Sammenkobling mellem firewall netværk 26
3.2.2. Virtuelt privat netværk (VPN) 26
3.2.3. IPSec-implementering 27
3.2.4. Sikker overførselsprotokol til udveksling af meddelelser 27
3.2.5. XML-kryptering og -signatur 27
3.2.6. Krypteringsnøgler 27
3.3. Liste over funktioner under sammenkoblingen 27
3.3.1. Forretningstransaktioner 28
3.3.2. Afstemningsprotokol 28
3.3.3. Testmeddelelse 28
3.4. Krav til journalføring af data 29
3.5. Driftskrav 29
4. BESTEMMELSER OM TILGÆNGELIGHED 30
4.1. Opbygning af kommunikationens tilgængelighed 30
4.2. Initialiserings-, kommunikations-, genaktiverings- og testplan 30
4.2.1. Interne IKT-infrastrukturtest 31
4.2.2. Kommunikationstest 31
4.2.3. Fulde systemtest (ende til ende) 31
4.2.4. Sikkerhedstest 31
4.3. Godkendelses-/testmiljøer 32
5. BESTEMMELSER OM FORTROLIGHED OG INTEGRITET 32
5.1. Sikkerhedstestinfrastruktur 32
5.2. Bestemmelser om suspension og genaktivering af sammenkoblingen 32
5.3. Bestemmelser om sikkerhedsbrud 33

5.4. Retningslinjer for sikkerhedstest 33
5.4.1. Software 33
5.4.2. Infrastruktur 34
5.5. Bestemmelser om risikovurdering 34

1. **ORDLISTE**

Tabel 1-1

Forretningsakronymer og definitioner

Akronym/begreb	Definition
Kvote	En ret til i en nærmere angivet periode at udlede et ton kuldioxidækvivalent, som udelukkende er gyldig til opfyldelse af kravene i en af enhedernes ETS.
CH	Det Schweiziske Forbund.
CHU	Type stationære kvoter, også kaldet CHU2 (med henvisning til Kyoto-protokollens forpligtelsesperiode 2), udstedt af CH.
CHUA	Schweizisk luftfartskvote.
FDP	Fælles driftsprocedurer. Fælles udviklede procedurer til at gennemføre sammenkoblingen mellem EU ETS og Schweiz' ETS.
ETR	Emissionshandelsregister.
ETS	Emissionshandelssystem.
EU	Den Europæiske Union.
EUA	Almindelig EU-kvote.
EUAA	EU-luftfartskvote.
EUCR	Den Europæiske Unions konsoliderede register.
EUTL	EU-transaktionsjournal.
Register	Et regnskabssystem for kvoter udstedt under det ETS, som holder styr på ejerskabet af kvoter, der opbevares på elektroniske konti.
SSTL	Det schweiziske registers supplerende transaktionsjournal.
Transaktion	En proces i et register, der omfatter overdragelse af en kvote fra en konto til en anden konto.
Transaktionsjournalsystem	Transaktionsjournalen indeholder en fortegnelse over hver foreslået transaktion, der sendes fra et register til et andet.

Tabel 1-2

Tekniske akronymer og definitioner

Akronym	Definition
Asymmetrisk kryptografi	Bruger offentlige og private nøgler til at kryptere og dekryptere data.
Certifikatmyndighed	Enhed, der udsteder digitale certifikater.
Krypteringsnøgle	En oplysning, der bestemmer det funktionelle output af en kryptografisk algoritme.
Dekryptering	Omvendt krypteringsproces.
Digital signatur	En matematisk metode til validering af ægthed og integritet af en meddelelse, software eller et digitalt dokument.
Kryptering	Konvertering af oplysninger eller data til en kode, navnlig for at forhindre uautoriseret adgang.
Filfangst	Læsning af en fil.

Akronym	Definition
Firewall	Netsikkerhedsudstyr eller -software, der overvåger og kontrollerer indgående og udgående nettrafik baseret på forudbestemte regler.
Heartbeat-overvågning	Periodisk signal, der genereres og overvåges af hardware eller software for at angive normal drift eller synkronisere andre dele af et computersystem.
IPSec	IP SECurity. Netværksprotokolfamilie, der autentificerer og krypterer datapakkerne med henblik på at sikre krypteret kommunikation mellem to computere via et internetprotokolnetværk.
Penetrationstest	Afprøvning af et computersystem, et netværk eller en webapplikation for at identificere sikkerhedsmæssige sårbarheder, som en angriber kan udnytte.
Afstemningsproces	Sikring af, at to fortegnelser er overensstemmende.
VPN	Virtuelt privat net.
XML	Extensible Mark-up Language. Udviklere kan hermed oprette deres egne skræddersyede tags, der muliggør definition, fremsendelse, validering og fortolkning af data mellem applikationer og mellem organisationer.

2. **INDLEDNING**

Aftalen mellem Den Europæiske Union og Det Schweiziske Forbund om sammenkobling af deres systemer for handel med drivhusgasemissioner af 23. november 2017 (»aftalen«) indeholder bestemmelser om gensidig anerkendelse af emissionskvoter, der kan anvendes til at opfylde kravene i Den Europæiske Unions emissionshandelssystem (»EU ETS«) eller Schweiz' emissionshandelssystem (»Schweiz' ETS«). Med henblik på at gennemføre sammenkoblingen af EU ETS og Schweiz' ETS vil der blive etableret en direkte forbindelse mellem EU-registrets EU-transaktionsjournal (EUTL) og det schweiziske registers supplerende transaktionsjournal (SSTL), som vil muliggøre overdragelse af emissionskvoter udstedt i et af ETS'erne mellem registrene (aftalens artikel 3, stk. 2). For at gennemføre sammenkoblingen af EU ETS og Schweiz' ETS blev der gennemført en foreløbig løsning i 2020. Fra og med 2023 vil registerforbindelsen mellem de to emissionshandelssystemer gradvis blive udviklet hen imod en permanent registerforbindelse, der forventes at blive gennemført senet i 2024, og som gør det muligt for de forbundne markeder at fungere, for så vidt angår fordelene ved markedslikviditet og gennemførelse af transaktioner mellem de to forbundne systemer på en måde, der svarer til et marked bestående af to systemer, og som gør det muligt for markedsdeltagerne at handle, som om de befandt sig på ét marked, kun med det forbehold, at de er underlagt parternes individuelle forskrifter (bilag II til aftalen).

I henhold til aftalens artikel 3, stk. 7, udvikler administratoren af det schweiziske register og Unionens centrale administrator tekniske standarder for sammenkobling på grundlag af de principper, der er opstillet i bilag II til aftalen, som beskriver de detaljerede krav til etablering af en robust og sikker forbindelse mellem SSTL og EUTL. De tekniske standarder for sammenkobling, der udvikles af administratorerne, træder i kraft, når de er vedtaget ved en afgørelse truffet af det fælles udvalg.

De tekniske standarder for sammenkobling blev vedtaget af det fælles udvalg ved afgørelse nr. 2/2020. De opdaterede tekniske standarder for sammenkobling, der fremgår af dette dokument, vil blive vedtaget af det fælles udvalg ved afgørelse nr. 1/2024. I overensstemmelse med denne afgørelse og efter anmodninger fra det fælles udvalg har administratoren af det schweiziske register og Unionens centrale administrator udviklet yderligere tekniske retningslinjer for at gennemføre sammenkoblingen og sikre, at disse løbende tilpasses til den tekniske udvikling og nye krav til sammenkoblingens sikkerhed og sikring og dens effektive drift.

2.1. **Anvendelsesområde**

Dette dokument repræsenterer den fælles forståelse mellem parterne i aftalen om oprettelsen af det tekniske grundlag for forbindelsen mellem registrene under EU ETS og Schweiz' ETS. Udgangspunktet for de tekniske specifikationer, hvad angår kravene til arkitektur, tjenester og sikkerhed, er beskrevet i dokumentet, men der mangler yderligere detaljerede retningslinjer for at kunne gennemføre sammenkoblingen.

For at sikre sammenkoblingens korrekte funktion skal der indføres processer og procedurer for yderligere gennemførelse af den. I henhold til aftalens artikel 3, stk. 6, beskrives disse spørgsmål nærmere i et separat dokument med fælles driftsprocedurer (FDP), der skal vedtages separat ved afgørelse truffet af det fælles udvalg.

2.2. **Adressater**

Dette dokument er stilet til administratoren af det schweiziske register og Unionens centrale administrator.

3. **ALMINDELIGE BESTEMMELSER**

3.1. **Kommunikationsforbindelsens arkitektur**

Dette afsnit har til formål at beskrive den generelle arkitektur bag gennemførelsen af forbindelsen mellem EU's ETS og Schweiz' ETS og de forskellige komponenter, der indgår i den.

Sikkerhed indgår som en vigtig del af fastlæggelsen af registerforbindelsens arkitektur, og alle foranstaltninger er derfor blevet truffet med henblik på at skabe en robust arkitektur. Den permanente registerforbindelse anvender en filudvekslingsmekanisme som gennemførelse af en sikker air gap-forbindelse.

Den tekniske løsning gør brug af:

— en sikker overførselsprotokol til udveksling af meddelelser

— XML-meddelelser

— XML-baseret digital signatur og kryptering

— VPN.

3.1.1. *Udveksling af meddelelser*

Kommunikationen mellem EU-registret og det schweiziske register er baseret på en mekanisme til udveksling af meddelelser via sikrede kanaler. Hver ende råder over et eget datalager for modtagne meddelelser.

Begge parter fører en journal over de modtagne meddelelser, hvoraf også oplysningerne om behandlingen fremgår.

Fejl eller en uventet status skal indberettes som advarsler, og der bør være menneskelig kontakt mellem de ansvarlige supporthold.

Fejl og uventede hændelser håndteres under overholdelse af de driftsprocedurer, der er fastlagt i proceduren for håndtering af hændelser i FDP.

3.1.2. *XML-meddelelse — beskrivelse på højt plan*

En XML-meddelelse indeholder en af følgende:

— en eller flere transaktionsanmodninger og/eller et eller flere transaktionssvar

— en operation/et svar i forbindelse med afstemning

— en testmeddelelse.

Alle meddelelser omfatter et sidehoved med:

— ophavs-ETS

— sekvensnummer.

3.1.3. *Datafangstvinduer*

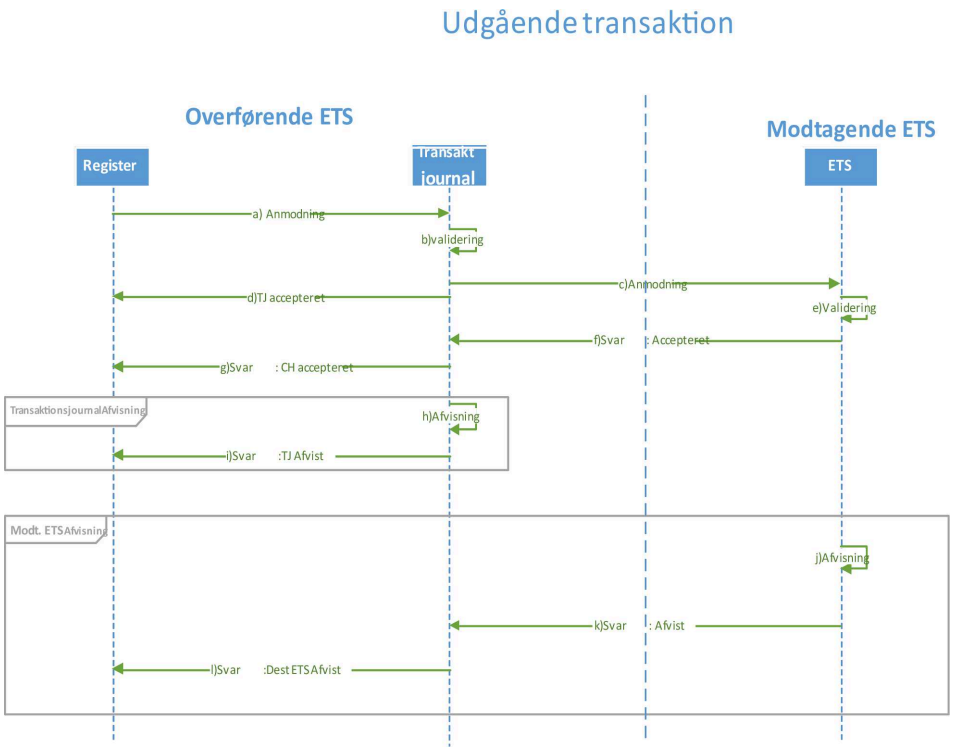
Den permanente registerforbindelse er baseret på forhåndsfastsatte datafangstvinduer, der efterfølges af en række navngivne begivenheder. De transaktionsanmodninger, der modtages via forbindelsen, vil kun blive fanget med på forhånd fastsatte intervaller. Datafangstvinduerne omfatter en teknisk validering af udgående og indgående transaktioner. Desuden kan der på daglig basis foregå afstemninger, og disse kan tilmed udløses manuelt.

Ændringer i hyppigheden og/eller timingen for disse begivenheder håndteres under overholdelse af de driftsprocedurer, der er fastlagt i proceduren for anmodningsbehandling i FDP.

3.1.4. *Transaktionsmeddelelsesstrømme*

Udgående transaktioner

Dette afspejler det overførende ETS's perspektiv. Den specifikke rækkefølge er vist i følgende sekvensdiagram:



Basisrækkefølgen viser følgende trin (som på tegningen ovenfor):

a) I det overførende ETS sendes transaktionsanmodningen fra registret til transaktionsjournalen efter alle forretningsmæssige forsinkelser (i givet fald 24 timers forsinkelse).

b) Transaktionsjournalen validerer transaktionsanmodningen.

c) Transaktionsanmodningen sendes til destinations-ETS'et.

d) Acceptsvaret sendes til registret under ophavs-ETS'et.

e) Destinations-ETS'et validerer transaktionsanmodningen.

f) Destinations-ETS'et sender acceptsvaret tilbage til ophavs-ETS'ets transaktionsjournal.

g) Transaktionsjournalen sender acceptsvaret til registret.

Alternativ rækkefølge »Transaktionsjournal afvisning« (som på tegningen ovenfor, hvor a) er startpunktet i basisrækkefølgen):

a) I ophavssystemet sendes transaktionsanmodningen fra registret til transaktionsjournalen efter alle forretningsmæssige forsinkelser (i givet fald 24 timers forsinkelse).

b) Transaktionsjournalen validerer ikke anmodningen.

c) Afvisningsmeddelelsen sendes til ophavsregistret.

Alternativ rækkefølge »ETS afvisning« (som på tegningen ovenfor, hvor d) er startpunktet i basisrækkefølgen):

a) I ophavs-ETS'et sendes transaktionsanmodningen fra registret til transaktionsjournalen efter alle forretningsmæssige forsinkelser (i givet fald 24 timers forsinkelse).

b) Transaktionsjournalen validerer transaktionen.

c) Transaktionsanmodningen sendes til destinations-ETS'et.

d) Acceptmeddelelsen sendes til registret under ophavs-ETS'et.

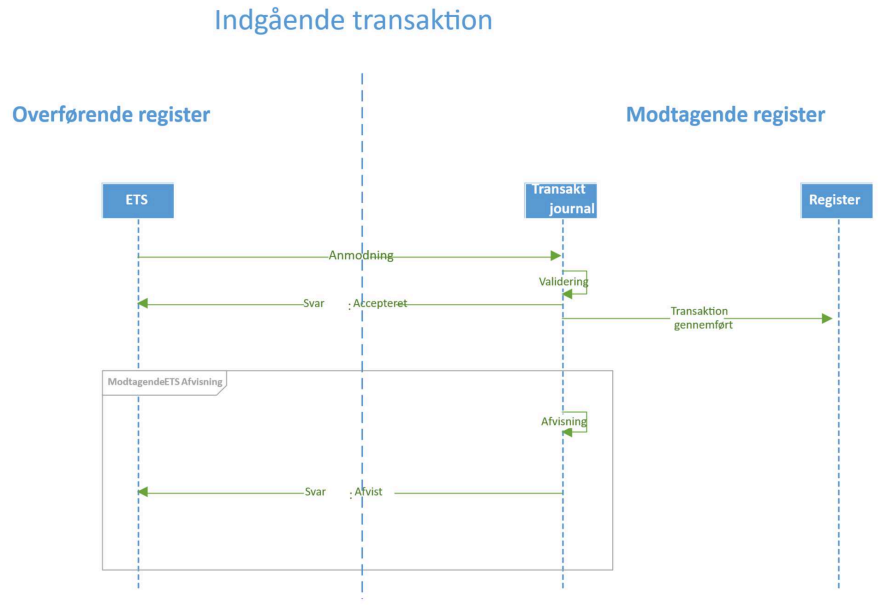
e) Det modtagende ETS's transaktionsjournal validerer ikke transaktionen.

f) Det modtagende ETS sender afvisningssvaret til det overførende ETS's transaktionsjournal

g) Transaktionsjournalen sender afvisningen til registret.

Indgående transaktioner

Dette afspejler det modtagende ETS's perspektiv. Den specifikke rækkefølge er vist i følgende sekvensdiagram:



Diagrammet viser:

1) Når det modtagende ETS's transaktionsjournal validerer anmodningen, sender den acceptmeddelelsen til det overførende ETS og en »transaktion gennemført«-meddelelse til registret under det modtagende ETS.

2) Hvis en indgående anmodning afvises i den modtagende transaktionsjournal og bliver afvist, sendes transaktionsanmodningen ikke til registret under det modtagende ETS.

Protokol

Cyklus for transaktionsmeddelelser omfatter kun to meddelelser:

— Transaktionsforslag fra overførende ETS → modtagende ETS.

— Transaktionssvar fra modtagende ETS → overførende ETS: enten Accepteret eller Afvist (herunder årsagen til afvisning).

  — Accepteret: Transaktionen er gennemført.

  — Afvist: Transaktionen er afsluttet.

Transaktionsstatus

— Transaktionsstatus for det overførende ETS sættes til »foreslået«, når anmodningen sendes af sted.

— Transaktionsstatus for det modtagende ETS sættes til »foreslået« ved modtagelse og behandling af anmodningen.

— Transaktionsstatus for det modtagende ETS sættes til »gennemført«/ »afsluttet«, når forslaget er blevet behandlet. Det modtagende ETS sender efterfølgende den pågældende accept-/afvisningsmeddelelse.

— Transaktionsstatus for det overførende ETS sættes til gennemført/afsluttet ved modtagelse og behandling af accepten/afvisningen.

— I det overførende ETS angives transaktionsstatus fortsat som foreslået, så længe der ikke er modtaget et svar.

— Transaktionsstatus for det modtagende ETS sættes til »afsluttet«, hvis en foreslået transaktion fortsat er »foreslået« efter 30 minutter.

Hændelser i forbindelse med transaktioner håndteres under overholdelse af de driftsprocedurer, der er fastlagt i proceduren for håndtering af hændelser i FDP.

3.2. **Sikker dataoverførsel**

Der gælder fire sikkerhedsniveauer for dataoverførsler:

1) netadgangskontrol: sammenkoblingslag mellem firewall og netværk

2) kryptering på transportniveau: VPN

3) kryptering på sessionsniveau: sikker overførselsprotokol til udveksling af meddelelser

4) kryptering på applikationsniveau: kryptering og signering af XML-indhold.

3.2.1. *Sammenkobling mellem firewall og netværk*

Sammenkoblingen etableres via et net, der er beskyttet af en hardwarebaseret firewall. Firewallen skal konfigureres med regler, der sikrer, at kun »registrerede« brugere kan opnå forbindelse til VPN-serveren.

3.2.2. *Virtuelt privat netværk (VPN)*

Al kommunikation mellem parterne skal beskyttes ved hjælp af en VPN-teknologi (virtuelt privat netværk, VPN). VPN-teknologier giver mulighed for at oprette en »tunnel« gennem et netværk som internettet fra et punkt til et andet og herved beskytte al kommunikation. Forud for oprettelsen af VPN-tunnelen udstedes der et digitalt certifikat til et fremadrettet brugerslutpunkt, der giver brugeren mulighed for at fremlægge identitetsdokumentation under forhandlingerne om forbindelsen. Hver part er ansvarlig for at installere certifikatet i sit VPN-slutpunkt. Ved hjælp af digitale certifikater vil hver slut-VPN-server få adgang til en central myndighed til at forhandle autentificeringsdata. Under tunneloprettelsesprocessen forhandles krypteringen, således at det sikres, at al kommunikation gennem tunnelen beskyttes.

Brugerens VPN-slutpunkter skal være konfigureret til permanent at opretholde VPN-tunnellen med henblik på en pålidelig tovejskommunikation i realtid mellem parterne til enhver tid.

Generelt anvender Den Europæiske Union de sikre transeuropæiske tjenester for telematik mellem administrationerne (STESTA) som et privat IP-baseret netværk. Dette netværk er derfor også egnet til den permanente registerforbindelse.

3.2.3. *IPSec-implementering*

Brugen af IPSec-protokollen til oprettelse af VPN-infrastrukturen mellem stederne sikrer autentificering mellem stederne, dataintegritet og datakryptering. IPsec-VPN-konfigurationer sørger for korrekt autentificering mellem to slutpunkter i en VPN-forbindelse. Parterne identificerer og autentificerer fjernbrugeren via IPSec-forbindelsen ved hjælp af et digitalt certifikat fra en certifikatmyndighed, der er anerkendt af den anden part.

IPsec sikrer også dataintegritet for al kommunikation gennem VPN-tunnelen. Datapakker hashes og signeres ved hjælp af autentifikationsinformation som etableret af VPN'en. IPSec-krypteringen sikrer endvidere datafortrolighed.

3.2.4. *Sikker overførselsprotokol til udveksling af meddelelser*

Den permanente registerforbindelse bygger på flere krypteringslag til sikker udveksling af data mellem parterne. Begge systemer og deres forskellige miljøer er indbyrdes forbundet på netniveau ved hjælp af VPN-tunneller. På applikationsniveau overføres filerne ved hjælp af en sikker overførselsprotokol til udveksling af meddelelser på sessionsniveau.

3.2.5. *XML-kryptering og -signatur*

I forbindelse med XML-filer sker signering og kryptering på to niveauer. Hver transaktionsanmodning, hvert transaktionssvar og hver afstemningsmeddelelse signeres digitalt hver for sig.

På andet trin krypteres hver underdel i »meddelelses-«elementet for sig.

Som et tredje trin — for at sikre integriteten og uafviseligheden af hele meddelelsen — signeres basiselementmeddelelsen digitalt. Dette resulterer i et højt beskyttelsesniveau for de XML-indbyggede data. Den tekniske implementering overholder standarderne fra World Wide Web Consortium.

For at dekryptere og kontrollere meddelelsen følges fremgangsmåden i omvendt rækkefølge.

3.2.6. *Krypteringsnøgler*

Der gøres brug af offentlig nøglekryptering til kryptering og signering.

I forbindelse med IPSec anvendes der et digitalt certifikat udstedt af en certifikatmyndighed, som begge parter har tillid til. Denne certifikatmyndighed kontrollerer certifikatindehaverens identitet af og udsteder certifikater, som anvendes til at identificere en organisation og etablere sikre datakommunikationskanaler mellem parterne.

Der bruges krypteringsnøgler til signering og kryptering af kommunikationskanaler og datafiler. De offentlige certifikater udveksles digitalt mellem parterne ved hjælp af sikre kanaler og kontrolleres separat. Denne procedure er en integreret del af proceduren for informationssikkerhedsstyring i FDP.

3.3. **Liste over funktioner under sammenkoblingen**

Sammenkoblingen udgøres af overførselssystemet, som har en række funktioner, der implementerer forretningsprocesserne i henhold til aftalen. Sammenkoblingen omfatter endvidere specifikationen for afstemningsprocessen og for de testmeddelelser, der vil gøre det muligt at implementere heartbeat-overvågning.

3.3.1. *Forretningstransaktioner*

Set fra et forretningsperspektiv omfatter sammenkoblingen fire (4) typer af transaktionsanmodninger:

— Ekstern overdragelse:

  — Efter ikrafttrædelsen af sammenkoblingen mellem ETS'erne er EU's og CH's kvoter ombyttelige og kan dermed overdrages fuldt ud mellem parterne.

  — En overdragelse via sammenkoblingen involverer en overdragelseskonto tilknyttet det ene ETS og en modtagelseskonto tilknyttet det andet ETS.

  — Overdragelsen kan omfatte forskellige mængder af de fire (4) typer af kvoter:

    — schweiziske almindelige kvoter (CHU)

    — schweiziske luftfartskvoter (CHUA)

    — almindelige EU-kvoter (EUA)

    — EU-luftfartskvoter (EUAA)

— International tildeling:

Luftfartøjsoperatører, der administreres af et ETS med forpligtelser i forhold til det andet ETS, og som har ret til at modtage gratis kvoter fra det andet ETS, modtager gratis luftfartskvoter fra det andet ETS gennem den internationale tildelingstransaktion.

— Tilbageførsel af international tildeling:

Denne transaktion finder sted, hvis de samlede gratis kvoter, der er tildelt en luftfartøjsdriftsleder fra det andet ETS, skal tilbageføres i deres helhed.

— Returnering af overskydende tildeling:

Dette minder om en tilbageførsel, men tildelingen skal ikke tilbageføres i sin helhed, og det kun er de overskydende kvoter, der skal returneres til det tildelende ETS.

3.3.2. *Afstemningsprotokol*

Afstemninger vil først finde sted efter afslutning af vinduerne for fangst, validering og behandling af meddelelser.

Afstemninger er en integreret del af foranstaltningerne vedrørende sikkerhed og overensstemmelse i forbindelse med sammenkoblingen. Begge parter skal nå til enighed om den nøjagtige timing for afstemningen, inden der udarbejdes en tidsplan. Der kan finde en planlagt daglig afstemning sted, hvis begge parter er enige herom. Der vil dog som minimum blive gennemført én planlagt afstemning, efter hver fangst har fundet sted.

Under alle omstændigheder kan hver af parterne på et hvilket som helst tidspunkt indlede manuelle afstemninger.

Ændringer i timingen og hyppigheden for den planlagte afstemning håndteres under overholdelse af de driftsprocedurer, der er fastlagt i proceduren for anmodningsbehandling i FDP.

3.3.3. *Testmeddelelse*

En testmeddelelse er fastlagt for at teste ende til ende-kommunikationen. Meddelelsen omfatter data, der identificerer meddelelsen som en test, og vil blive besvaret ved den anden endes modtagelse.

3.4. **Krav til journalføring af data**

For at støtte begge parters behov for at have adgang til nøjagtige og sammenhængende oplysninger og for at tilvejebringe værktøjer, der kan anvendes i afstemningsprocessen for at afhjælpe uoverensstemmelser, arbejder begge parter med fire (4) typer datajournaler:

— transaktionsjournaler

— afstemningsjournaler

— meddelelsesarkiv

— interne revisionsjournaler.

Alle data i disse journaler skal opbevares i mindst tre (3) måneder med henblik på fejlfinding, og deres yderligere lagring afhænger af den revisionslovgivning, der finder anvendelse i hver ende. Journalfiler, der er over tre (3) måneder gamle, kan arkiveres et sikkert sted i et uafhængigt IT-system, så længe de kan hentes eller tilgås inden for en rimelig periode.

Transaktionsjournaler

Både EUTL- og SSTL-undersystemerne er implementeringer af transaktionsjournaler.

Mere specifikt fører transaktionsjournalerne en fortegnelse over hver foreslået transaktion, der er sendt til det andet ETS. Hver enkelt fortegnelse indeholder hele transaktionens indhold og det efterfølgende resultat af transaktionen (svaret fra det modtagende ETS). Transaktionsjournalerne fører også en fortegnelse over de indgående transaktioner samt det svar, der er sendt til ophavs-ETS'et.

Afstemningsjournaler

Afstemningsjournalen indeholder en fortegnelse over hver afstemningsmeddelelse som udvekslet mellem begge parter, herunder afstemnings-ID, tidsstempel og resultatet af afstemningen: afstemningsstatus »Gennemført« eller »Uoverensstemmelser«. I det permanente register er afstemningsmeddelelser en integreret del af de udvekslede meddelelser og lagres derfor som beskrevet i afsnittet »Meddelelsesarkiv«.

Begge parter registrerer hver anmodning og det pågældende svar i afstemningsjournalen. Det kan være nødvendigt at få adgang til disse oplysninger for at afhjælpe uoverensstemmelser, selv om oplysningerne i afstemningsjournalen ikke deles direkte som en del af selve afstemningen.

Meddelelsesarkiv

Begge parter skal arkivere en kopi af de udvekslede data (XML-filer), der sendes og modtages, og hvorvidt disse eller XML-meddelelserne er korrekte i deres format eller ej.

Arkivet er hovedsagelig oprettet til revisionsformål for at kontrollere, hvad der er blevet sendt og modtaget til og fra den anden part. De relaterede certifikater skal således også arkiveres sammen med filerne.

Disse filer indeholder endvidere yderligere oplysninger til fejlfinding.

Intern revisionsjournal

Disse journaler defineres og anvendes særskilt af den enkelte part.

3.5. **Driftskrav**

Udvekslingen af data mellem de to systemer er ikke fuldstændigt selvkørende i den permanente registerforbindelse, hvilket betyder, at der skal operatører og procedurer til for at gennemføre sammenkoblingen. Der er med henblik herpå beskrevet flere roller og værktøjer i denne proces.

4. BESTEMMELSER OM TILGÆNGELIGHED

4.1. Opbygning af kommunikationens tilgængelighed

Arkitekturen for den permanente registerforbindelse er grundlæggende en IKT-infrastruktur og -software, der gør det muligt at kommunikere mellem Schweiz' ETS og EU ETS. I forbindelse med opbygningen af den permanente registerforbindelse bliver det derfor væsentligt at tage højde for, at der for denne datastrøm sikres en høj tilgængelighed, integritet og fortrolighed. Da der er tale om et projekt, hvor IKT-infrastrukturen, den specialdesignede software og processerne spiller en integreret rolle, skal alle tre elementer tages i betragtning med henblik på at opbygge et modstandsdygtigt system.

IKT-infrastrukturens modstandsdygtighed

Kapitlet med de almindelige bestemmelser i dette dokument indeholder en nærmere beskrivelse af arkitekturens elementer. På IKT-infrastruktursiden skaber den permanente registerforbindelse et modstandsdygtigt VPN-netværk, der etablerer sikre kommunikationstunneler til sikker meddelelsesudveksling. Der konfigureres andre infrastrukturelementer med en høj tilgængelighed og/eller understøttet af fallback-mekanismer.

Specialsoftwarens modstandsdygtighed

De specialdesignede softwaremoduler øger modstandsdygtigheden ved at prøve at genopbygge kommunikationen med den anden ende i en given periode, hvis den af en eller anden grund svigter.

Tjenestens modstandsdygtighed

I den permanente registerforbindelse finder dataudveksling mellem parterne sted med foruddefinerede intervaller. Nogle af de trin, der er nødvendige i forbindelse med den planlagte dataudveksling, kræver, at systemoperatører og/eller registeradministratorer manuelt går ind og gør noget. I lyset af ovenstående og for at øge udvekslingernes tilgængelighed og succes:

— I henhold til driftsprocedurerne skal der være tid til udførelse af det enkelte trin.

— Softwaremodulerne til den permanente registerforbindelse gennemfører asynkron kommunikation.

— Den automatiske afstemningsproces registrerer, om der var problemer med at fange datafiler i en af enderne.

— Overvågningsprocesser (IKT-infrastruktur og specialdesignede softwaremoduler) spiller ind og udløser procedurer til håndtering af hændelser (som defineret i dokumentet om de fælles driftsprocedurer). Disse procedurer, der har til formål at reducere den tid, det tager at genetablere normal drift efter hændelser, er af afgørende betydning for at sikre en høj grad af tilgængelighed.

4.2. Initialiserings-, kommunikations-, genaktiverings- og testplan

Alle de forskellige elementer, der indgår i den permanente registerforbindelses arkitektur, skal gennemgå en række individuelle og kollektive test til bekræftelse af, at platformen er klar på IKT-infrastruktur- og informationssystemniveau. Disse driftstest er en obligatorisk forudsætning, hver gang platformen overgår fra suspenderet til driftsstatus for den permanente registerforbindelse.

For at aktivere driftsstatus for sammenkoblingen skal der gennemføres en forud fastlagt testplan. Dette skal bekræfte, at hvert register har gennemgået en række interne test først, efterfulgt af en validering af ende til ende-konnektiviteten inden indgivelse af produktionstransaktioner mellem begge parter.

Testplanen bør indeholde den overordnede teststrategi og nærmere oplysninger om testinfrastrukturen. For hvert element i hver testblok bør den navnlig omfatte:

— testkriterier og -værktøjer

— tildelte roller til gennemførelse af testen

— forventede resultater (positive og negative)

— tidsplan for testen

— journalføring af krav til testresultaterne

— dokumentation af fejlfinding

— eskaleringsbestemmelser.

Som proces kan test til aktivering af driftsstatus opdeles i fire (4) konceptblokke eller faser:

4.2.1. *Interne IKT-infrastrukturtest*

Disse test skal udføres og/eller kontrolleres individuelt af registeradministratorer i hver ende.

Alle IKT-infrastrukturens elementer i hver ende skal testes hver for sig. Dette omfatter hver enkelt komponent af infrastrukturen. Disse test kan udføres automatisk eller manuelt, men skal kontrollere, at alle infrastrukturens elementer er operationelle.

4.2.2. *Kommunikationstest*

Disse test udløses individuelt af en af parterne, og afslutningen af testene kræver samarbejde fra den anden ende.

Når de enkelte elementer er operationelle, skal kommunikationskanalerne mellem de to registre testes. Med henblik herpå skal hver part kontrollere, at der er internetadgang, at der er oprettet VPN-tunneller, og at der er etableret IP-konnektivitet mellem de enkelte steder. Sikring af adgang til lokale og fjerntliggende infrastrukturelementer og IP-konnektivitet bør derefter bekræftes over for den anden ende.

4.2.3. *Fulde systemtest (ende til ende)*

Disse test skal udføres i hver ende, og resultaterne deles med den anden part.

Når kommunikationskanalerne og hver enkelt komponent i begge registre er blevet testet, skal hver ende forberede en række simulerede transaktioner og afstemninger, som er repræsentative for alle de funktioner, der skal implementeres under sammenkoblingen.

4.2.4. *Sikkerhedstest*

Disse test skal udføres og/eller udløses af registeradministratorer i hver ende og som beskrevet i afsnit 5.4. »Retningslinjer for sikkerhedstest« og 5.5. »Bestemmelser om risikovurdering«.

Først når hver af de fire faser/blokke er afsluttet med forudsigelige resultater, kan den permanente registerforbindelse betragtes som operationel.

Testressourcer

Hver part skal råde over specifikke testressourcer (specifik IKT-infrastruktursoftware og -hardware) og skal udvikle testfunktioner i deres respektive systemer for at støtte den manuelle og kontinuerlige validering af platformen. Registeradministratorerne kan til enhver tid udføre manuelle individuelle eller samarbejdsbaserede testprocedurer. Selve aktiveringen af driftsstatus er en manuel proces.

Det er ligeledes fastlagt, at platformen med jævne mellemrum skal udføre automatiske kontroller. Formålet med disse kontroller er at øge platformens tilgængelighed ved at opdage tidlige potentielle infrastruktur- eller softwareproblemer. Denne platformovervågningsplan består af to elementer:

— overvågning af IKT-infrastrukturer: Infrastrukturen overvåges af IKT-infrastrukturtjenesteudbydere i hver ende. De automatiske test omfatter de forskellige infrastrukturelementer og kommunikationskanalernes tilgængelighed

— overvågning af applikationer: Softwaremodulerne til den permanente registersammenkobling implementerer overvågningen af systemkommunikationen på applikationsniveau (enten manuelt og/eller med regelmæssige mellemrum), som tester sammenkoblingens ende til ende-tilgængelighed ved at simulere nogle af transaktionerne via sammenkoblingen.

4.3. **Godkendelses-/testmiljøer**

EU-registrets og det schweiziske registers arkitektur består af følgende tre miljøer:

— produktion (PROD): Dette miljø omfatter de reelle data og behandler de reelle transaktioner

— godkendelse (ACC): Dette miljø omfatter ikkereelle eller anonymiserede, repræsentative data. Begge parters systemoperatører validerer nye frigivelser inden for dette miljø

— test (TEST): Dette miljø omfatter ikkereelle eller anonymiserede, repræsentative data. Dette miljø er begrænset til registeradministratorer og skal bruges, så begge parter kan udføre integrationstest.

Bortset fra VPN fungerer de tre miljøer helt uafhængigt af hinanden, dvs. hardware, software, databaser, virtuelle miljøer, IP-adresser og porte etableres og drives uafhængigt af hinanden.

Hvad angår VPN-opbygningen, skal kommunikationen mellem de tre miljøer være fuldstændig uafhængig, hvilket sikres ved hjælp af STESTA.

5. **BESTEMMELSER OM FORTROLIGHED OG INTEGRITET**

I sikkerhedsmekanismer og -procedurer benyttes metoden med to personer (fire øjne-princippet) i forbindelse med operationer knyttet til forbindelsen mellem EU-registret og det schweiziske register. Metoden med to personer anvendes, når det er nødvendigt. Den finder dog ikke nødvendigvis anvendelse på alle de trin, som registeradministratorerne udfører.

Der tages højde for sikkerhedskravene, som behandles i sikkerhedsstyringsplanen, der også omfatter processer i forbindelse med håndtering af sikkerhedshændelser efter et eventuelt sikkerhedsbrud. Den operationelle del af disse processer er beskrevet i de FDP.

5.1. **Sikkerhedstestinfrastruktur**

Hver part forpligter sig til at oprette en sikkerhedstestinfrastruktur (ved hjælp af den fælles software og hardware, der anvendes til registrering af sårbarheder i udviklings- og driftsfasen):

— Denne adskiller sig fra produktionsmiljøet.

— Her analyseres sikkerheden af et team, der er uafhængigt af systemets udvikling og drift.

Hver part forpligter sig til både at foretage statiske og dynamiske analyser.

I tilfælde af dynamiske analyser (såsom penetrationstest) forpligter begge parter sig til almindeligvis at begrænse evalueringerne til godkendelses- og testmiljøer (som defineret i afsnit 4.3. »Godkendelses-/testmiljøer«). Undtagelser fra denne politik skal godkendes af begge parter.

Inden ibrugtagningen i produktionsmiljøet skal alle sammenkoblingens softwaremoduler (som defineret i afsnit 3.1. »Kommunikationsforbindelsens arkitektur«) være sikkerhedstestet.

Testinfrastrukturen skal på både net- og infrastrukturniveau være adskilt fra produktionsinfrastrukturen. De sikkerhedstest, der er nødvendige for at kontrollere, at sikkerhedskravene overholdes, udføres i testinfrastrukturen.

5.2. **Bestemmelser om suspension og genaktivering af sammenkoblingen**

Hvis der er mistanke om, at sikkerheden for det schweiziske register, SSTL, EU-registret eller EUTL er blevet kompromitteret, skal hver part straks underrette den anden part og suspendere forbindelsen mellem SSTL og EUTL.

Procedurerne for udveksling af oplysninger, for beslutning om suspension og for beslutning om genaktivering indgår i proceduren for anmodningsbehandling i FDP.

Suspensioner

Suspension af registerforbindelsen i overensstemmelse med bilag II til aftalen kan ske af:

— administrative årsager (f.eks. vedligeholdelse), som er planlagt

— sikkerhedsmæssige årsager (eller IT-infrastruktursvigt), som ikke er planlagt.

I nødsituationer underretter hver part den anden part og suspenderer ensidigt registerforbindelsen.

Hvis der træffes beslutning om suspension af registerforbindelsen, sikrer hver part, at forbindelsen afbrydes på netniveau (ved at blokere dele eller alle indgående og udgående forbindelser).

Beslutningen om at suspendere registerforbindelsen — hvad enten det er planlagt eller ikke er planlagt — træffes i overensstemmelse med proceduren for ændringsstyring eller håndtering af sikkerhedshændelser i FDP.

Genaktivering af kommunikationen

En beslutning om genaktivering af registerforbindelsen træffes som beskrevet i FDP og under alle omstændigheder ikke før, der er gennemført en vellykket sikkerhedstestprocedure som beskrevet i afsnit 5.4. »Retningslinjer for sikkerhedstest« og afsnit 4.2. »Initialiserings-, kommunikations-, genaktiverings- og testplan«.

5.3. **Bestemmelser om sikkerhedsbrud**

Et brud på sikkerheden betragtes som en sikkerhedshændelse, der påvirker fortroligheden og integriteten af følsomme oplysninger og/eller tilgængeligheden af det system, der håndterer dem.

Følsomme oplysninger identificeres i listen over følsomme oplysninger og kan håndteres i systemet eller dele heraf.

Oplysninger, der er direkte relateret til sikkerhedsbruddet, betragtes som følsomme, mærkes med »SPECIAL HANDLING: *ETS Critical*« og håndteres i overensstemmelse med håndteringsinstrukserne, medmindre andet er anført.

Ethvert brud på sikkerheden håndteres i overensstemmelse med kapitlet om håndtering af sikkerhedshændelser i FDP.

5.4. **Retningslinjer for sikkerhedstest**

5.4.1. *Software*

Sikkerhedstesten, herunder i givet fald penetrationstest, skal som minimum udføres på alle nye større frigivelser af software i overensstemmelse med de sikkerhedskrav, der er fastsat i de tekniske standarder for sammenkobling, for at vurdere sammenkoblingens sikkerhed og de dermed forbundne risici.

Hvis der ikke er blevet produceret nogen større frigivelse inden for de sidste 12 måneder, foretages der sikkerhedstest af det nuværende system under hensyntagen til den udvikling i cybertrusler, der har fundet sted de seneste 12 måneder.

Sikkerhedstesten af registerforbindelsen skal foregå i godkendelsesmiljøet og om nødvendigt i produktionsmiljøet og skal koordineres med og aftales mellem begge parter.

Webapplikationstest skal overholde de internationale åbne standarder som dem, der er udviklet af Open Web Application Security Project (OWASP).

5.4.2. *Infrastruktur*

Den infrastruktur, der understøtter produktionssystemet, skal regelmæssigt scannes for sårbarheder (mindst en gang om måneden), og de registrerede sårbarheder skal afhjælpes i henhold til samme princip som defineret i det foregående afsnit ved hjælp af en ajourført sårbarhedsdatabase.

5.5. **Bestemmelser om risikovurdering**

Hvis der skal gennemføres en penetrationstest, skal denne indgå i sikkerhedstesten.

Hver part kan bestille en specialiseret virksomhed til at udføre sikkerhedstesten, forudsat at denne virksomhed:

— råder over færdigheder og erfaringer inden for en sådan sikkerhedstest

— ikke direkte rapporterer til udvikleren og/eller dennes kontrahent og hverken er involveret i udviklingen af sammenkoblingssoftwaren eller er underkontrahent til udvikleren

— har underskrevet fortrolighedsaftalen med henblik på at holde resultaterne fortrolige og behandle dem på niveauet »SPECIAL HANDLING: ETS Critical« i overensstemmelse med håndteringsinstrukserne.