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]

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 3, stk. 7, og artikel 13, stk. 2, heri, og

ud fra følgende betragtninger:

(1) Ved afgørelse nr. 2/2019 truffet af det fælles udvalg den 5. december 2019 ([2]) blev bilag I og II til aftalen ændret med henblik på opfyldelse af sammenkoblingsbetingelserne i aftalen.

(2) Efter vedtagelsen af det fælles udvalgs afgørelse nr. 2/2019 og i overensstemmelse med aftalens artikel 21, stk. 3, har parterne udvekslet deres ratifikations- eller godkendelsesinstrumenter, da de finder, at alle betingelser for sammenkobling er opfyldt.

(3) I overensstemmelse med aftalens artikel 21, stk. 4, trådte aftalen i kraft den 1. januar 2020.

(4) Bilag I til aftalen bør ændres i overensstemmelse med aftalens artikel 13, stk. 2, for at sikre en gnidningsløs omstilling af administrationen af luftfartøjsoperatører, der første gang tilskrives Schweiz, ved at tage hensyn til de fremskridt, der er gjort med hensyn til oprettelsen af registerforbindelsen.

(5) For at tage højde for den seneste udvikling og sikre øget fleksibilitet til at oprette den registerforbindelse, der kræves i henhold til aftalen, bør bilag II til aftalen ændres i overensstemmelse med aftalens artikel 13, stk. 2, for at sikre mere omfattende, men tilsvarende teknologier til oprettelse af registerforbindelsen.

(6) I henhold til aftalens artikel 3, stk. 7, bør administratoren af det schweiziske register og Unionens centrale administrator udvikle tekniske standarder for sammenkobling på grundlag af de principper, der er opstillet i bilag II til aftalen. De tekniske standarder for sammenkobling bør beskrive de detaljerede krav til etablering af en robust og sikker forbindelse mellem det schweiziske registers supplerende transaktionsjournal (SSTL) og EU-registrets EU-transaktionsjournal (EUTL). De tekniske standarder for sammenkobling bør træde i kraft, når de er vedtaget ved afgørelse i det fælles udvalg.

(7) I henhold til aftalens artikel 13, stk. 1, bør det fælles udvalg vedtage tekniske retningslinjer for at sikre den korrekte gennemførelse af aftalen, herunder hvad angår etablering af en robust og sikker forbindelse mellem SSTL og EUTL. De tekniske retningslinjer kan udarbejdes af en arbejdsgruppe nedsat i henhold til aftalens artikel 12, stk. 5. Arbejdsgruppen bør som minimum omfatte administratoren af det schweiziske register og EU's centrale administrator og bør bistå det fælles udvalg i dets funktioner i henhold til aftalens artikel 13.

(8) I betragtning af retningslinjernes tekniske karakter og behovet for at tilpasse dem til den løbende udvikling bør de tekniske retningslinjer, som er udarbejdet af administratoren af det schweiziske register og Unionens centrale administrator, forelægges det fælles udvalg til orientering eller i givet fald godkendelse —

([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 (EUT L 314 af 29.9.2020, s. 68).

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Punkt 17, andet afsnit, i del B i bilag I til aftalen affattes således:

»Luftfartøjsoperatører, der første gang tilskrives Schweiz efter denne aftales ikrafttræden, administreres af Schweiz efter den 30. april i tilskrivningsåret, og så snart den foreløbige registerforbindelse er operationel.«

Artikel 2

Fjerde underafsnit i bilag II til aftalen affattes således:

»I de tekniske standarder for sammenkobling angives det, at kommunikationen mellem SSTL og EUTL udgøres af sikker udveksling af webtjeneste-meddelelser baseret på følgende teknologier (*) eller lignende:

— webtjenester, der anvender SOAP

— hardwarebaseret VPN (Virtual Private Network)

— XML (Extensible Markup Language)

— digital signatur og

— network time-protokoller.

(*) Disse teknologier anvendes aktuelt til at etablere en forbindelse mellem EU-registret og den internationale transaktionsjournal samt mellem det schweiziske register og den internationale transaktionsjournal.«

Artikel 3

De tekniske standarder for sammenkobling, der er knyttet som bilag til denne afgørelse, vedtages hermed.

Artikel 4

Hermed nedsættes der en arbejdsgruppe i henhold til aftalens artikel 12, stk. 5. Den bistår det fælles udvalg med at sikre en korrekt gennemførelse af aftalen, herunder udarbejdelse af tekniske retningslinjer for gennemførelsen af de fælles driftsprocedurer.

Arbejdsgruppen skal som minimum omfatte administratoren af det schweiziske register og EU's centrale administrator.

Artikel 5

Denne afgørelse træder i kraft på dagen for vedtagelsen.

Udfærdiget i Bruxelles, den 5. november 2020.

På det fælles udvalgs vegne	Formand	Caroline BAUMANN
Sekretær for Den Europæiske Union	Beatriz YORDI	Sekretær for Schweiz
Maja-Alexandra DITTEL		

BILAG

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 FORELØBIG LØSNING

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 EU's emissionshandelssystem eller Schweiz' emissionshandelssystem.
CH	Det Schweiziske Forbund.
CHU	Schweiziske almindelige kvoter (begrebet »CHU2« bruges som forkortelse for CHU-kvoter i anden forpligtelsesperiode).
CHUA	Schweizisk luftfartskvote.
FDP	De fælles driftsprocedurer, som parterne i aftalen har udviklet i fællesskab med henblik på at gennemføre sammenkoblingen af EU's emissionshandelssystem og Schweiz' emissionshandelssystem.
EHR	Emissionshandelsregister.
ETS	Emissionshandelssystem.
EU	Den Europæiske Union.
EUK	Almindelig EU-kvote.
EULK	EU-luftfartskvote.
EUKR	Den Europæiske Unions konsoliderede register.
EUTL	EU-transaktionsjournal.
Registrer	Et regnskabssystem for kvoter udstedt under emissionshandelssystemet, som holder styr på ejerskabet af kvoter 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.

Akronym	Definition
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.
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.
Indtrængningstest	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's emissionshandelssystem«) eller Schweiz' emissionshandelssystem. Med henblik på at gennemføre sammenkoblingen af EU's emissionshandelssystem og Schweiz' emissionshandelssystem 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 emissionshandelssystemerne mellem registrene (aftalens artikel 3, stk. 2). For at gennemføre sammenkoblingen mellem EU's emissionshandelssystem og Schweiz' emissionshandelssystem skal en foreløbig løsning være på plads senest i maj 2020 eller så hurtigt som muligt derefter. Parterne samarbejder om at erstatte den foreløbige løsning med en permanent registerforbindelse hurtigst muligt (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 i det fælles udvalg.

De tekniske standarder for sammenkobling, jf. dette dokument, vedtages af det fælles udvalg ved afgørelse nr. 2/2020. I overensstemmelse med denne afgørelse anmoder det fælles udvalg administratoren af det schweiziske register og Unionens centrale administrator om at udvikle 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's emissionshandelssystem og Schweiz' emissionshandelssystem. 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 korrekt funktion skal der indføres processer og procedurer for yderligere gennemførelse af sammenkoblingen. I henhold til aftalens artikel 3, stk. 6, beskrives disse spørgsmål nærmere i et separat dokument med fælles driftsprocedurer (FDP), der vedtages særskilt ved afgørelse i det fælles udvalg.

2.2. *Målgrupper*

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 emissionshandelssystem og Schweiz' emissionshandelssystem og de forskellige komponenter, der indgår i den.

Sikkerhed indgår som en vigtig del af arkitekturen for registerforbindelsen, og alle foranstaltninger er derfor blevet truffet med henblik på at skabe en robust arkitektur. Selv om den planlagte permanente registerforbindelse baseres på webtjenester, vil den foreløbige løsning i stedet anvende en filudvekslingsmekanisme.

Den tekniske løsning gør brug af:

— en sikker overførselsprotokol til udveksling af meddelelser

— XML-meddelelser

— XML-baseret digital signatur og kryptering

— VPN Appliance eller et tilsvarende sikkert datatransportnet.

3.1.1. Udveksling af meddelelser

Kommunikationen mellem EU-registret og det schweiziske register baseres på en mekanisme til udveksling af meddelelser via sikrede kanaler. Hver ende skal råde 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:

— ophavsemissionshandelssystem

— sekvensnummer.

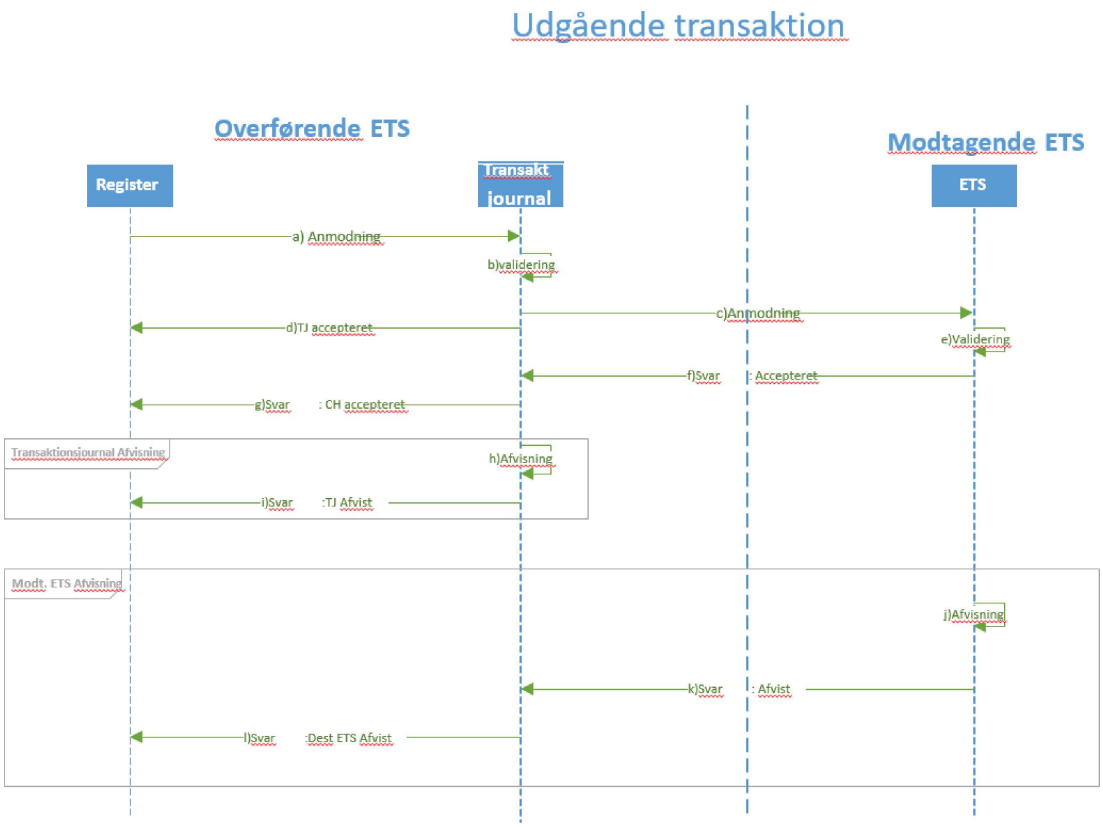
3.1.3. Datafangstvinduer

Den foreløbige løsning 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. Datafangstvinduer 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 hændelser af enhver art 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 emissionshandelssystems perspektiv. Ovenstående sekvensdiagram viser alle de specifikke udgående transaktionsstrømme.

Basisrækkefølgen »Normal transaktion« (med de trin, der er vist på ovenstående tegning):

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

b) Transaktionsjournalen validerer transaktionsanmodningen.

c) Transaktionsanmodningen sendes til destinationsemissionshandelssystemet.

d) Acceptsvaret sendes til registret under ophavsemissionshandelssystemet.

e) Destinationsemissionshandelssystemet validerer transaktionsanmodningen.

(f) Destinationsemissionshandelssystemet sender acceptsvaret tilbage til ophavsemissionshandelssystemets transaktionsjournal.

g) Transaktionsjournalen sender acceptsvaret til registret.

Alternativ rækkefølge »Transaktionsjournal afvisning« (med de trin, der er vist på ovenstående tegning. Her er a) ligeledes startpunktet):

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

Efterfulgt af:

b) Transaktionsjournalen validerer ikke anmodningen.

c) Afvisningsmeddelelsen sendes til ophavsregistret.

Alternativ rækkefølge »ETS Afvisning« (med de trin, der er vist på ovenstående tegning. Her er a) startpunktet):

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

b) Transaktionsjournalen validerer transaktionen.

c) Transaktionsanmodningen sendes til destinationsemissionshandelssystemet.

d) Acceptmeddelelsen sendes til registret under ophavsemissionshandelssystemet.

Efterfulgt af:

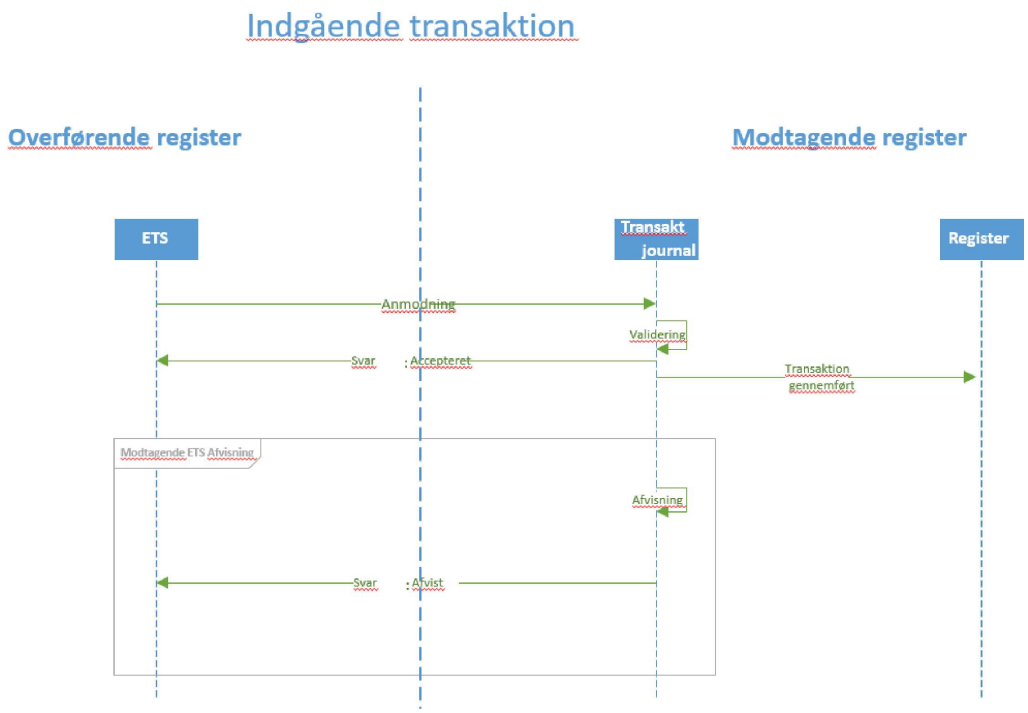
e) Det modtagende emissionshandelssystems transaktionsjournal validerer ikke transaktionen.

f) Det modtagende emissionshandelssystem sender afvisningssvaret til det overførende emissionshandelssystems transaktionsjournal

g) Transaktionsjournalen sender afvisningen til registret.

Indgående transaktioner

Dette afspejler det modtagende emissionshandelssystems perspektiv. Den specifikke rækkefølge er vist i følgende sekvensdiagram:



Diagrammet viser:

1. Når det modtagende emissionshandelssystems transaktionsjournal validerer anmodningen, sender den acceptmeddelelsen til det overførende emissionshandelssystem og en »transaktion gennemført«-meddelelse til registret under det modtagende emissionshandelssystem.
2. Hvis en indgående anmodning afvises i den modtagende transaktionsjournal og bliver afvist, sendes transaktionsanmodningen ikke til registret under det modtagende emissionshandelssystem.

Protokol

Cyklus for transaktionsmeddelelser omfatter kun to meddelelser:

— Transaktionsforslag fra overførende emissionshandelssystem modtagende emissionshandelssystem.

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

  — Accepteret: Transaktionen gennemføres.

  — Afvist: Transaktionen afsluttes.

Transaktionsstatus

— Transaktionsstatus for det overførende emissionshandelssystem sættes til "foreslået", når anmodningen sendes af sted.

— Transaktionsstatus for det modtagende emissionshandelssystem sættes til "foreslået" ved modtagelse og behandling af anmodningen.

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

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

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

— Transaktionsstatus for det overførende emissionshandelssystem sættes til »afsluttet«, hvis en foreslået transaktion fortsat har status som »foreslået« efter mere end 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 eller et tilsvarende sikkert datatransportnet

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 sikker datatransportteknologi. I tilfælde af et virtuelt privat netværk (VPN) bør infrastrukturen være baseret på hardware eller virtuelle enheder. 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.

Enhver anden tilsvarende løsning skal være i overensstemmelse med ovennævnte principper.

3.2.3. IPSec-implementering

Hvis der gøres brug af en VPN-løsning, sikrer brugen af IPSec-protokollen til oprettelse af VPN-infrastrukturen mellem stederne 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 foreløbige løsning 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 eller tilsvarende sikre datatransportnet. 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 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 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 emissionshandelssystemerne 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 emissionshandelssystem og en modtagelseskonto tilknyttet det andet emissionshandelssystem.

— 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 emissionshandelssystem med forpligtelser i forhold til det andet emissionshandelssystem, og som har ret til at modtage gratis kvoter fra det andet emissionshandelssystem, modtager gratis luftfartskvoter fra det andet emissionshandelssystem 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 emissionshandelssystem, 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 emissionshandelssystem.

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 som minimum blive gennemført mindst én planlagt afstemning, efter at 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 har til formål 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. *Standarder for webtjenester*

Der vil ikke blive gjort brug af webtjenester i forbindelse med den foreløbige løsning. Det er dog værd at bemærke, at XML-meddelelsernes form og format i vid udstrækning forbliver uændret. Med indførelsen af den permanente registerforbindelse i fremtiden bør webtjenester give mulighed for udveksling af XML-meddelelser i realtid.

3.5. *Specifik definition af webtjenester*

Dette afsnit er ikke relevant i forbindelse med den foreløbige løsning. Som anført i foregående afsnit vil der udelukkende blive gjort brug af webtjenester i forbindelse med den fremtidige permanente registerforbindelse.

3.6. *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 omfatter implementeringer af transaktionsjournaler.

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

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 den foreløbige løsning udgør afstemningsmeddelelserne en integreret del af de udvekslede meddelelser.

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.

3.7. *Driftskrav*

Udvekslingen af data mellem de to systemer er ikke fuldstændigt selvkørende i den foreløbige løsning. Det betyder, at der skal operatører og procedurer til for at gennemføre sammenkoblingen.

4. **Bestemmelser om tilgængelighed**

4.1. *Opbygning af kommunikationens tilgængelighed*

Arkitekturen for den foreløbige løsning er grundlæggende en IKT-infrastruktur og -software, der gør det muligt at kommunikere mellem Schweiz' og EU's emissionshandelssystem. I forbindelse med opbygningen af den foreløbige løsning og 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 foreløbige sammenkobling et modstandsdygtigt VPN-netværk (eller tilsvarende), 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 i en given periode med den anden ende, hvis kommunikationen af en eller anden grund svigter.

Tjenestens modstandsdygtighed

I den foreløbige løsning finder dataudvekslingen mellem parterne sted på foruddefinerede tidspunkter i løbet af året. 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 rigelig tid til udførelse af det enkelte trin.

— Softwaremodulerne til den foreløbige løsning 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 foreløbige løsnings 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 foreløbige løsning.

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 begge parter i hver ende.

Alle IKT-infrastrukturens elementer i hver ende skal testes 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 (eller et tilsvarende sikkert transportnet), 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 ved 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 begge parter i hver ende og som beskrevet i afsnit 5.4, »Retningslinjer for sikkerhedstest«, og afsnit 5.5, »Bestemmelser om risikovurdering«.

Først når hver af de fire faser/blokke er afsluttet med forudsigelige resultater, kan den foreløbige sammenkobling 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 foreløbig sammenkobling 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 knyttet til 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 (eller et tilsvarende net) 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, består denne af to forskellige miljøer — et for PROD og et andet uafhængigt for ACC og TEST.

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 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 at foretage både statiske og dynamiske analyser.

I tilfælde af dynamiske analyser (såsom indtrængningstest) 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 inden for testinfrastrukturen.

5.2. *Bestemmelser om suspension og genaktivering af sammenkoblingen*

Hvis der er mistanke om, at sikkerheden for Schweiz' 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 derfor, 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 genaktiveringsbeslutning 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 »ETS KRITISK« 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 indtrængningstest, 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. Test udføres efter den metode, der er beskrevet i afsnit 5.4.1, ved hjælp af en ajourført sårbarhedsdatabase.

5.5. *Bestemmelser om risikovurdering*

Hvis der skal gennemføres en indtrængningstest, 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 »ETS KRITISK« i overensstemmelse med håndteringsinstrukser.