BESLUT nr 2/2020 AV DEN GEMENSAMMA KOMMITTÉ SOM INRÄTTATS GENOM AVTALET MELLAN EUROPEISKA UNIONEN OCH SCHWEIZISKA EDSFÖRBUNDET OM SAMMANKOPPLING AV DERAS UTSLÄPPSHANDELSSYSTEM FÖR VÄXTHUSGASER

av den 5 november 2020

om ändring av bilagorna I och II till avtalet och antagande av tekniska standarder för sammankoppling [2021/1034]

DEN GEMENSAMMA KOMMITTÉN HAR ANTAGIT DETTA BESLUT,

med beaktande av avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser ([1]) (*avtalet*), särskilt artikel 3.7 och artikel 13.2, och

av följande skäl:

1) Genom den gemensamma kommitténs beslut nr 2/2019 av den 5 december 2019 ([2]) ändrades bilagorna I och II till avtalet, vilket innebär att de villkor för sammankoppling som anges i avtalet därmed är uppfyllda.

2) Efter antagandet av beslut nr 2/2019 av den gemensamma kommittén och i enlighet med artikel 21.3 i avtalet har parterna utväxlat sina ratifikations- eller godkännandeinstrument, eftersom de anser att samtliga villkor för sammankoppling som anges i avtalet är uppfyllda.

3) I enlighet med artikel 21.4 i avtalet trädde avtalet i kraft den 1 januari 2020.

4) Bilaga I till avtalet bör ändras i enlighet med artikel 13.2 i avtalet för att säkerställa en friktionsfri övergång i administrationen av luftfartygsoperatörer som tillskrivs Schweiz första gången genom beaktande av framstegen med att upprätta registerkopplingen.

5) För att ta hänsyn till den senaste utvecklingen och säkerställa ökad flexibilitet i upprättandet av den registerkoppling som krävs enligt avtalet, bör bilaga II till avtalet ändras i enlighet med artikel 13.2 i avtalet för att göra det möjligt att använda en större men likvärdig uppsättning teknik för att upprätta registerkopplingen.

6) Enligt artikel 3.7 i avtalet ska den schweiziska registerförvaltaren och unionens centrala förvaltare utarbeta tekniska standarder för sammankoppling baserade på principerna i bilaga II till avtalet. De tekniska standarderna för sammankoppling ska beskriva de detaljerade kraven för att upprätta en robust och säker förbindelse mellan den schweiziska kompletterande transaktionsförteckningen (SSTL) och unionens transaktionsförteckning (EUTL). De tekniska standarderna för sammankoppling ska träda i kraft när de antagits genom beslut av den gemensamma kommittén.

7) I enlighet med artikel 13.1 i avtalet ska den gemensamma kommittén enas om tekniska riktlinjer för att säkerställa att avtalet genomförs på korrekt sätt, inbegripet för att upprätta en robust och säker förbindelse mellan SSTL och EUTL. Tekniska riktlinjer får utarbetas av en arbetsgrupp som är inrättad i enlighet med artikel 12.5 i avtalet. Arbetsgruppen bör minst omfatta förvaltaren av det schweiziska registret och unionens centrala förvaltare och bistå den gemensamma kommittén i dess uppgifter enligt artikel 13 i avtalet.

8) Mot bakgrund av riktlinjernas tekniska karaktär och behovet att anpassa dem till utvecklingen bör de tekniska riktlinjer som utarbetas av den schweiziska registerförvaltaren och unionens centrala förvaltare läggas fram inför den gemensamma kommittén för kännedom eller, vid behov, godkännande.

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

([2]) Beslut nr 2/2019 av den gemensamma kommitté som inrättats genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser av den 5 december 2019 om ändring av bilagorna I och II till avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser (EUT L 314, 29.9.2020, s. 68).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Andra stycket i punkt 17 i del B av bilaga I till avtalet ska härmed ersättas med följande text:

”De luftfartygsoperatörer som tillskrivs Schweiz första gången efter att detta avtal träder i kraft ska administreras av Schweiz efter den 30 april det året och när den provisoriska registerkopplingen har tagits i drift.”

Artikel 2

Fjärde stycket i bilaga II till avtalet ska härmed ersättas med följande text:

”I de tekniska standarderna för sammankoppling ska anges att kommunikationen mellan SSTL och EUTL ska utgöras av utväxling av webbtjänstmeddelanden baserat på följande teknik (*) eller likvärdig teknik:

— Webbtjänster som använder Simple Object Access Protocol (SOAP).

— Hårdvarubaserat virtuellt privat nät (VPN).

— XML (Extensible Markup Language).

— Digital signatur.

— NTP (Network Time Protocol).

_____

(*) Denna teknik används i dag för att upprätta en förbindelse mellan unionsregistret och den internationella transaktionsförteckningen, liksom för förbindelsen mellan det schweiziska registret och den internationella transaktionsförteckningen.”

Artikel 3

Härmed antas de tekniska standarder för sammankoppling som bifogas detta beslut.

Artikel 4

Härmed ska en arbetsgrupp inrättas i enlighet med artikel 12.5 i avtalet. Denna ska bistå den gemensamma kommittén i att säkerställa att avtalet genomförs på korrekt sätt, bland annat genom att utarbeta tekniska riktlinjer för genomförandet av de tekniska standarderna för sammankoppling.

Arbetsgruppen ska minst omfatta den schweiziska registerförvaltaren och unionens centrala förvaltare.

Artikel 5

Detta beslut träder i kraft samma dag som det antas.

Utfärdat i Bryssel den 5 november 2020.

På gemensamma kommitténs vägnar	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL	Ordförande	Sekreterare för Schweiz
Sekreterare för Europeiska unionen		

BILAGA

Standarder för sammankoppling (LTS) i enlighet med artikel 3.7 i avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser

STANDARDER FÖR EN PROVISORISK LÖSNING

1. **Ordlista**

Tabell 1-1

Verksamhetsrelaterade förkortningar och definitioner

Förkortning/Term	Definition
Utsläppsrätt	En rätt att släppa ut ett ton koldioxidekvivalenter under en fastställd period, som är giltig endast för uppfyllande av de krav som fastställs i unionens utsläppshandelssystem eller Schweiz utsläppshandelssystem.
Schweiz	Schweiziska edsförbundet
CHU	Schweiziska allmänna utsläppsrätter (termen ”CHU2” används som förkortning för schweiziska allmänna utsläppsrätter under andra åtagandeperioden).
CHUA	Schweizisk utsläppsrätt för luftfart
COP	Gemensamma driftsförfaranden som parterna i avtalet gemensamt har tagit fram för att praktiskt genomföra sammankopplingen av unionens utsläppshandelssystem och Schweiz utsläppshandelssystem.
ETR	Register för handel med utsläppsrätter
Utsläppshandelssystem	System för handel med utsläppsrätter
EU	Europeiska unionen
EUA	Allmän utsläppsrätt
EUAA	Utsläppsrätt för luftfart
EUCR	EU:s konsoliderade register
EUTL	EU:s transaktionsförteckning
Register	Ett redovisningssystem för utsläppsrätter som utfärdats inom ramen för utsläppshandelssystemet för att hålla reda på innehavaren av utsläppsrätter på elektroniska konton.
SSTL	Den schweiziska kompletterande transaktionsförteckningen
Transaktion	En process i ett register som inbegriper överföring av en utsläppsrätt från ett konto till ett annat konto.
Transaktionsförteckning	Transaktionsförteckningen omfattar alla föreslagna transaktioner som skickas från ett register till ett annat.

Tabell 1-2

Tekniska förkortningar och definitioner

Förkortning	Definition
Asymmetriskt kryptosystem	Krypterar och dekrypterar data med hjälp av öppna och privata nycklar.
Certifikatutfärdare	Enhet som utfärdar digitala certifikat.

Förkortning	Definition
Krypteringsnyckel	Information som bestämmer en krypteringsalgoritms funktionella utdata.
Dekryptering	Motsatsen till kryptering.
Digital signatur	En matematisk metod som används för kontroll av ett meddelandes, programs eller digitalt dokuments äkthet och integritet.
Kryptering	Att omvandla information eller data till kod, särskilt för att förhindra obehörig åtkomst.
Filintagning	Att läsa en fil.
Brandvägg	En apparat eller ett program för nätverkssäkerhet som övervakar och kontrollerar inkommande och utgående nättrafik enligt bestämda regler.
Heartbeat-övervakning	Periodisk signal som avges och övervakas av hårdvara eller programvara för att bekräfta att driften är normal eller för att synkronisera andra delar av ett datorsystem.
IPSec	IP SECurity. Nätverksprotokoll som autentiserar och krypterar datapaket för säker krypterad kommunikation mellan två datorer över ett IP-nätverk.
Penetrationsprovning	Provning av ett datorsystem, ett nätverk eller en webbapplikation för att hitta sårbarheter som en angripare skulle kunna utnyttja.
Avstämning	Att säkerställa att två uppsättningar av uppgifter överensstämmer med varandra.
VPN	Virtuellt privat nät.
XML	*Extensible Mark-up Language*. Gör att webbdesigner kan skapa sina egna specialtaggar, vilket möjliggör definition, överföring, validering och tolkning av data mellan applikationer och mellan organisationer.

2. **Inledning**

Avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser av den 23 november 2017 (*avtalet*) innehåller bestämmelser om ett ömsesidigt erkännande av utsläppsrätter som kan användas för fullgörande i Europeiska unionens utsläppshandelssystem eller i Schweiz utsläppshandelssystem. För att praktiskt genomföra sammankopplingen av unionens utsläppshandelssystem och Schweiz utsläppshandelssystem ska en direkt koppling mellan unionens transaktionsförteckning (EUTL) och den schweiziska kompletterande transaktionsförteckningen (SSTL) i det schweiziska registret upprättas, vilket kommer att möjliggöra överföring mellan registren av utsläppsrätter som har utfärdats i något av utsläppshandelssystemen (artikel 3.2 i avtalet). För att praktiskt genomföra sammankopplingen av EU:s utsläppshandelssystem och Schweiz utsläppshandelssystem ska en provisorisk lösning vara införd i maj 2020, eller så snart som möjligt därefter. Parterna ska samarbeta för att så snart som möjligt ersätta den provisoriska lösningen med den permanenta registerkopplingen (bilaga II till avtalet).

Enligt artikel 3.7 i avtalet ska den schweiziska registerförvaltaren och unionens centrala förvaltare utarbeta tekniska standarder för sammankoppling baserade på principerna i bilaga II till avtalet, där de detaljerade kraven för att upprätta en robust och säker förbindelse mellan SSTL och EUTL beskrivs. De tekniska standarder för sammankoppling som förvaltarna utarbetar ska träda i kraft när de antagits genom beslut av den gemensamma kommittén.

De tekniska standarder för sammankoppling som anges i detta dokument ska antas av den gemensamma kommittén genom dess beslut nr 2/2020. I enlighet med detta beslut ska den gemensamma kommittén be den schweiziska registerförvaltaren och unionens centrala förvaltare att fastställa ytterligare tekniska riktlinjer för att praktiskt genomföra sammankopplingen och säkerställa att dessa kontinuerligt anpassas till den tekniska utvecklingen och nya krav på kopplingens säkerhet och skydd samt till en ändamålsenlig och effektiv drift av kopplingen.

2.1 *Tillämpningsområde*

Detta dokument utgör en gemensam överenskommelse mellan parterna till avtalet avseende fastställandet av en teknisk grund för kopplingen mellan registren i unionens utsläppshandelssystem och Schweiz utsläppshandelssystem. I dokumentet anges baslinjen för de tekniska specifikationerna när det gäller arkitektur-, tjänste- och säkerhetskrav, men vissa ytterligare detaljerade riktlinjer kommer att krävas för att praktiskt genomföra sammankopplingen.

För att kopplingen ska fungera korrekt krävs processer och förfaranden för att praktiskt genomföra den. I enlighet med artikel 3.6 i avtalet ska de närmare detaljerna i dessa beskrivas i det dokument om gemensamma driftsförfaranden som ska antas separat genom beslut av den gemensamma kommittén.

2.2 *Målgrupper*

Detta dokument är riktat till den schweiziska registerförvaltaren och unionens centrala registerförvaltare.

3. **Allmänna bestämmelser**

3.1 *Kommunikationslänkens arkitektur*

Syftet med detta avsnitt är att beskriva den allmänna arkitekturen för att praktiskt genomföra sammankopplingen av EU:s utsläppshandelssystem och Schweiz utsläppshandelssystem samt dess olika komponenter.

Eftersom säkerheten är central för registerkopplingens arkitekturen har man gjort allt för att arkitekturen ska vara robust. Den planerade permanenta registerkopplingen ska bygga på webbtjänster, men den provisoriska lösningen ska i stället använda en mekanism för dataöverföring mellan filer.

Den tekniska lösningen använder

— ett säkert meddelandeöverföringsprotokoll,

— XML-meddelanden,

— XML-baserad digital signatur och kryptering,

— VPN eller ett likvärdigt nätverk för säker dataöverföring.

3.1.1 Utbyte av meddelanden

Kommunikationen mellan unionsregistret och det schweiziska registret ska bygga på utbyte av meddelanden via säkra kanaler. Varje ändpunkt ska ha sin egen databas med mottagna meddelanden.

Båda parterna ska ha en förteckning över de mottagna meddelandena, tillsammans med uppgifter om behandlingen.

Fel eller oväntad status ska rapporteras, som påminnelser, och mänsklig kontakt mellan supportgrupperna ska äga rum.

Fel och oväntade händelser ska hanteras i enlighet med de driftsförfaranden som fastställs i de gemensamma driftsförfarandenas incidenthanteringsprocess.

3.1.2 XML-meddelande – högnivåbeskrivning

Ett XML-meddelande innehåller något av följande:

— En eller flera transaktionsbegäranden och/eller ett eller flera transaktionssvar.

— En operation/ett svar för avstämning.

— Ett provmeddelande.

Varje meddelande har ett huvud med

— avsändande utsläppshandelssystem,

— ordningsnummer.

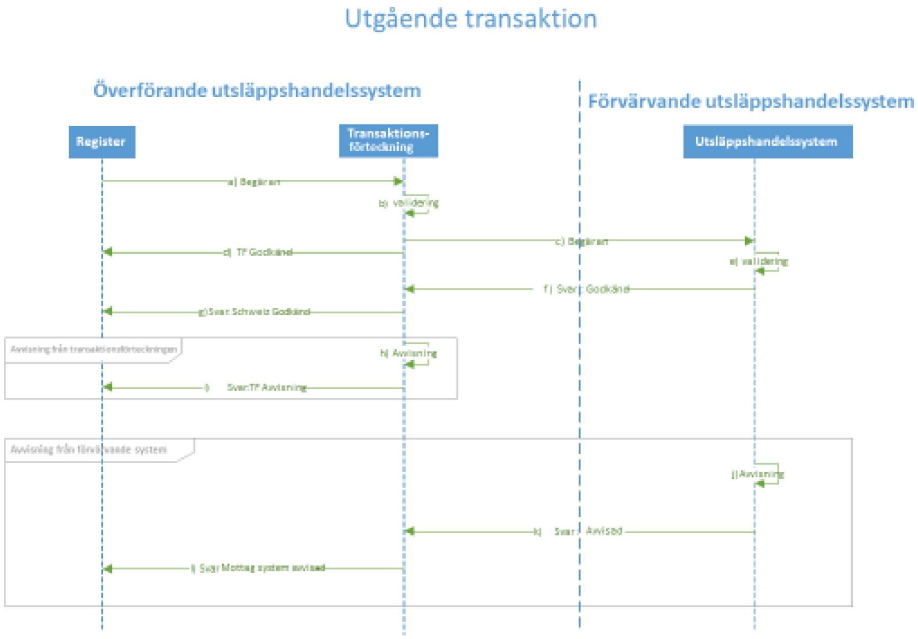
3.1.3 Intagningsluckor

Den provisoriska lösningen bygger på fördefinierade intagningsluckor som följs av en rad namngivna händelser. Transaktionsbegäranden som tas emot via kopplingen inhämtas endast med fördefinierade intervall. Intagningsluckorna omfattar en teknisk kontroll för utgående och inkommande transaktioner. Dessutom får avstämningar köras dagligen och kan startas manuellt.

Ändringar i frekvensen och/eller tidpunkten för dessa händelser hanteras i enlighet med de driftsförfaranden som fastställs i de gemensamma driftsförfarandenas process för tillgodoseende av begäranden.

3.1.4 Meddelandeflöden för transaktioner

Utgående transaktioner



Detta återspeglar det överförande utsläppshandelssystemets synvinkel. I ovanstående sekvensdiagram återges alla särskilda utgående transaktionsflöden.

Huvudflödet ”Normal transaktion” (med stegen angivna i ovanstående diagram):

a) I det överförande utsläppshandelssystemet skickas transaktionsbegäran från registret till transaktionsförteckningen, efter alla fördröjningar (24 timmars fördröjning, i tillämpliga fall).

b) Transaktionsförteckningen validerar transaktionsbegäran.

c) Transaktionsbegäran skickas till det mottagande utsläppshandelssystemet.

d) Svaret om godkännande skickas till det avsändande utsläppshandelssystemets register.

e) Det mottagande utsläppshandelssystemet validerar transaktionsbegäran.

f) Det mottagande utsläppshandelssystemet skickar tillbaka svaret om godkännande till det avsändande utsläppshandelssystemets transaktionsförteckning.

g) Transaktionsförteckningen skickar svaret om godkännande till registret.

Det alternativa flödet ”Avvisning från transaktionsförteckningen” (med stegen angivna i ovanstående diagram, som också inleds med a):

a) I det avsändande utsläppshandelssystemet skickas transaktionsbegäran från registret till transaktionsförteckningen, efter alla fördröjningar (24 timmars fördröjning, i tillämpliga fall).

Följt av följande:

b) Transaktionsförteckningen validerar inte begäran.

c) Avvisningsmeddelande skickas till det avsändande registret.

Det alternativa flödet ”Avvisning från utsläppshandelssystemet” (med stegen angivna i ovanstående diagram, som inleds med a):

a) I det avsändande utsläppshandelssystemet skickas transaktionsbegäran från registret till transaktionsförteckningen, efter alla fördröjningar (24 timmars fördröjning, i tillämpliga fall).

b) Transaktionsförteckningen validerar transaktionen.

c) Transaktionsbegäran skickas till det mottagande utsläppshandelssystemet.

d) Meddelandet om godkännande skickas till det avsändande utsläppshandelssystemets register.

Följt av följande:

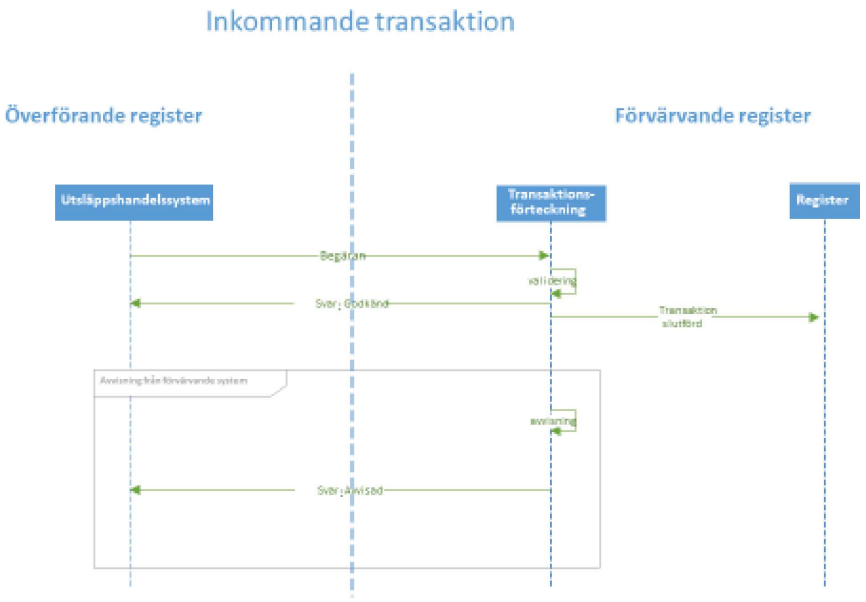
e) Det förvärvande utsläppshandelssystemets transaktionsförteckning validerar inte transaktionen.

f) Det förvärvande utsläppshandelssystemet skickar svaret om avslag till det överförande utsläppshandelssystemets transaktionsförteckning.

g) Transaktionsförteckningen skickar avslaget till registret.

Inkommande transaktioner

Detta återspeglar det förvärvande utsläppshandelssystemets synvinkel. Detta flöde återges i följande sekvensdiagram:



Diagrammet visar följande:

1. När det förvärvande utsläppshandelssystemets transaktionsförteckning har validerat begäran skickar det ett meddelande om godkännande till det överförande utsläppshandelssystemet och ett meddelande om att transaktionen är slutförd till det förvärvande utsläppshandelssystemets register.

2. När en inkommande begäran avslås i den förvärvande transaktionsförteckningen skickas inte transaktionsbegäran till det förvärvande utsläppshandelssystemets register.

Protokoll

Cykeln för transaktionsmeddelanden omfattar endast två meddelanden:

— Transaktionsförslag, överförande system förvärvande system.

— Transaktionssvar, förvärvande system överförande system: antingen Godkänd eller Avvisad (samt skälet till avvisningen).

  — Godkänd: Transaktionen slutförs.

  — Avvisad: Transaktionen avbryts.

Transaktionsstatus

— Det överförande utsläppshandelssystemets transaktionsstatus blir ”föreslagen” när begäran skickas.

— Det förvärvande utsläppshandelssystemets transaktionsstatus blir ”föreslagen” när begäran tas emot och behandlas.

— Det förvärvande systemets transaktionsstatus blir ”slutförd/avbruten” när förslaget har behandlats. Det förvärvande systemet skickar därefter motsvarande meddelande om godkännande/avvisning.

— Det överförande systemets transaktionsstatus blir slutförd/avbruten när godkännandet/avvisningen har tagits emot och behandlats.

— Om inget svar tas emot förblir transaktionsstatusen föreslagen i det överförande systemet.

— Det förvärvande systemet avbryter alla transaktioner som är föreslagna i mer än 30 minuter.

Incidenter som rör transaktioner hanteras i enlighet med de driftsförfaranden som fastställs i de gemensamma driftsförfarandenas incidenthanteringsprocess.

3.2 *Säkerheten för överföring av uppgifter*

Uppgifter som överförs omfattas av fyra säkerhetsnivåer:

1) Kontroll av tillgång till nätverket: brandvägg och skikt för sammankoppling av nätverk.

2) Kryptering på överföringsnivå: VPN eller ett likvärdigt nätverk för säker dataöverföring.

3) Kryptering på sessionsnivå: säkert meddelandeöverföringsprotokoll.

4) Kryptering på applikationsnivå: XML-baserad kryptering och signatur.

3.2.1 Brandvägg och sammankoppling av nätverk

Kopplingen ska upprättas över ett nätverk som skyddas av en hårdvarubaserad brandvägg. Brandväggen ska vara konfigurerad med regler så att endast ”registrerade” slutanvändare kan ansluta sig till VPN-servern.

3.2.2 Virtuellt privat nät (VPN)

All kommunikation mellan parterna ska skyddas med hjälp av teknik för säker dataöverföring. När det gäller virtuella privata nät (VPN) bör infrastrukturen bygga på hårdvara eller virtuella funktionsdatorer. VPN-tekniken ger möjlighet att skapa en ”tunnel” mellan två punkter i ett nätverk som internet för att skydda all kommunikation. Innan VPN-tunneln skapas utfärdas ett digitalt certifikat till en blivande slutanvändare, som gör att slutanvändaren kan styrka sin identitet när förbindelsen upprättas. Varje part har ansvar för att installera certifikatet i sin VPN-ändpunkt. Med hjälp av digitala certifikat ansluter varje VPN-server till en central myndighet för att utverka autentiseringsuppgifter. Trafiken i tunneln är krypterad, vilket gör att all kommunikation genom tunneln är skyddad.

Slutanvändarnas VPN-ändpunkter ska konfigureras så att VPN-tunneln blir permanent och alltid möjliggör tillförlitlig tvåvägskommunikation i realtid mellan parterna.

Alla likvärdiga lösningar ska följa ovanstående principer.

3.2.3 Implementering av IPSec

Om en VPN-lösning används möjliggör användning av IPSec-protokollet för plats-till-plats-VPN autentisering, dataintegritet och datakryptering från plats till plats. VPN-konfigurationer med IPSec säkerställer tillräcklig autentisering mellan två ändpunkter i en VPN-förbindelse. Parterna identifierar och autentiserar fjärrklienten via IPSec-förbindelsen med hjälp av digitala certifikat från den certifikatutfärdare som erkänns av den andra parten.

IPSec säkerställer också dataintegriteten för all kommunikation genom VPN-tunneln. Datapaket hashas och signeras med den autentiseringsinformation som VPN upprättar. Även uppgifternas konfidentialitet garanteras genom IPSec-kryptering.

3.2.4 Säkert meddelandeöverföringsprotokoll

Den provisoriska lösningen använder flera krypteringsskikt för att parterna säkert ska kunna utbyta data. Både systemen och deras olika miljöer är sammankopplade på nätverksnivå genom VPN-tunnlar eller likvärdiga nätverk för säker överföring av uppgifter. På applikationsnivå överförs filerna med hjälp av ett säkert meddelandeöverföringsprotokoll på sessionsnivå.

3.2.5 XML-baserad kryptering och signatur

I XML-filer sker signeringen och krypteringen på två nivåer. Varje transaktionsbegäran, transaktionssvar och avstämningsmeddelande signeras digitalt.

I ett andra steg krypteras varje del av ”meddelande”-elementet individuellt.

Som ett tredje steg signeras dessutom rotelementmeddelandet digitalt för att säkerställa hela meddelandets integritet och oavvislighet. Detta ger ett starkt skydd för inbäddade XML-data. Den tekniska implementeringen följer World Wide Web Consortiums standarder.

För att dekryptera och verifiera meddelandet följs processen i omvänd ordning.

3.2.6 Krypteringsnycklar

För kryptering och signering används kryptosystem med öppna nycklar.

För IPSec ska ett digitalt certifikat från en certifikatutfärdare som båda parterna litar på användas. Denna certifikatutfärdare verifierar certifikatsinnehavarens identiteten och utfärdar certifikat som används för att säkert identifiera en organisation och upprätta kanaler för säker datakommunikation mellan parterna.

Krypteringsnycklar används för att signera och kryptera kommunikationskanaler och datafiler. Certifikaten för öppen nyckel utbyts digitalt av parterna med hjälp av säkra kanaler och verifieras via ytterligare en kanal. Detta förfarande är en väsentlig del av de gemensamma driftsförfarandenas process för informationssäkerhetshantering.

3.3 *Förteckning över funktioner inom ramen för kopplingen*

I kopplingen specificeras överföringssystemet för en rad funktioner som genomför de verksamhetsprocesser som härleder sig från avtalet. Kopplingen omfattar också specifikationen för avstämningen och för de provmeddelanden som möjliggör heartbeat-övervakning.

3.3.1 Verksamhetstransaktioner

Ur verksamhetsperspektiv räknar sammankopplingen med fyra (4) typer av transaktionsbegäranden:

— Extern överföring:

  — Efter att sammankopplingen av utsläppshandelssystemen har trätt i kraft är EU:s och Schweiz utsläppsrätter fungibla, och därmed helt överförbara, mellan parterna.

— En överföring via kopplingen kräver ett överförande konto i ett utsläppshandelssystem och ett förvärvande konto i det andra utsläppshandelssystemet.

— Överföringen kan omfatta valfri mängd av de fyra (4) utsläppsrätterna:

— Schweiziska allmänna utsläppsrätter (CHU)

— Schweiziska utsläppsrätter för luftfart (CHUA)

— Allmänna utsläppsrätter (EUA)

— Utsläppsrätter för luftfart (EUAA)

— Internationell tilldelning:

Luftfartygsoperatörer som administreras av ett utsläppshandelssystem med skyldigheter i det andra utsläppshandelssystemet och med rätt till gratis utsläppsrätter från det andra systemet, kommer att få gratis utsläppsrätter för luftfart från det andra systemet genom transaktionen för internationell tilldelning.

— Upphävande av internationell tilldelning:

Denna transaktion utförs om gratis utsläppsrätter som tilldelats en luftfartygsoperatör av det andra utsläppshandelssystemet måste upphävas helt.

— Återlämnande av övertilldelning:

Liknar upphävandet, men tilldelningen måste inte upphävas helt, och endast övertilldelningen av utsläppsrätter måste återlämnas till det tilldelande utsläppshandelssystemet.

3.3.2 Avstämningsprotokoll

Avstämningar äger endast rum efter att tidluckorna för intagning, validering och behandling av meddelanden har löpt ut.

Avstämningarna är en väsentlig del av sammankopplingens säkerhets- och samstämmighetsåtgärder. Parterna kommer överens om den exakta tidpunkten för avstämningen innan något tidsschema tas fram. Om parterna kommer överens om detta kan avstämningen ske varje dag. Minst en schemalagd avstämning ska utföras efter varje intagning.

Under alla omständigheter kan endera parten när som helst inleda manuella avstämningar.

Ändringar av tidpunkten och frekvensen för den schemalagda avstämningen hanteras i enlighet med de driftsförfaranden som fastställs i de gemensamma driftsförfarandenas process för tillgodoseende av begäranden.

3.3.3 Provmeddelande

Ett provmeddelande ska användas för att testa kommunikationen från ändpunkt till ändpunkt. Meddelandet ska innehålla uppgifter som identifierar det som ett test och besvaras av den andra ändpunkten vid mottagandet.

3.4 *Standarder för webbtjänster*

Webbtjänster ska inte användas i den provisoriska lösningen. Det är dock värt att notera att XML-meddelandenas form och format i stor utsträckning förblir oförändrade. Genom införandet av den permanenta registerkopplingen i framtiden bör webbtjänsterna möjliggöra utbyte av XML-meddelanden i realtid.

3.5 *Definitionen av webbtjänsterna*

Detta avsnitt är inte tillämpligt för den provisoriska lösningen. Som nämnts i föregående avsnitt ska webbtjänster endast användas i den framtida permanenta registerkopplingen.

3.6 *Kraven för uppgiftslagring*

För att tillgodose båda parternas behov av noggrann och konsekvent information, och för att tillhandahålla verktyg för att avhjälpa inkonsekvenser vid avstämningen, ska båda parterna ha fyra (4) typer av uppgiftsförteckningar:

— Transaktionsförteckningar.

— Avstämningsförteckningar.

— Meddelandearkiv.

— Internrevisionsförteckningar.

Alla uppgifter i dessa förteckningar ska sparas i minst tre (3) månader för felsökningsändamål, och deras fortsatta lagring kommer att vara beroende av den tillämpliga lagstiftningen för varje ändpunkt för revisionsändamål. Loggfiler som är äldre än tre (3) månader får arkiveras på en säker plats i ett oberoende it-system, så länge de kan hämtas eller tas fram inom en rimlig tidsperiod.

Transaktionsförteckningar

I både EUTL- och SSTL-delsystemen används transaktionsförteckningar.

Mer bestämt registreras varje föreslagen transaktion som skickas till det andra utsläppshandelssystemet i transaktionsförteckningen. Varje post innehåller alla fält i transaktionsinnehållet samt transaktionens resultat (svaret från det mottagande utsläppshandelssystemet). I transaktionsförteckningarna registreras också inkommande transaktioner samt svaret till det avsändande utsläppshandelssystemet.

Avstämningsförteckningar

Avstämningsförteckningen innehåller uppgifter om varje avstämningsmeddelande som har skickats mellan parterna, däribland avstämnings-id, tidsstämpel och avstämningens resultat: avstämningsstatus ”Godkänd” eller ”Brist på överensstämmelse”. I den provisoriska lösningen är avstämningsmeddelandena en väsentlig del av de skickade meddelandena.

Båda parterna ska föra in varje begäran och dess svar i avstämningsförteckningen. Även om informationen i avstämningsförteckningen inte delas direkt som en del av själva avstämningen kan åtkomst till denna information vara nödvändig för att avhjälpa inkonsekvenser.

Meddelandearkiv

Båda parterna ska arkivera en kopia av de utbytta uppgifterna (XML-filerna), både skickade och mottagna, oavsett om dessa eller XML-meddelandena hade rätt format eller inte.

Arkivet är framför allt till för revisionsändamål, för att ha bevis på vad som har skickats till och mottagits från den andra parten. Utöver filerna måste därför även de tillhörande certifikaten arkiveras.

Dessa filer ger också ytterligare information för felsökningsändamål.

Internrevisionsförteckning

Dessa förteckningar definieras och används på egen hand av varje part.

3.7 *Driftskrav*

Utbytet av uppgifter mellan de båda systemen är inte helt självstyrande i den provisoriska lösningen, vilket innebär att det krävs operatörer och förfaranden för att praktiskt genomföra sammankopplingen.

4. **Tillgänglighet**

4.1 *Utformning för tillgänglig kommunikation*

Arkitekturen för den provisoriska lösningen utgörs i grunden av IKT-infrastruktur och programvara som möjliggör kommunikation mellan Schweiz utsläppshandelssystem och unionens utsläppshandelssystem. Det blir därför väsentligt att säkerställa en hög tillgänglighet, integritet och konfidentialitet för detta dataflöde vid utformningen av den provisoriska lösningen och den permanenta registerkopplingen. Eftersom IKT-infrastrukturen, den specialanpassade programvaran och processerna är nödvändiga i projektet måste alla tre inslagen beaktas för att systemet ska bli motståndskraftigt.

IKT-infrastrukturens motståndskraft

I kapitlet om allmänna bestämmelser i detta dokument beskrivs arkitekturens byggstenar. När det gäller IKT-infrastrukturen upprättar den provisoriska sammankopplingen ett motståndskraftigt VPN-nät (eller ett likvärdigt nätverk) som skapar säkra kommunikationstunnlar för säkert utbyte av meddelanden. Andra delar av infrastrukturen konfigureras för hög tillgänglighet och/eller är beroende av reservmekanismer.

Den specialanpassade programvarans motståndskraft

De specialanpassade programmodulerna ökar motståndskraften genom att upprepa kommunikationsförsöken med den andra ändpunkten under en viss tidsperiod, om den av någon anledning inte är tillgänglig.

Tjänsternas motståndskraft

I den provisoriska lösningen utbyter parterna uppgifter i fördefinierade tidluckor under året. Vissa av de steg som krävs vid de schemalagda utbytena av uppgifter kräver manuella ingripanden av systemoperatörer och/eller registerförvaltare. Mot bakgrund av detta, och för att öka utbytenas tillgänglighet och framgång

— räknar man i driftsförfarandena med betydande tidsluckor för varje steg,

— bygger programmodulerna för den provisoriska lösningen på asynkron kommunikation,

— upptäcker den automatiska avstämningen om det uppstod problem vid intagningen av datafiler i någon ände,

— beaktas övervakningsprocesser (IKT-infrastruktur och specialanpassade programmoduler) i incidenthanteringsförfaranden (enligt definitionen i dokumentet om gemensamma driftsförfaranden) och utlöser dem. De förfaranden som ska minska tidsåtgången vid återställning av normal drift efter incidenter är väsentliga för en hög tillgänglighet.

4.2 *Initialisering, kommunikation, reaktivering och provningsplan*

Alla olika delar av den provisoriska lösningens arkitektur ska genomgå en rad individuella och kollektiva provningar för att bekräfta att plattformen är redo på IKT-infrastrukturens och informationssystemets nivå. Dessa driftprov är en nödvändig förutsättning varje gång den provisoriska lösningen tas i drift av plattformen.

För att kopplingen ska kunna tas i drift måste följaktligen en fördefinierad provningsplan framgångsrikt genomföras. Denna ska bekräfta att varje register har genomfört en rad interna provningar först, följda av en validering av slutanvändarnas möjlighet att nå varandra, innan produktionstransaktioner börjar skickas mellan parterna.

Provningsplanen bör innehålla information om den övergripande provningsstrategin och provningsinfrastrukturen. För varje element i alla provningsblock ska den särskilt omfatta

— provningskriterierna och verktygen,

— de tilldelade rollerna för provningen,

— de förväntade resultaten (positiva och negativa),

— provningsschema,

— kraven för lagring av provresultat,

— dokumentation för felsökning,

— eskaleringsvillkor.

Som process kan provningarna för aktivering av driftstatus delas upp i fyra (4) konceptuella block eller faser:

4.2.1 Intern provning av IKT-infrastruktur

Dessa provningar ska göras och/eller kontrolleras individuellt av båda parterna vid varje ändpunkt.

Varje del av IKT-infrastrukturen ska provas individuellt vid varje ändpunkt. Detta inbegriper varje enskild del av infrastrukturen. Dessa provningar kan utföras automatiskt eller manuellt, men ska verifiera att varje del av infrastrukturen är funktionsduglig.

4.2.2 Provning av kommunikationen

Dessa provningar ska inledas individuellt av varje part och resultera i samarbete med den andra ändpunkten.

När individuella element är i drift måste kommunikationskanalerna mellan båda registren provas. I detta syfte ska varje part verifiera att internetåtkomsten fungerar, att VPN-tunnlarna (eller likvärdiga nätverk för säker överföring) har upprättats och att IP-förbindelsen från plats till plats fungerar. Den lokala infrastrukturens och fjärrinfrastrukturens tillgänglighet samt IP-förbindelsens funktion bör därefter bekräftas för den andra parten.

4.2.3 Provning av hela systemet (från ändpunkt till ändpunkt)

Denna provning ska utföras vid varje ändpunkt, och resultaten ska delas med den andra parten.

När kommunikationskanalerna och varje enskild del av båda registren har provats ska varje slutanvändare förbereda en rad simulerade transaktioner och avstämning som är representativ för alla funktioner som ska genomföras inom ramen för kopplingen.

4.2.4 Provning av säkerheten

Denna provning ska utföras och/eller utlösas av båda parterna i varje ände i enlighet med avsnitt 5.4 om riktlinjer för provning av säkerheten och avsnitt 5.5 om bestämmelser för riskbedömning.

Först när alla fyra faser/block har gett förutsägbara resultat kan den provisoriska kopplingen anses vara i drift.

Resurser för provning

Varje part ska använda särskilda resurser för provning (särskild programvara och hårdvara för IKT-infrastruktur) och ska införa provningsfunktioner i sina respektive system för att underlätta den manuella och kontinuerliga valideringen av plattformen. Manuella individuella eller samarbetsbaserade förfaranden för provning kan när som helst verkställas av registerförvaltarna. Aktiveringen av driftstatus är i sig en manuell process.

Det är också tänkt att plattformen ska utföra automatiska kontroller med regelbundna intervall. Syftet med dessa kontroller är att öka plattformens tillgänglighet genom att tidigt upptäcka möjliga infrastruktur- eller programvaruproblem. Denna plan för plattformsövervakning består av två delar:

— Övervakning av IKT-infrastruktur: leverantörerna av IKT-infrastrukturen övervakar infrastrukturen i båda ändarna. De automatiska provningarna omfattar infrastrukturens olika delar och kommunikationskanalernas tillgänglighet.

— Applikationsövervakning: den provisoriska kopplingens programmoduler genomför övervakning av systemkommunikationen på applikationsnivå (antingen manuellt och/eller med regelbundna intervall) som provar kopplingens tillgänglighet från ändpunkt till ändpunkt genom att simulera några av transaktionerna via kopplingen.

4.3 *Acceptans-/provmiljöer*

Arkitekturen i unionsregistret och det schweiziska registret består av följande tre miljöer:

— Produktion (PROD): Denna miljö omfattar de verkliga uppgifterna och behandlar verkliga transaktioner.

— Acceptans (ACC): Denna miljö omfattar icke-verkliga eller anonymiserade, representativa uppgifter. I denna miljö validerar båda parters systemoperatörer nya leveransversioner.

— Prov (TEST): Denna miljö omfattar icke-verkliga eller anonymiserade, representativa uppgifter. Miljön är endast avsedd för registerförvaltare och ska användas för integrationsprovning av båda parter.

Med undantag för VPN (eller ett likvärdigt nätverk) är dessa tre miljöer helt oberoende av varandra, vilket innebär att hårdvara, programvara, databaser, virtuella miljöer, IP-adresser och portar upprättas och drivs oberoende av varandra.

VPN upprättas i två olika miljöer, en för PROD samt en annan för ACC och TEST.

5. **Konfidentialitet och integritet**

Säkerhetsmekanismerna och säkerhetsförfarandena räknar med en tvåpersonsmetod (fyra ögon-principen) för verksamhet i kopplingen mellan unionsregistret och det schweiziska registret. Tvåpersonsrollen ska tillämpas vid behov. Det kan dock hända att den inte är tillämplig på alla registerförvaltarnas åtgärder.

Säkerhetskraven tas upp och behandlas i säkerhetsplanen, som även omfattar förfaranden för hantering av säkerhetsincidenter efter en säkerhetsöverträdelse. Den operativa delen av dessa förfaranden beskrivs i de gemensamma driftsförfarandena.

5.1 *Infrastruktur för provning av säkerheten*

Varje part åtar sig att upprätta en infrastruktur för provning av säkerheten (genom att använda den gemensamma programvaran och hårdvaran för att hitta sårbarheter i utvecklings- och driftfaserna)

— som är skild från produktionsmiljön,

— där säkerheten analyseras av en grupp som inte har att göra med utvecklingen och driften av systemet.

Varje part åtar sig att utföra både statisk och dynamisk analys.

När det gäller dynamisk analys (som penetrationsprovning) åtar sig båda parterna att normalt begränsa utvärderingarna till prov- och acceptansmiljön (som de definieras i avsnitt 4.3 om acceptans-/provmiljöer). Undantag från denna policy måste godkännas av båda parterna.

Innan den används i produktionsmiljön ska varje programmodul i kopplingen (som den definieras i avsnitt 3.1 om kommunikationslänkens arkitektur) genomgå en provning av säkerheten.

Infrastrukturen för provning måste vara skild från produktionsmiljön på både nätverks- och infrastrukturnivå. Den provning av säkerheten som krävs för att kontrollera överensstämmelsen med säkerhetskraven utförs inom provningsinfrastrukturen.

5.2 *Avstängning och reaktivering av kopplingen*

Om det finns misstankar om att säkerheten i det schweiziska registret, SSTL, unionsregistret eller EUTL har äventyrats ska båda parter omedelbart underrätta varandra och stänga kopplingen mellan SSTL och EUTL.

Förfarandena för informationsutbyte, beslut om avstängning och beslut om reaktivering ingår i de gemensamma driftsförfarandenas process för tillgodoseende av begäranden.

Avstängningar

Registerkopplingen i enlighet med bilaga II till avtalet kan stängas av

— administrativa skäl (t.ex. underhåll), vilket är planerat,

— säkerhetsskäl (eller på grund av störningar i it-infrastrukturen), vilket är oplanerat.

I nödfall ska en part informera den andra parten och ensidigt stänga registerkopplingen.

Om ett beslut fattas om att stänga registerkopplingen ska varje part se till att kopplingen bryts på nätverksnivå (genom att blockera delar av eller alla inkommande och utgående förbindelser).

Beslutet om att stänga registerkopplingen, vare sig planerat eller oplanerat, fattas i enlighet med förfarandet för förändringshantering eller hantering av säkerhetsincidenter i de gemensamma driftsförfarandena.

Reaktivering av kommunikationen

Beslutet om reaktivering av registerkopplingen fattas i enlighet med de gemensamma driftsförfarandena och i alla händelser efter att förfarandena för provning av säkerheten i enlighet med avsnitt 5.4 om riktlinjer för provning av säkerheten och avsnitt 4.2 om initialisering, kommunikation, reaktivering och provningsplan framgångsrikt har slutförts.

5.3 *Säkerhetsöverträdelse*

En säkerhetsöverträdelse betraktas som en säkerhetsincident som påverkar känsliga uppgifters konfidentialitet och integritet och/eller tillgängligheten till det system som hanterar dem.

Känsliga uppgifter anges i förteckningen över känsliga uppgifter och får hanteras i systemet eller i någon av systemets tillhörande delar.

Uppgifter som direkt berör säkerhetsöverträdelsen ska betraktas som känsliga, märkas med ”ETS KRITISK” och hanteras i enlighet med hanteringsanvisningarna, såvida inte något annat anges.

Alla säkerhetsöverträdelser kommer att hanteras i enlighet med kapitlet om hantering av säkerhetsincidenter i de gemensamma driftsförfarandena.

5.4 *Riktlinjer för provning av säkerheten*

5.4.1 Programvara

Provningen av säkerheten, i tillämpliga fall även penetrationsprovning, ska åtminstone göras på alla nya större leveransversioner av programvaran i enlighet med de säkerhetskrav som anges i de tekniska standarderna för sammankoppling, för att bedöma kopplingens säkerhet och de därmed sammanhängande riskerna.

Om ingen större leveransversion har släppts under de senaste tolv månaderna ska en provning av säkerheten genomföras på det nuvarande systemet med beaktande av cyberhotens utveckling under de senaste tolv månaderna.

Provningen av registerkopplingens säkerhet ska göras i acceptansmiljön och vid behov i produktionsmiljön, under samordning och ömsesidig överenskommelse mellan båda parterna.

Provningen av webbapplikationer ska följa internationella öppna standarder, t.ex. de som har tagits fram av Open Web Application Security Project (Owasp).

5.4.2 Infrastruktur

Produktionsmiljöns infrastruktur ska regelbundet avsökas för att hitta sårbarheter (minst en gång i månaden), och upptäckta sårbarheter ska åtgärdas. Testning utförs enligt den metod som beskrivs i avsnitt 5.4.1 med hjälp av en uppdaterad sårbarhetsdatabas.

5.5 *Riskbedömning*

Om penetrationsprovning är tillämplig måste den ingå i provningen av säkerheten.

Varje part får anlita ett specialiserat företag för provningen av säkerheten, på villkor att detta företag

— har den kompetens och erfarenhet som krävs för sådan provning av säkerheten,

— inte är direkt underställt utvecklaren och/eller dess uppdragstagare och varken deltar i utvecklingen av kopplingens programvara eller är en underleverantör till utvecklaren,

— har undertecknat ett sekretessavtal för att hålla resultaten konfidentiella och hantera dem på nivån ”ETS KRITISK” i enlighet med hanteringsanvisningarna.