2024/1873

5.7.2024

RÅDETS BESLUT (EU) 2024/1873

av den 24 juni 2024

om den ståndpunkt som ska intas på Europeiska unionens vägnar i den gemensamma kommitté som inrättats genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser, avseende ändring av bilaga II till avtalet, samt av gemensamma driftsförfaranden och tekniska standarder för sammankoppling

(Text av betydelse för EES)

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 192.1 jämförd med artikel 218.9,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) Avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser [1] (*avtalet*) undertecknades den 23 november 2017 i enlighet med rådets beslut (EU) 2017/2240 [2].

(2) Avtalet ingicks genom rådets beslut (EU) 2018/219 [3] och trädde i kraft den 1 januari 2020.

(3) Enligt artikel 12.3 i avtalet får den gemensamma kommittén fatta beslut som ska vara bindande för parterna när de träder i kraft.

(4) I artikel 13.2 i avtalet föreskrivs att den gemensamma kommittén får ändra bilagorna till avtalet.

(5) I artiklarna 3.6 och 3.7 föreskrivs att de gemensamma driftsförfarandena och de tekniska standarderna för sammankoppling ska träda i kraft när de antagits genom beslut av den gemensamma kommittén. Genom beslut nr 1/2020 [4] och 2/2020 [5] antog den gemensamma kommittén de gemensamma driftsförfarandena och de tekniska standarderna för sammankoppling.

(6) Det är lämpligt att ändra bilaga II till avtalet för att återspegla utvecklingen av registerkopplingen mellan EU:s system för handel med utsläppsrätter och Schweiz system för handel med utsläppsrätter och för att anpassa bestämmelserna i bilaga II med hänsyn till den tekniska utvecklingen. För att säkerställa att de gemensamma driftsförfarandena och de tekniska standarderna för sammankoppling överensstämmer med bilaga II bör även dessa dokument ändras.

[1] EUT L 322, 7.12.2017, s. 3.
[2] Rådets beslut (EU) 2017/2240 av den 10 november 2017 om undertecknande på unionens vägnar och om provisorisk tillämpning av avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser (EUT L 322, 7.12.2017, s. 1).
[3] Rådets beslut (EU) 2018/219 av den 23 januari 2018 om ingående av avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser (EUT L 43, 16.2.2018, s. 1).
[4] Beslut nr 1/2020 av den gemensamma kommitté som inrättas genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser av den 5 november 2020 om antagande av gemensamma driftsförfaranden [2021/1033] (EUT L 226, 25.6.2021, s. 2).
[5] Beslut nr 2/2020 av den gemensamma kommitté som inrättas 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 om antagande av de tekniska standarderna för sammankoppling (LTS) [2021/1034] (EUT L 226, 25.6.2021, s. 16).

(7) Den gemensamma kommittén ska, under sitt sjunde möte, eller tidigare genom det skriftliga förfarandet enligt artikel 8.4 i den gemensamma kommitténs arbetsordning ([6]), anta ett beslut vad gäller ändring av bilaga II till avtalet, och ändring av de gemensamma driftsförfarandena och de tekniska standarderna för sammankoppling.

(8) Det är lämpligt att fastställa den ståndpunkt som ska intas på unionens vägnar i den gemensamma kommittén, avseende ändring av bilaga II till avtalet, och ändring av gemensamma driftsförfaranden och tekniska standarder för sammankoppling, eftersom beslutet kommer att vara bindande för unionen.

(9) Unionens ståndpunkt i den gemensamma kommittén bör därför baseras på det åtföljande utkastet till beslut.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Den ståndpunkt som ska intas på unionens vägnar under det sjunde mötet i den gemensamma kommittén, eller tidigare genom det skriftliga förfarandet enligt artikel 8.4 i den gemensamma kommitténs arbetsordning, ska baseras på det utkast till beslut av den gemensamma kommittén som åtföljer det här beslutet.

Artikel 2

Detta beslut träder i kraft samma dag som det antas.

Utfärdat i Luxemburg den 24 juni 2024.

På rådets vägnar

D. CLARINVAL

Ordförande

([6]) Beslut nr 1/2019 av den gemensamma kommitté som inrättas genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser av den 25 januari 2019 om antagande av dess arbetsordning och rådets beslut (EU) 2018/1279 av den 18 september 2018 om den ståndpunkt som ska intas på Europeiska unionens vägnar i den gemensamma kommitté som inrättas genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser avseende antagandet av dess arbetsordning (EUT L 239, 24.9.2018, s. 8).

BESLUT NR 1/2024 AV DEN GEMENSAMMA KOMMITTÉ SOM INRÄTTATS GENOM AVTALET MELLAN EUROPEISKA UNIONEN OCH SCHWEIZISKA EDSFÖRBUNDET OM SAMMANKOPPLING AV DERAS UTSLÄPPSHANDELSSYSTEM FÖR VÄXTHUSGASER

av den …

om ändring av bilaga II till avtalet, och av de gemensamma driftsförfarandena och de tekniska standarderna för sammankoppling

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 artiklarna 9 och 13.2, och

av följande skäl:

(1) I den gemensamma kommitténs beslut nr 2/2019 ([2]) föreskrivs en provisorisk lösning för att praktiskt genomföra sammankopplingen mellan EU:s och Schweiziska edsförbundets utsläppshandelssystem.

(2) Vid sitt tredje möte beslutade den gemensamma kommittén att det fanns behov av att analysera kostnadseffektiviteten för en permanent koppling mellan unionens register och Schweiz register.

(3) Vid sitt femte möte godkände den gemensamma kommittén en rapport som överlämnats av den arbetsgrupp som inrättats genom beslut nr 1/2020 ([3]) och 2/2020 ([4]). I den rapporten analyserade och rekommenderade arbetsgruppen ett tillvägagångssätt för att genomföra den permanenta kopplingen mellan unionens register och Schweiz register.

(4) För att återspegla de tekniska kraven på en permanent koppling mellan unionens register och Schweiz register, och för att anpassa bestämmelserna i bilaga II till avtalet med hänsyn till den tekniska utvecklingen, bör bilaga II till avtalet ändras.

(5) För att säkerställa att de gemensamma driftsförfarandena och de tekniska standarderna för sammankoppling överensstämmer med bilaga II till avtalet bör även dessa dokument ändras.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Bilaga II till avtalet ska ersättas med texten i bilaga I till detta beslut.

2. De gemensamma driftsförfaranden som avses i artikel 3.6 i avtalet fastställs i bilaga II till detta beslut. De ersätter de gemensamma driftsförfaranden som fastställs i bilagan till beslut nr 1/2020.

3. De tekniska standarder för sammankoppling som avses i artikel 3.7 i avtalet fastställs i bilaga III till detta beslut. De ersätter de tekniska standarder för sammankoppling som fastställs i bilagan till beslut nr 2/2020.

([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 [2020/1359] (EUT L 314, 29.9.2020, s. 68).

([3]) Beslut nr 1/2020 av den gemensamma kommitté som inrättas genom avtalet mellan Europeiska unionen och Schweiziska edsförbundet om sammankoppling av deras utsläppshandelssystem för växthusgaser av den 5 november 2020 om antagande av gemensamma driftsförfaranden [2021/1033] (EUT L 226, 25.6.2021, s. 2).

([4]) Beslut nr 2/2020 av den gemensamma kommitté som inrättas 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 om antagande av de tekniska standarderna för sammankoppling (LTS) [2021/1034] (EUT L 226, 25.6.2021, s. 16).

Artikel 2

Detta beslut träder i kraft samma dag som det antas.

Utfärdat i … den …

På den gemensamma kommitténs vägnar

Sekreterare för Europeiska unionen	*Ordförande*	*Sekreterare för Schweiz*

BILAGA I

”BILAGA II

TEKNISKA STANDARDER FÖR SAMMANKOPPLING

För att praktiskt genomföra sammankopplingen av EU:s utsläppshandelssystem och Schweiz utsläppshandelssystem infördes en provisorisk lösning 2020. Från och med 2023 utvecklas registerkopplingen mellan de två utsläppshandelssystemen gradvis till en permanent registerkoppling som förväntas vara genomförd senast 2024 och som gör att de sammankopplade marknaderna kan utnyttja fördelarna med marknadslikviditet och genomförande av transaktioner mellan de två sammankopplade systemen på ett sätt som är likvärdigt med en marknad bestående av två system, där marknadsaktörerna kan att agera som om de handlade på en enda marknad och det enda förbehållet är parternas individuella bestämmelser.

I de tekniska standarderna för sammankoppling ska följande specificeras:

— Kommunikationslänkens arkitektur.

— Kommunikation mellan SSTL och EUTL.

— Säkerheten för överföring av uppgifter.

— Förteckningen över funktioner (för transaktioner, avstämning m.m.).

— Definitionen av transportskiktet.

— Kraven för registrering av data.

— Driftsarrangemangen (hjälpcentral, support).

— Aktiveringsplanen och provningsförfarandet för kommunikationen.

— Förfarandet för provning av säkerheten.

I de tekniska standarderna för sammankoppling ska anges att förvaltare ska vidta alla rimliga åtgärder för att säkerställa att SSTL, EUTL och kopplingen är i drift 24 timmar om dygnet, sju dagar i veckan, och att driftsavbrotten i SSTL, EUTL och kopplingen begränsas till ett minimum.

De tekniska standarderna för sammankoppling ska ange ytterligare säkerhetskrav för det schweiziska registret, SSTL, unionsregistret och EUTL som ska dokumenteras i en säkerhetsplan. I de tekniska standarderna för sammankoppling ska följande specificeras:

— 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.

— Vid händelse av en säkerhetsöverträdelse ska parterna förbinda sig att omedelbart underrätta varandra. I den mån de tekniska uppgifterna finns tillgängliga ska en rapport som beskriver händelsen (datum, orsak, påverkan, åtgärder) utbytas mellan förvaltaren av det schweiziska registret och unionens centrala förvaltare inom 24 timmar efter det att en incident har identifierats som en säkerhetsöverträdelse.

Den provning av säkerheten som anges i de tekniska standarderna för sammankoppling ska vara helt genomförd innan kommunikationslänken mellan SSTL och EUTL upprättas och när en ny version eller release (leveransversion) av SSTL eller EUTL krävs.

De tekniska standarderna för sammankoppling ska föreskriva två provmiljöer utöver produktionsmiljön: en provmiljö för utvecklare och en acceptansmiljö.

Parterna ska genom förvaltaren av det schweiziska registret och unionens centrala förvaltare tillhandahålla bevis för att en oberoende säkerhetsbedömning av systemen har gjorts under de föregående tolv månaderna i enlighet med de krav som anges i de tekniska standarderna för sammankoppling. Provning av säkerheten och i synnerhet penetrationsprovning ska göras på alla nya större releaser av programvaran i enlighet med de säkerhetskrav som anges i de tekniska standarderna för sammankoppling. Penetrationsprovningen får inte utföras av programvaruutvecklaren eller av en underleverantör till programvaruutvecklaren.”

BILAGA II

GEMENSAMMA DRIFTSFÖRFARANDEN I ENLIGHET MED ARTIKEL 3.6 I AVTALET MELLAN EUROPEISKA UNIONEN OCH SCHWEIZISKA EDSFÖRBUNDET OM SAMMANKOPPLING AV DERAS UTSLÄPPSHANDELSSYSTEM FÖR VÄXTHUSGASER

Förfaranden för permanent registerkoppling

Innehållsförteckning

1. ORDLISTA . . . 9
2. INLEDNING . . . 9
2.1. Tillämpningsområde . . . 10
2.2. Målgrupper . . . 10
3. TILLVÄGAGÅNGSSÄTT OCH STANDARDER . . . 10
4. INCIDENTHANTERING . . . 11
4.1. Upptäckt och registrering av incidenter . . . 11
4.2. Klassificering och inledande support . . . 11
4.3. Utredning och diagnostisering . . . 12
4.4. Åtgärd och återställning . . . 12
4.5. Stängning av incidenter . . . 12
5. PROBLEMHANTERING . . . 13
5.1. Identifiering och registrering av problem . . . 13
5.2. Prioritering av problem . . . 13
5.3. Utredning och diagnostisering av problem . . . 13
5.4. Åtgärd . . . 13
5.5. Stängning av problem . . . 13
6. TILLGODOSEENDE AV BEGÄRAN . . . 13
6.1. Initiering av tjänsteförfrågningar . . . 13
6.2. Registrering och analys av tjänsteförfrågningar . . . 14
6.3. Godkännande av tjänsteförfrågningar . . . 14
6.4. Tillgodoseende av begäran . . . 14
6.5. Eskalering av tjänsteförfrågningar . . . 14
6.6. Granskning av tillgodoseende av begäran . . . 14
6.7. Stängning av förfrågningar . . . 14
7. FÖRÄNDRINGSHANTERING . . . 14
7.1. Förändringsförfrågningar . . . 15
7.2. Utvärdering och planering av förändringar . . . 15
7.3. Godkännande av förändringar . . . 15
7.4. Implementering av förändringar . . . 15
8. RELEASEHANTERING . . . 15
8.1. Planering av releaser . . . 15
8.2. Byggande och provning av releasepaket . . . 16
8.3. Förberedelse av produktionssättningar . . . 16

8.4. Återställning av tillståndet före releasen . . . 16
8.5. Granskning och stängning av releasen . . . 16
9. HANTERING AV SÄKERHETSINCIDENTER . . . 17
9.1. Kategorisering av informationssäkerhetsincidenter . . . 17
9.2. Hantering av informationssäkerhetsincidenter . . . 17
9.3. Identifiering av säkerhetsincidenter . . . 17
9.4. Analys av säkerhetsincidenter . . . 17
9.5. Allvarlighetsbedömning, eskalering och rapportering för säkerhetsincidenter . . . 17
9.6. Rapportering av säkerhetsåtgärder . . . 18
9.7. Övervakning, kapacitetsuppbyggnad och kontinuerlig förbättring . . . 18
10. INFORMATIONSSÄKERHETSHANTERING . . . 18
10.1. Identifiering av känsliga uppgifter . . . 18
10.2. Känslighetsnivåer för informationstillgångar . . . 18
10.3. Tilldelning av ägarskap för informationstillgångar . . . 18
10.4. Registrering av känsliga uppgifter . . . 19
10.5. Hantering av känsliga uppgifter . . . 19
10.6. Åtkomsthantering . . . 19
10.7 Hantering av certifikat/nycklar . . . 19

1. ORDLISTA

Tabell 1-1 Förkortningar och definitioner

Förkortning/Term	Definition
Certifikatutfärdare	Enhet som utfärdar digitala certifikat
CH	Schweiziska edsförbundet
ETS (*Emissions Trading System*)	System för handel med utsläppsrätter
EU	Europeiska unionen
IMT (*Incident Management Team*)	Incidenthanteringsgrupp
Informationstillgång	Information som är värdefull för ett företag eller en organisation
IT	Informationsteknik
ITIL (*Information Technology Infrastructure Library*)	Internationellt erkänd uppsättning bästa praxis och normer som stöder förvaltning av it-tjänster
ITSM (*IT Service Management*)	Hantering av IT-tjänster
LTS (*Linking Technical Standards*)	Tekniska standarder för sammankoppling
Register	Ett redovisningssystem för utsläppsrätter som utfärdats inom ramen för utsläppshandelssystemet för att hålla reda på innehavaren av utsläppsrätter på elektroniska konton
RFC (*Request For Change*)	Förändringsförfrågan
SIL (*Sensitive Information List*)	Förteckning över känsliga uppgifter
SR (*Service Request*)	Tjänsteförfrågan
Wiki	Webbplats som ger användarna möjlighet att utbyta information och kunskaper genom att lägga till eller anpassa innehåll direkt via en webbläsare.

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 att uppfylla kraven i Europeiska unionens utsläppshandelssystem eller i Schweiz utsläppshandelssystem. För att praktiskt genomföra sammankopplingen av unionens utsläppshandelssystem och Schweiz utsläppshandelssystem kommer en direkt koppling mellan unionens transaktionsförteckning (EUTL) i unionsregistret och den schweiziska kompletterande transaktionsförteckningen (SSTL) i det schweiziska registret att 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 infördes en provisorisk lösning 2020. Från och med 2023 utvecklas registerkopplingen mellan de två utsläppshandelssystemen gradvis till en permanent registerkoppling som förväntas vara genomförd senast 2024 och som gör att de sammankopplade marknaderna kan utnyttja fördelarna med marknadslikviditet och genomförande av transaktioner mellan de två sammankopplade systemen på ett sätt som är likvärdigt med en marknad bestående av två system, där marknadsaktörerna kan agera som om de handlade på en enda marknad och det enda förbehållet är parternas individuella bestämmelser (bilaga II till avtalet).

Enligt artikel 3.6 i avtalet ska den schweiziska registerförvaltaren och unionens centrala förvaltare fastställa gemensamma driftsförfaranden för tekniska angelägenheter eller angelägenheter som är nödvändiga för driften av kopplingen, och beakta prioriterade områden i nationell lagstiftning. De gemensamma driftsförfaranden som förvaltarna utarbetar ska träda i kraft när de antagits genom beslut av den gemensamma kommittén.

De gemensamma driftsförfarandena antogs av den gemensamma kommittén genom dess beslut nr 1/2020. De uppdaterade gemensamma driftsförfaranden som anges i detta dokument kommer att antas av den gemensamma kommittén genom dess beslut nr 1/2024. I enlighet med detta beslut och på begäran av den gemensamma kommittén har den schweiziska registerförvaltaren och unionens centrala förvaltare utvecklat ytterligare tekniska riktlinjer för att praktiskt genomföra sammankopplingen och kommer att uppdatera dessa för att säkerställa att de kontinuerligt anpassas till den tekniska utvecklingen och till 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 förfarandemässig grund för kopplingen mellan registren i unionens utsläppshandelssystem och Schweiz utsläppshandelssystem. I dokumentet anges de övergripande kraven på driftsförfaranden, men vissa ytterligare tekniska riktlinjer kommer att krävas för att praktiskt genomföra sammankopplingen.

För att den ska fungera korrekt krävs tekniska specifikationer för att praktiskt genomföra den. I enlighet med artikel 3.7 i avtalet ska dessa beskrivas i närmare detalj i det dokument om tekniska standarder för sammankoppling som ska antas separat genom beslut av den gemensamma kommittén.

Syftet med de gemensamma driftsförfarandena är att säkerställa att IT-tjänster som rör driften av kopplingen mellan registren i unionens utsläppshandelssystem och Schweiz utsläppshandelssystem tillhandahålls på ett ändamålsenligt och effektivt sätt, i synnerhet när det gäller tjänsteförfrågningar, lösning av tjänsteavbrott, åtgärdande av problem samt utförande av rutinmässiga driftsuppgifter i enlighet med internationella standarder för hantering av IT-tjänster.

För den permanenta registerkopplingen krävs endast följande gemensamma driftsförfaranden, som ingår i detta dokument:

— Incidenthantering.

— Problemhantering.

— Tillgodoseende av begäran.

— Förändringshantering.

— Releasehantering.

— Hantering av säkerhetsincidenter.

— Informationssäkerhetshantering.

2.2. Målgrupper

Målgrupperna för dessa gemensamma driftsförfaranden är supportgrupperna för unionsregistret och det schweiziska registret.

3. TILLVÄGAGÅNGSSÄTT OCH STANDARDER

Följande principer gäller för samtliga gemensamma driftsförfaranden:

— EU och Schweiz har enats om att definiera de gemensamma driftsförfarandena baserat på ITIL (Information Technology Infrastructure Library, version 4). Metoderna i denna standard återanvänds för och anpassas till de specifika behoven i samband med den permanenta registerkopplingen.

— Den kommunikation och samordning mellan de båda parterna som krävs för utförandet av de gemensamma driftsförfarandena sker via servicedeskarna för det schweiziska registret och unionsregistret. Uppgifter tilldelas alltid inom en av parterna.

— Om det råder olika uppfattningar om hur en uppgift i de gemensamma driftsförfarandena ska utföras ska frågan analyseras och lösas av båda servicedeskarna. Om ingen överenskommelse kan nås ska frågan om en gemensam lösning hänskjutas till nästa eskaleringsnivå.

Eskaleringsnivåer	EU	CH
Nivå 1	EU:s servicedesk	Schweiz servicedesk
Nivå 2	EU:s driftsansvarige	Schweiz applikationsansvarige för registret
Nivå 3	Den gemensamma kommittén (som kan delegera detta ansvar i enlighet med artikel 12.5 i avtalet)	
Nivå 4	Den gemensamma kommittén (om nivå 3 har delegerats)	

— Varje part kan fastställa förfaranden för driften av sitt eget registersystem, med beaktande av de krav och gränssnitt som berörs av dessa gemensamma driftsförfaranden.

— Ett verktyg för hantering av IT-tjänster ska användas till stöd för de gemensamma driftsförfarandena, i synnerhet för incidenthantering, problemhantering och tillgodoseende av begäranden samt för kommunikation mellan de båda parterna.

— Utbyte av information via e-post är också tillåtet.

— Båda parterna ska säkerställa att informationssäkerhetskraven uppfylls i enlighet med hanteringsanvisningarna.

4. INCIDENTHANTERING

Syftet med incidenthanteringsprocessen är att säkerställa att IT-tjänster återställs till en normal nivå för tjänsten så snabbt som möjligt efter en incident och med minimal påverkan på verksamheten.

Vid incidenthantering bör incidenter även registreras för rapporteringsändamål, och incidenthanteringen bör integreras med andra processer som underlag för kontinuerliga förbättringar.

På en övergripande nivå omfattar incidenthantering följande aktiviteter:

— Upptäckt och registrering av incidenter.

— Klassificering och inledande support.

— Utredning och diagnostisering.

— Åtgärd och återställning.

— Stängning av incidenter.

Under incidentens hela livscykel ansvarar incidenthanteringsprocessen för att kontinuerligt hantera ägarskap, övervakning, uppföljning och kommunikation.

4.1. Upptäckt och registrering av incidenter

En incident kan upptäckas av en supportgrupp, med hjälp av verktyg för automatiserad övervakning eller av teknisk personal i samband med rutinmässig övervakning.

När en incident upptäcks ska den registreras och tilldelas en unik identifikationskod så att den kan följas upp och övervakas på lämpligt sätt. Den unika identifieringskoden för en incident är den identifieringskod som den tilldelats i det gemensamma ärendesystem som används av partens servicedesk (antingen EU:s eller Schweiz) och där incidenten har registrerats, och identifieringskoden ska användas i all kommunikation om incidenten.

För alla incidenter bör kontaktpunkten vara den parts servicedesk som har registrerat incidenten.

4.2. Klassificering och inledande support

Syftet med att klassificera incidenter är att förstå och fastställa vilket system och/eller vilka tjänster som påverkas av en incident och i vilken omfattning. För att klassificeringen ska vara ändamålsenlig bör den redan från början dirigera incidenten till rätt resurs så att den snabbt kan åtgärdas.

I klassificeringsfasen bör incidenten kategoriseras och prioriteras i enlighet med vilken påverkan den har och hur snabbt den måste lösas så att den kan behandlas inom den tidsram som gäller för prioriteringsnivån.

Om incidenten potentiellt kan påverka känsliga uppgifters sekretess och integritet och/eller påverkar systemets tillgänglighet ska incidenten betecknas som en säkerhetsincident och hanteras enligt den process som fastställs i avsnittet ”Hantering av säkerhetsincidenter” i detta dokument.

Om möjligt ska den servicedesk som registrerade ärendet genomföra den inledande diagnostiseringen. För att göra detta kontrollerar servicedesken om incidenten härrör från ett känt fel. I så fall är åtgärden för att lösa eller kringgå problemet redan känd och dokumenterad.

Om servicedesken lyckas lösa incidenten stänger den incidenten i detta skede, eftersom huvudsyftet med incidenthanteringen har uppnåtts (dvs. att snabbt återställa tjänsten för slutanvändaren). Om servicedesken inte lyckas lösa incidenten eskalerar servicedesken incidenten till lämplig lösningsgrupp för vidare utredning och diagnostisering.

4.3. Utredning och diagnostisering

Utredning och diagnostisering av incidenter görs om en incident inte kan lösas av servicedesken under den inledande diagnostiseringen och därför har eskalerats på lämpligt sätt. Eskalering av incidenter ingår som en integrerad del i utrednings- och diagnostiseringsprocessen.

En vanlig metod i utrednings- och diagnostiseringsfasen är att försöka återskapa incidenten under kontrollerade förhållanden. Vid utredning och diagnostisering av incidenter är det viktigt att man förstår vilken följd av händelser som ledde fram till incidenten.

Eskalering innebär en insikt om att incidenten inte kan lösas på den aktuella supportnivån utan måste skickas vidare till en supportgrupp på högre nivå eller till den andra parten. Eskaleringen kan följa två vägar: horisontell (funktionell) eskalering eller vertikal (hierarkisk) eskalering.

Den servicedesk som registrerade och initierade incidentärendet ansvarar för att incidenten eskaleras till lämplig resurs och för att följa upp den övergripande statusen för incidenten och vem den tilldelats.

Den av parterna som tilldelats incidenten ansvarar för att se till att de åtgärder som begärs utförs inom lämplig tid och för att återkoppla till sin egen servicedesk.

4.4. Åtgärd och återställning

Åtgärder och återställning i samband med incidenter utförs när man har en full förståelse av incidenten. Att hitta en åtgärd för en incident innebär att man har identifierat ett sätt att korrigera felet. Tillämpningen av åtgärden sker i återställningsfasen.

När lämpliga resurser har åtgärdat felet i tjänsten skickas incidenten tillbaka till den servicedesk som registrerade den, och den servicedesken kontrollerar med den som rapporterade incidenten att felet är löst och att incidenten kan stängas. Kunskaperna från hanteringen av incidenten ska dokumenteras för framtida bruk.

Återställningen kan göras av IT-supportpersonal eller genom att ge slutanvändaren instruktioner som han eller hon kan följa.

4.5. Stängning av incidenter

Stängning av incidenter är det sista steget i incidenthanteringsprocessen och görs kort efter det att incidenten har åtgärdats.

Checklistan med åtgärder som behöver göras i stängningsfasen för en incident omfattar i synnerhet följande:

— Kontrollera att den ursprungliga kategoriseringen av incidenten var korrekt.

— På lämpligt sätt samla in all information om omständigheterna kring incidenten.

— På lämpligt sätt dokumentera incidenten och uppdatera kunskapsdatabasen.

— På lämpligt sätt informera alla intressenter som direkt eller indirekt påverkades av incidenten.

En incident stängs formellt när servicedesken har genomfört stängningsfasen för incidenten och informerat den andra parten.

När en incident har stängts kan den inte öppnas på nytt. Om en incident uppstår på nytt inom kort tid öppnas inte den ursprungliga incidenten på nytt utan en ny incident registreras.

Om en incident följs upp av både EU:s och Schweiz servicedeskar ansvarar den servicedesk som registrerade ärendet för att slutgiltigt stänga incidenten.

5. PROBLEMHANTERING

Detta förfarande bör följas om ett problem har identifierats, vilket utgör startpunkten för problemhanteringsprocessen. Problemhantering fokuserar på att förbättra kvaliteten och minska volymen av incidenter. Ett problem kan vara orsaken till en eller flera incidenter. När en incident rapporteras är målet för incidenthanteringen att så snabbt som möjligt återställa tjänsten, eventuellt genom tillfälliga lösningar. Syftet med att registrera ett problem är att utreda grundorsaken till felet för att fastställa en förändring som kan genomföras för att hindra att problemet och de incidenter som kan kopplas till det uppstår på nytt.

5.1. Identifiering och registrering av problem

Kontaktpunkt för problemrelaterade frågor är antingen EU:s eller Schweiz servicedesk, beroende på vilken av parterna som initierade ärendet.

Den unika identifieringskoden för ett problem är den identifieringskod som det tilldelades inom ramen för hanteringen av IT-tjänster. Den måste användas i all kommunikation som rör det aktuella problemet.

Ett problem kan initieras genom en incident eller öppnas på eget initiativ för att lösa fel som i något skede upptäckts i systemet.

5.2. Prioritering av problem

För att underlätta uppföljningen kan problem, på samma sätt som incidenter, kategoriseras enligt hur allvarliga och prioriterade de är, med hänsyn till vilken påverkan de incidenter som kan knytas till problemet har och hur ofta de uppstår.

5.3. Utredning och diagnostisering av problem

Varje part kan initiera ett problem, och det är den initierande partens servicedesk som ansvarar för att registrera problemet, skicka det vidare till lämplig resurs och följa upp den övergripande statusen för det problemet.

Den lösningsgrupp som problemet har eskalerats till ansvarar för att hantera problemet inom lämplig tid och kommunicera med servicedesken.

På begäran ansvarar båda parterna för att de åtgärder som fastställts utförs och för att återkoppla till den egna partens servicedesk.

5.4. Åtgärd

Den lösningsgrupp som tilldelats problemet ansvarar för att åtgärda det och lämna relevant information till den egna partens servicedesk.

Kunskaperna från hanteringen av problemet ska dokumenteras för framtida bruk.

5.5. Stängning av problem

Ett problem stängs formellt när problemet har lösts genom att en förändring har genomförts. Stängningsfasen för ett problem genomförs av den servicedesk som registrerade problemet och informerade den andra partens servicedesk.

6. TILLGODOSEENDE AV BEGÄRAN

Processen för tillgodoseende av begäran är hanteringen av en tjänsteförfrågan avseende en ny eller befintlig tjänst under hela dess livscykel, från registrering och godkännande av tjänsteförfrågan till stängningen av den. Tjänsteförfrågningar är vanligtvis förfrågningar om mindre, fördefinierade, återkommande, förhandsgodkända tjänster och förfaranden.

De viktigaste stegen i hanteringen av en begäran är följande:

6.1. Initiering av tjänsteförfrågningar

Uppgifterna om en tjänsteförfrågan skickas till EU:s eller Schweiz servicedesk via e-post eller telefon, eller via verktyget för hantering av IT-tjänster eller någon annan överenskommen kommunikationskanal.

6.2. Registrering och analys av tjänsteförfrågningar

För alla tjänsteförfrågningar bör kontaktpunkten vara EU:s eller Schweiz servicedesk, beroende på vilken av parterna som initierade tjänsteförfrågan. Denna servicedesk ansvarar för att registrera och analysera tjänsteförfrågan med erforderlig noggrannhet.

6.3. Godkännande av tjänsteförfrågningar

Servicedesken hos den av parterna som initierade tjänsteförfrågan kontrollerar om godkännande från den andra parten krävs och vänder sig i så fall till den för att erhålla godkännande. Om tjänsteförfrågan inte godkänns uppdaterar servicedesken ärendet och stänger det.

6.4. Tillgodoseende av begäran

I detta steg ombesörjs en ändamålsenlig och effektiv hantering av tjänsteförfrågningar. Åtskillnad måste göras mellan följande fall:

— Tillgodoseende av en tjänsteförfrågan som bara påverkar en av parterna. I så fall utfärdar den parten arbetsorder och samordnar utförandet.

— Tillgodoseendet av tjänsteförfrågan påverkar både EU och Schweiz. I så fall utfärdar servicedeskarna arbetsorder inom sina respektive ansvarsområden. Processen för att tillgodose tjänsteförfrågan samordnas av båda servicedeskarna. Det övergripande ansvaret ligger hos den servicedesk som mottog och initierade tjänsteförfrågan.

När tjänsteförfrågan har tillgodosetts måste den tilldelas statusen åtgärdad.

6.5. Eskalering av tjänsteförfrågningar

Servicedesken kan vid behov eskalera ej åtgärdade tjänsteförfrågningar till lämplig resurs (tredje part).

Eskalering görs till respektive tredje part, dvs. EU:s servicedesk måste vända sig till Schweiz servicedesk för eskalering till Schweiz tredje part och omvänt.

Den tredje part som tjänsteförfrågan eskalerats till ansvarar för att hantera den inom lämplig tid och kommunicera med den servicedesk som eskalerade tjänsteförfrågan.

Den servicedesk som registrerade tjänsteförfrågan ansvarar för att följa upp den övergripande statusen för den och vem den tilldelats.

6.6. Granskning av tillgodoseende av begäran

Den ansvariga servicedesken gör en slutlig kvalitetskontroll av de uppgifter som registrerats i tjänsteförfrågan innan den stängs. Syftet är att kontrollera att tjänsteförfrågan verkligen har behandlats och att alla uppgifter som krävs för att beskriva livscykeln för den anges i tillräcklig detalj. Kunskaperna från hanteringen av tjänsteförfrågan ska också dokumenteras för framtida bruk.

6.7. Stängning av förfrågningar

Om de parter som tilldelats tjänsteförfrågan är överens om att den har tillgodosetts och den som gjorde förfrågan betraktar ärendet som åtgärdat, ska tjänsteförfrågan tilldelas nästa status, ”Stängd” (”Closed”).

En tjänsteförfrågan stängs formellt när den servicedesk som registrerade den har genomfört stängningsfasen för tjänsteförfrågan och informerat den andra partens servicedesk.

7. FÖRÄNDRINGSHANTERING

Syftet med förändringshantering är att tillse att standardiserade metoder och förfaranden används för en effektiv och snabb hantering av alla förändringar för att kontrollera IT-infrastrukturen, så att antalet relaterade incidenter och deras påverkan på tjänsten minimeras. Förändringar av IT-infrastrukturen kan genomföras reaktivt för att lösa problem eller tillgodose externa krav, t.ex. förändrad lagstiftning, eller proaktivt för att förbättra effektivitet och ändamålsenlighet eller för att möjliggöra eller ta hänsyn till verksamhetsinitiativ.

Förändringshanteringsprocessen omfattar olika steg för att samla in alla detaljer om en förändringsbegäran för framtida spårning. Genom processerna säkerställs att förändringen valideras och provas innan den produktionssätts. Ansvaret för en lyckad produktionssättning ligger i releasehanteringsprocessen.

7.1. Förändringsförfrågningar

En förändringsförfrågan skickas till förändringshanteringsgruppen för validering och godkännande. För alla förändringsförfrågningar bör kontaktpunkten vara EU:s eller Schweiz servicedesk, beroende på vilken av parterna som initierade förfrågan. Denna servicedesk ansvarar för att registrera och analysera förfrågan med lämplig omsorg.

En förändringsförfrågan kan ha sitt ursprung i

— en incident som ger upphov till en förändring,

— ett befintligt problem som leder till en förändring,

— en begäran om en ny förändring från en slutanvändare,

— en förändring till följd av pågående underhåll,

— ändrad lagstiftning.

7.2. Utvärdering och planering av förändringar

I denna fas hanteras bedömningen och planeringen av förändringar. Här ingår prioriterings- och planeringsaktiviteter för att minimera risker och påverkan.

Om genomförandet av en förändringsförfrågan påverkar både EU och Schweiz kontrollerar den part som registrerade förändringsförfrågan utvärderingen och planeringen av förändringen med den andra parten.

7.3. Godkännande av förändringar

Alla registrerade förändringsförfrågningar måste godkännas på relevant eskaleringsnivå.

7.4. Implementering av förändringar

Implementering av förändringar hanteras inom releasehanteringsprocessen. Båda parternas releasehanteringsgrupper följer sina egna processer som omfattar planering och provning. När implementeringen slutförts granskas förändringen. För att säkerställa att allt går planenligt ses förändringshanteringsprocessen över kontinuerligt och uppdateras vid behov.

8. RELEASEHANTERING

En release är en eller flera förändringar inom en IT-tjänst som ingår i en releaseplan och måste godkännas, förberedas, byggas, provas och produktionssättas tillsammans. En release kan innehålla en felrättning, en förändring av hårdvara eller andra komponenter, programändringar, uppgradering av programversioner och ändringar av dokumentation och/eller processer. Innehållet i varje release hanteras, provas och produktionssätts som en enhet.

Syftet med releasehantering är att planera, bygga, prova, validera och leverera förmågan att tillhandahålla den tjänst som tagits fram för att uppfylla intressentens krav och uppfylla de avsedda målen. Acceptanskriterier för alla förändringar av tjänsten fastställs och dokumenteras under designkoordineringen och lämnas till releasehanteringsgrupperna.

En release består oftast av ett antal problemrättningar och förbättringar av tjänsten. Den innehåller den nya eller ändrade programvara som krävs och ny eller ändrad hårdvara som behövs för att implementera de godkända förändringarna.

8.1. Planering av releaser

Det första steget i processen är att gruppera godkända förändringar i releasepaket och att fastställa omfattningen och innehållet i releaserna. Baserat på denna information utarbetas inom ramen för delprocessen releaseplanering ett tidsschema för att bygga, prova och produktionssätta releasen.

I releaseplaneringen bör följande information ingå:

— Releasens omfattning och innehåll.

— Riskbedömning av releasen och releasens riskprofil.

— Kunder/användare som påverkas av releasen.

— Vilken grupp som ansvarar för releasen.

— Strategi för leverans och produktionssättning.

— Resurser som krävs för releasen och produktionssättning av den.

Båda parterna ska informera varandra om sin releaseplanering och sina underhållsperioder. Om en release påverkar både EU och Schweiz ska parterna samordna sin planering och fastställa en gemensam underhållsperiod.

8.2. Byggande och provning av releasepaket

I bygg- och provningsstegen i releasehanteringsprocessen fastställs tillvägagångssättet för att genomföra releasen eller releasepaketet och för att upprätthålla en kontrollerad miljö före förändringen av produktionsmiljön, samt för provning av alla förändringar i alla miljöer där de driftsätts.

Om en release påverkar både EU och Schweiz ska parterna samordna sin leveransplanering och provningar. Detta omfattar följande aspekter:

— Hur och när releaseenheter och tjänstekomponenter levereras.

— De typiska ledtiderna och vad som händer vid fördröjningar.

— Hur arbetets fortskridande ska följas upp och bekräftas.

— Mätmetoder för att övervaka och fastställa i vilken utsträckning produktionssättningen av releasen har varit framgångsrik.

— Gemensamma testfall för relevanta funktioner och förändringar.

Vid slutet av denna delprocess är alla releasekomponenter klara för driftsättning i produktionsmiljön.

8.3. Förberedelse av produktionssättningar

Genom denna delprocess säkerställs att korrekta kommunikationsplaner tagits fram och att meddelanden är klara att skickas till alla intressenter och slutanvändare som påverkas, samt att releasen har integrerats med förändringshanteringsprocessen så att alla förändringar genomförs på ett kontrollerat sätt och har godkänts i de forum som krävs.

Om en release påverkar både EU och Schweiz ska parterna samordna följande:

— Uppgifterna i förändringsförfrågan för schemaläggning och förberedelse av driftsättning i produktionsmiljön.

— Utarbetandet av en övergripande implementeringsplan.

— En strategi för återställning så att en återgång till tillståndet före produktionssättningen kan göras om produktionssättningen misslyckas.

— Meddelanden till alla nödvändiga parter.

— Begäran om godkännande att genomföra releasen från relevant eskaleringsnivå.

8.4. Återställning av tillståndet före releasen

Om produktionssättningen misslyckas eller provning visar att produktionssättningen inte lyckades eller inte uppfyller de överenskomna acceptans- eller kvalitetskriterierna måste båda parternas releasehanteringsgrupper återställa produktionsmiljön till tillståndet före produktionssättningen. Alla nödvändiga intressenter måste informeras, inbegripet de slutanvändare som påverkas eller utgjorde målgruppen för releasen. I avvaktan på godkännande kan processen återstartas vid något av de tidigare stegen.

8.5. Granskning och stängning av releasen

Vid granskningen av produktionssättningen bör följande aktiviteter ingå:

— Samla in synpunkter från kunden och användarna om deras tillfredsställelse med produktionssättningen och leveransen av tjänsten (samla in synpunkter och använda som underlag för kontinuerlig förbättring).

— Granska eventuella kvalitetskriterier som inte uppfylldes.

— Kontrollera att alla åtgärder, nödvändiga rättningar och förändringar är kompletta.

— Säkerställa att inga problem i fråga om funktionalitet, resurser, kapacitet eller prestanda förekommer efter produktionssättningen.

— Kontrollera att eventuella problem, kända fel eller tillfälliga lösningar har dokumenterats och godtas av kunden, slutanvändare, driftsupport och andra berörda parter.

— Övervaka incidenter och problem som orsakas av produktionssättningen (tillhandahålla tidig support till driftspersonal om releasen har medfört ökad arbetsbelastning).

— Uppdatera supportdokumentationen (t.ex. dokument med teknisk information).

— Formellt överlämna den produktionssatta releasen till tjänstedriften.

— Dokumentera de erfarenheter som gjorts.

— Ta emot den sammanfattande rapporten om releasen från implementeringsgrupperna.

— Formellt stänga releasen efter verifiering mot uppgifterna i förändringsförfrågan.

9. HANTERING AV SÄKERHETSINCIDENTER

Hantering av säkerhetsincidenter är en process med syftet att möjliggöra kommunikation om incidenter till potentiellt berörda intressenter, incidentbedömning och incidentprioritering samt incidentåtgärder för att ta hand om alla faktiska, misstänkta eller potentiella överträdelser som påverkar känsliga informationstillgångars sekretess, tillgänglighet eller integritet.

9.1. Kategorisering av informationssäkerhetsincidenter

Alla incidenter som påverkar kopplingen mellan unionsregistret och det schweiziska registret ska analyseras för att fastställa eventuell påverkan på sekretessen, integriteten eller tillgängligheten för uppgifter i förteckningen över känsliga uppgifter.

Om en sådan påverkan kan fastställas ska incidenten betecknas som en informationssäkerhetsincident, omedelbart registreras i verktyget för hantering av IT-tjänster och behandlas som en informationssäkerhetsincident.

9.2. Hantering av informationssäkerhetsincidenter

Ansvaret för säkerhetsincidenter ligger hos eskaleringsnivå 3 och lösningen av incidenterna ska hanteras av en särskild incidenthanteringsgrupp.

Incidenthanteringsgruppen ansvarar för att

— göra en inledande analys och kategorisera och bedöma incidentens allvarlighetsgrad,

— samordna insatserna från alla intressenter, inbegripet en fullständig dokumentation av incidentanalysen, de beslut som fattats för att åtgärda incidenten och eventuella svagheter som har identifierats,

— beroende på hur allvarlig säkerhetsincidenten är, snabbt eskalera incidenten till lämplig nivå för information och/eller beslut.

I processen för informationssäkerhetshantering klassificeras all information om incidenter enligt den högsta känslighetsnivån hos de uppgifter som berörs, dock aldrig lägre än KÄNSLIG (SENSITIVE: *ETS*).

Under en pågående utredning och/eller i samband med en svaghet som skulle kunna utnyttjas och tills denna har avhjälpts klassificeras informationen som SPECIALHANTERING (SPECIAL HANDLING: *ETS Critical*).

9.3. Identifiering av säkerhetsincidenter

Beroende på typen av säkerhetshändelse fastställer den informationssäkerhetsansvarige vilka organisationer som bör involveras och ingå i incidenthanteringsgruppen.

9.4. Analys av säkerhetsincidenter

Incidenthanteringsgruppen samverkar med alla involverade organisationer och relevanta medlemmar i deras grupper för att bedöma incidenten. Vid analysen fastställs i vilken utsträckning sekretessen, integriteten eller tillgängligheten för en tillgång har förlorats, och följderna för alla berörda organisationer bedöms. Därefter fastställs vilka inledande åtgärder och uppföljningsåtgärder som ska vidtas för att åtgärda incidenten och hantera dess påverkan, inbegripet vilka resurser som krävs för åtgärderna.

9.5. Allvarlighetsbedömning, eskalering och rapportering för säkerhetsincidenter

Incidenthanteringsgruppen ska bedöma alla nya säkerhetsincidenter efter att de betecknats som sådana och omedelbart inleda de åtgärder som krävs i enlighet med incidentens allvarlighetsgrad.

9.6. Rapportering av säkerhetsåtgärder

I åtgärdsrapporten för informationssäkerhetsincidenten anger incidenthanteringsgruppen vidtagna åtgärder för incidentbegränsning och resultatet av återställningsåtgärderna. Rapporten lämnas till eskaleringsnivå 3 via säker e-post eller annan ömsesidigt godtagbar metod för säker kommunikation.

Den ansvariga parten granskar begränsningsåtgärderna och resultatet av återställningsåtgärderna, och

— återstartar registerkopplingen, om den tidigare stängts av,

— kommunicerar incidentinformationen till registergrupperna,

— stänger incidenten.

Incidenthanteringsgruppen bör, på ett säkert sätt, ange relevanta uppgifter i åtgärdsrapporten för informationssäkerhetsincidenten för att säkerställa en enhetlig dokumentation och kommunikation och möjliggöra snabba och lämpliga åtgärder för att begränsa incidenten. När rapporten har färdigställts lämnar incidenthanteringsgruppen slutversionen av åtgärdsrapporten för informationssäkerhetsincidenten inom lämplig tid.

9.7. Övervakning, kapacitetsuppbyggnad och kontinuerlig förbättring

Incidenthanteringsgruppen lämnar rapporter om alla säkerhetsincidenter till eskaleringsnivå 3. Denna eskaleringsnivå använder rapporterna för att fastställa

— svagheter i säkerhetskontroller eller drift som behöver avhjälpas,

— eventuella behov att förbättra förfarandet för att effektivisera hanteringen av incidenter,

— möjligheter till utbildning och kapacitetsuppbyggnad för att ytterligare förstärka registersystemens motståndskraft mot informationssäkerhetshot, minska risken för framtida incidenter och minimera incidenternas påverkan.

10. INFORMATIONSSÄKERHETSHANTERING

Informationssäkerhetshanteringens syfte är att säkerställa sekretessen, integriteten och tillgängligheten för en organisations säkerhetsskyddsklassificerade uppgifter, data och IT-tjänster. Utöver tekniska komponenter, inklusive deras utformning och provning (se de tekniska standarderna för sammankoppling) krävs följande gemensamma driftsförfaranden för att uppfylla säkerhetskraven för den permanenta registerkopplingen:

10.1. Identifiering av känsliga uppgifter

En uppgifts känslighet bedöms genom att fastställa i vilken omfattning en säkerhetsöverträdelse som rör uppgiften kan påverka verksamheten (t.ex. i form av ekonomiska förluster, försämrad uppfattning om verksamheten, lagöverträdelser osv.).

Känsliga informationstillgångar ska identifieras på grundval av deras påverkan på sammankopplingen.

Känslighetsnivån för dessa uppgifter ska bedömas enligt en känslighetsskala som kan tillämpas på sammankopplingen och som beskrivs i avsnittet ”Hantering av informationssäkerhetsincidenter” i detta dokument.

10.2. Känslighetsnivåer för informationstillgångar

Informationstillgångar som identifierats som känsliga ska klassificeras med hjälp av följande regler:

— Tillgångar som omfattar minst en (1) uppgift för vilken känslighetsnivån i fråga om sekretess, integritet eller tillgänglighet har angetts som HÖG (HIGH) ska klassificeras som SPECIALHANTERING (SPECIAL HANDLING: *ETS Critical*).

— Tillgångar som omfattar minst en (1) uppgift för vilken känslighetsnivån i fråga om sekretess, integritet eller tillgänglighet har angetts som MEDELHÖG (MEDIUM) ska klassificeras som KÄNSLIG (SENSITIVE: *ETS*).

— Tillgångar som endast omfattar uppgifter för vilka känslighetsnivån i fråga om sekretess, integritet eller tillgänglighet har angetts som LÅG (LOW) ska klassificeras som (EU-markering) KÄNSLIG (SENSITIVE: *ETS Joint Procurement),* respektive (CH-markering) BEGRÄNSAD (LIMITED): ETS).

10.3. Tilldelning av ägarskap för informationstillgångar

Alla informationstillgångar ska tilldelas en ägare. Informationstillgångar i utsläppshandelssystemet som ingår i eller används för kopplingen mellan EUTL och SSTL bör föras upp på en gemensam förteckning över informationstillgångar som underhålls av båda parterna. Informationstillgångar i utsläppshandelssystemet som ligger utanför kopplingen mellan EUTL och SSTL bör föras upp på en förteckning över informationstillgångar som underhålls av respektive part.

Ägarskapet för varje informationstillgång som ingår i eller används för kopplingen mellan EUTL och SSTL ska överenskommas av parterna. Ägaren till en informationstillgång ansvarar för att bedöma dess känslighet.

Ägaren bör ha en tjänstegrad som är lämplig med hänsyn till värdet på den eller de tilldelade tillgångarna. Ägarens ansvar för tillgången eller tillgångarna och hans eller hennes skyldighet att upprätthålla den nödvändiga sekretess-, integritets- och tillgänglighetsnivån bör godkännas och formaliseras.

10.4. Registrering av känsliga uppgifter

Alla känsliga uppgifter ska registreras i förteckningen över känsliga uppgifter.

Om en aggregering av känsliga uppgifter skulle kunna leda till en större påverkan än påverkan av en enda uppgift, ska detta beaktas och registreras i förteckningen över känsliga uppgifter (t.ex. en uppsättning uppgifter i systemets databas).

Förteckningen över känsliga uppgifter är inte statisk. Hot, sårbarheter, sannolikheten för eller konsekvenserna av säkerhetsincidenter som rör tillgångarna kan förändras utan förvarning, och nya tillgångar kan tillkomma i samband med driften av registersystemen.

En översyn av förteckningen över känsliga uppgifter ska därför göras regelbundet, och nya uppgifter som identifieras som känsliga ska omedelbart föras upp på förteckningen.

Förteckningen över känsliga uppgifter ska innehålla minst följande information om varje post:

— Beskrivning av uppgiften.

— Uppgiftsägare.

— Känslighetsnivå.

— Information om huruvida uppgiften omfattar personuppgifter.

— Ytterligare information om så krävs.

10.5. Hantering av känsliga uppgifter

När känsliga uppgifter behandlas utanför kopplingen mellan unionsregistret och det schweiziska registret ska de hanteras i enlighet med hanteringsanvisningarna.

Känsliga uppgifter som behandlas genom kopplingen mellan unionsregistret och det schweiziska registret ska hanteras i enlighet med parternas säkerhetskrav.

10.6. Åtkomsthantering

Syftet med åtkomsthantering är att ge auktoriserade användare rätt att använda en tjänst och samtidigt förhindra tillgången för icke auktoriserade användare. Åtkomsthantering kallas ibland även ”rättighetshantering” eller ”identitetshantering”.

När det gäller den permanenta registerkopplingen och driften av denna behöver båda parterna åtkomst till följande komponenter:

— Wiki: en samarbetsmiljö för utbyte av gemensam information, exempelvis releaseplanering.

— Verktyg för hantering av IT-tjänster, för incident- och problemhantering (se avsnitt 3 ”Tillvägagångssätt och standarder”).

— System för meddelandeutbyte: varje part ska tillhandahålla ett säkert överföringssystem för utbyte av meddelanden för överföring av de meddelanden som innehåller transaktionsuppgifter.

Den schweiziska registerförvaltaren och unionens centrala förvaltare säkerställer att åtkomsträttigheterna hålls aktuella och fungerar som respektive parts kontaktpunkt för aktiviteter som rör åtkomsthetshantering. Åtkomstförfrågningar hanteras i enlighet med förfarandena för tillgodoseende av begäran.

10.7. Hantering av certifikat/nycklar

Varje part ansvarar för sin egen hantering av certifikat/nycklar (skapande, registrering, lagring, installation, användning, förnyelse, återkallande, säkerhetskopiering och återställning av certifikat/nycklar). Som anges i de tekniska standarderna för sammankoppling ska bara digitala certifikat som utfärdats av en certifikatutfärdare som är betrodd av båda parterna användas. Hanteringen och lagringen av certifikat/nycklar måste följa bestämmelserna i hanteringsanvisningarna.

Återkallande och/eller förnyelse av certifikat och nycklar ska samordnas av båda parterna. Detta görs i enlighet med förfarandena för tillgodoseende av begäran.

Den schweiziska registerförvaltaren och unionens centrala förvaltare utbyter certifikat/nycklar via en säker kommunikationsmetod i enlighet med bestämmelserna i hanteringsanvisningarna.

All verifiering av certifikat/nycklar som på något sätt görs av parterna ska ske via en separat kanal.

BILAGA III

TEKNISKA STANDARDER FÖR SAMMANKOPPLING I ENLIGHET MED ARTIKEL 3.7 I AVTALET MELLAN EUROPEISKA UNIONEN OCH SCHWEIZISKA EDSFÖRBUNDET OM SAMMANKOPPLING AV DERAS UTSLÄPPSHANDELSSYSTEM FÖR VÄXTHUSGASER

Standarder för permanent registerkoppling

Innehållsförteckning

1.	ORDLISTA	23
2.	INLEDNING	25
2.1.	Tillämpningsområde	25
2.2.	Målgrupper	25
3.	ALLMÄNNA BESTÄMMELSER	25
3.1.	Kommunikationslänkens arkitektur	25
3.1.1.	Utbyte av meddelanden	26
3.1.2.	XML-meddelande – högnivåbeskrivning	26
3.1.3.	Tidsluckor för intagning	26
3.1.4.	Meddelandeflöden för transaktioner	27
3.2.	Säkerheten för överföring av uppgifter	29
3.2.1.	Brandvägg och sammankoppling av nätverk	29
3.2.2.	Virtuellt privat nätverk (VPN)	29
3.2.3.	Implementering av IPSec	29
3.2.4.	Säkert meddelandeöverföringsprotokoll	30
3.2.5.	XML-baserad kryptering och signatur	30
3.2.6.	Krypteringsnycklar	30
3.3.	Förteckning över funktioner inom ramen för kopplingen	30
3.3.1.	Verksamhetstransaktioner	30
3.3.2.	Avstämningsprotokoll	31
3.3.3.	Provmeddelande	31
3.4.	Kraven för registrering av data	31
3.5.	Driftskrav	32
4.	TILLGÄNGLIGHET	32
4.1.	Utformning för tillgänglig kommunikation	32
4.2.	Initialisering, kommunikation, reaktivering och provningsplan	33
4.2.1.	Intern provning av IKT-infrastruktur	33
4.2.2.	Provning av kommunikationen	33
4.2.3.	Provning av hela systemet (ändpunkt-till-ändpunkt)	33
4.2.4.	Provning av säkerheten	33
4.3.	Acceptans-/provmiljöer	34
5.	KONFIDENTIALITET OCH INTEGRITET	34
5.1.	Infrastruktur för provning av säkerheten	34
5.2.	Avstängning och reaktivering av kopplingen	35

5.3. Säkerhetsöverträdelse 35
5.4. Riktlinjer för provning av säkerheten 35
5.4.1. Programvara 35
5.4.2. Infrastruktur 36
5.5. Riskbedömning 36

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 kraven i endera enhetens utsläppshandelssystem.
CH	Schweiziska edsförbundet
CHU	Typ av stationär utsläppsrätt, även kallad CHU2 (avser andra åtagandeperioden i Kyoto-protokollet), fastställd av Schweiziska edsförbundet
CHUA	Schweizisk utsläppsrätt för luftfart
COP (*Common Operational Procedures*)	Gemensamma driftsförfaranden. Förfaranden som parterna gemensamt har tagit fram för att praktiskt genomföra sammankopplingen mellan unionens utsläppshandelssystem och Schweiz utsläppshandelssystem.
ETR (*Emissions Trading Registry*)	Register för handel med utsläppsrätter
ETS (*Emissions Trading System*)	System för handel med utsläppsrätter
EU	Europeiska unionen
EUA	Allmän utsläppsrätt i EU:s system
EUAA (*EU Aviation Allowance*)	Utsläppsrätt för luftfart i EU:s system
EUCR (*European Union Consolidated Registry*)	EU:s konsoliderade register
EUTL (*European Union Transaction Log*)	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 (*Swiss Supplementary Transaction Log*)	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 kryptografi	Krypterar och dekrypterar data med hjälp av öppna och privata nycklar
Certifikatutfärdare	Enhet som utfärdar digitala certifikat
Krypteringsnycklar	Information som bestämmer en krypteringsalgoritms funktionella utdata
Dekryptering	Motsatsen till kryptering
Digital signatur	En matematisk metod som används för validering av ett meddelandes, programs eller digitalt dokuments autenticitet och integritet
Kryptering	Att omvandla information eller data till en kod, särskilt för att förhindra obehörig åtkomst
Filintagning	Att läsa en fil
Brandvägg	Hårdvara eller ett programvara för nätverkssäkerhet som övervakar och kontrollerar inkommande och utgående nätverkstrafik enligt bestämda regler
Heartbeat-övervakning	Periodiskt genererad signal som övervakas av hårdvara eller programvara för att indikera normal drift 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 säkerhetssårbarheter som en angripare skulle kunna utnyttja
Avstämning	Att säkerställa att två uppsättningar av uppgifter överensstämmer med varandra
VPN (*Virtual Private Network*)	Virtuellt privat nätverk
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 kommer en direkt koppling mellan unionens transaktionsförteckning (EUTL) i unionsregistret och den schweiziska kompletterande transaktionsförteckningen (SSTL) i det schweiziska registret att 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 infördes en provisorisk lösning 2020. Från och med 2023 utvecklas registerkopplingen mellan de två utsläppshandelssystemen gradvis till en permanent registerkoppling som förväntas vara genomförd senast 2024 och som gör det möjligt för de sammankopplade marknaderna att fungera och utnyttja fördelarna med marknadslikviditet och genomförande av transaktioner mellan de två sammankopplade systemen på ett sätt som är likvärdigt med en marknad bestående av två system, där marknadsaktörerna kan agera som om de handlade på en enda marknad och det enda förbehållet är parternas individuella bestämmelser (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 standarderna för sammankoppling antogs av den gemensamma kommittén genom dess beslut nr 2/2020. De uppdaterade tekniska standarder för sammankoppling som anges i detta dokument kommer att antas av den gemensamma kommittén genom dess beslut nr 1/2024. I enlighet med detta beslut och på begäran av den gemensamma kommittén har den schweiziska registerförvaltaren och unionens centrala förvaltare utvecklat ytterligare tekniska riktlinjer för att praktiskt genomföra sammankopplingen och kommer att uppdatera dessa för att säkerställa att de kontinuerligt anpassas till den tekniska utvecklingen och till 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 den ska fungera korrekt krävs tekniska specifikationer för att praktiskt genomföra den. I enlighet med artikel 3.6 i avtalet ska de närmare detaljerna i dessa beskrivas i det dokument om tekniska standarder för sammankoppling som ska antas separat genom beslut av den gemensamma kommittén.

2.2. Målgrupper

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

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 arkitektur har alla åtgärder vidtagits för att arkitekturen ska vara robust. Den permanenta registerkopplingen använder en mekanism för utbyte av filer via en säker förbindelse baserad på luftgap.

Den tekniska lösningen använder

— ett säkert meddelandeöverföringsprotokoll,

— XML-meddelanden,

— XML-baserad digital signatur och kryptering,

— VPN.

3.1.1. Utbyte av meddelanden

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

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

Fel eller oväntad status ska rapporteras, i form av varningar, och supportgrupperna ska ha ömsesidig direktkontakt.

Fel och oväntade händelser 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 en startdel med

— avsändande utsläppshandelssystem,

— ordningsnummer.

3.1.3. Tidsluckor för intagning

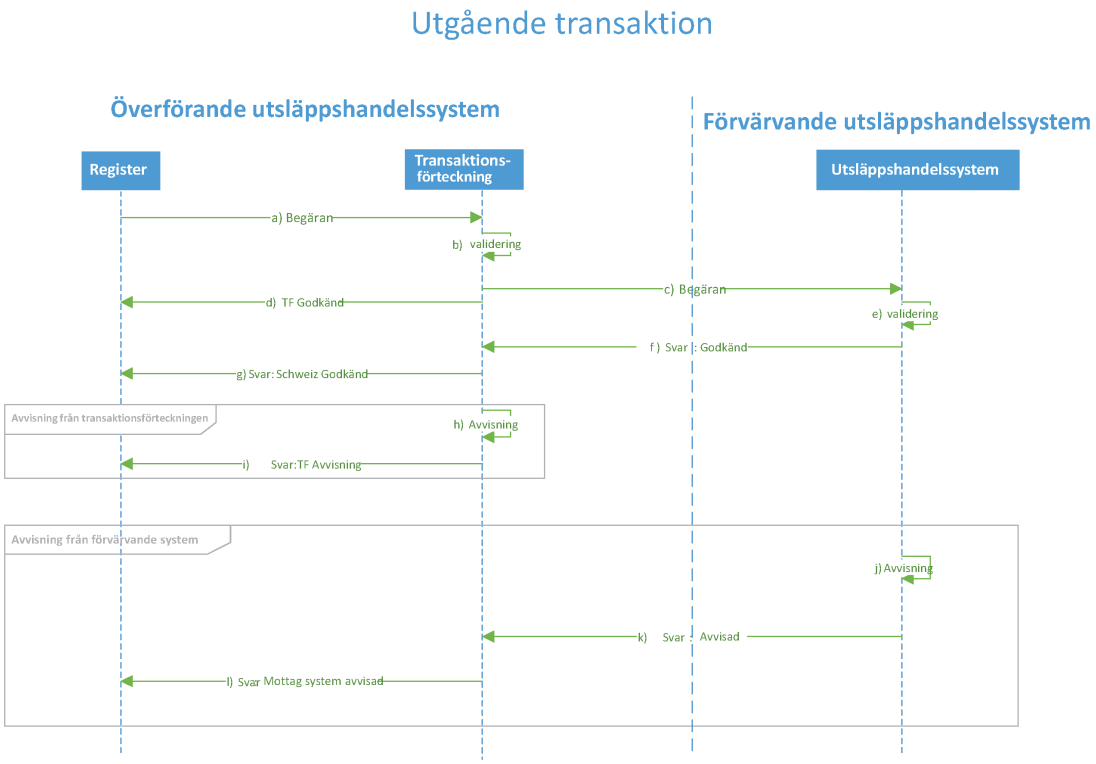
Den permanenta registerkopplingen bygger på fördefinierade tidsluckor för intagning som följs av en rad specifika namngivna händelser. Transaktionsbegäranden som tas emot via kopplingen tas in endast med fördefinierade intervall. Tidsluckor för intagning omfattar en teknisk validering av utgående och 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. Detta flöde återges i följande sekvensdiagram:



Huvudflödet består av följande steg (angivna i ovanstående flödesschema):

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” (angivet i ovanstående flödesschema; inleds med steg a i huvudflödet):

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

b) Transaktionsförteckningen validerar inte begäran.

c) Avvisningsmeddelande skickas till det avsändande registret.

Det alternativa flödet ”Avvisning från utsläppshandelssystemet” (angivet i ovanstående flödesschema; inleds med steg d i huvudflödet):

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.

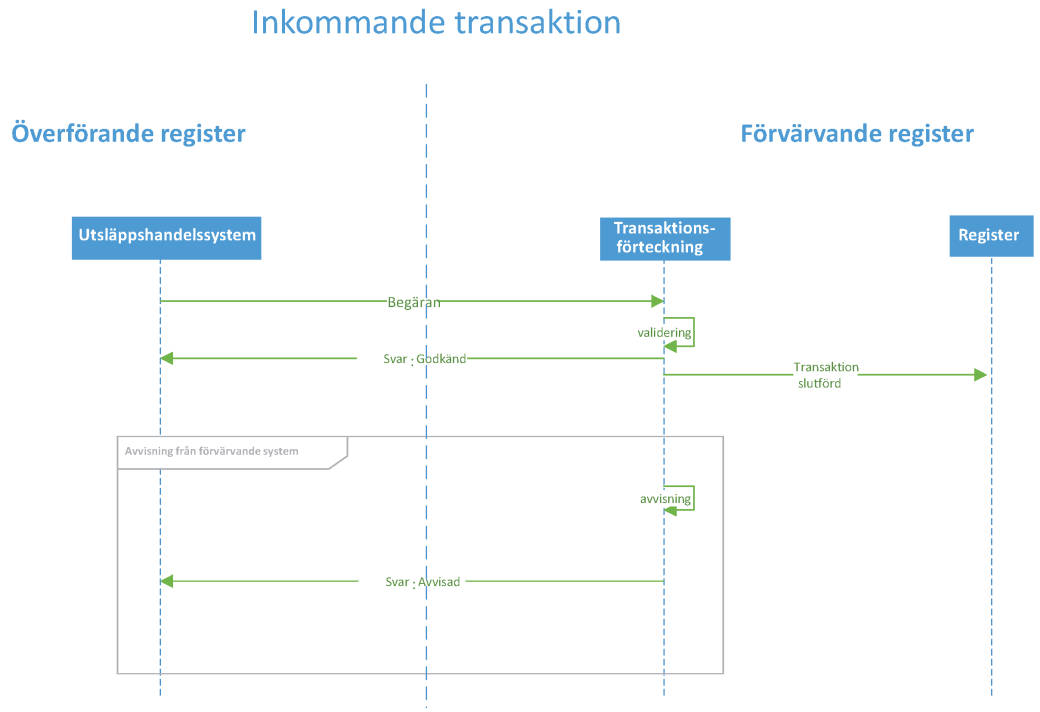
e) Det förvärvande utsläppshandelssystemets transaktionsförteckning validerar inte transaktionen.

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 från överförande utsläppshandelssystem → förvärvande utsläppshandelssystem.

— Transaktionssvar från förvärvande utsläppshandelssystem → överförande utsläppshandelssystem: antingen Godkänd (Accepted) eller Avvisad (Rejected) (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 utsläppshandelssystemet avbryter alla föreslagna transaktioner som har status ”föreslagen” 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 åtkomst till nätverket: brandvägg och nätverksskikt.

2) Kryptering i transportskikt: VPN.

3) Kryptering i sessionsskikt: säkert överföringsprotokoll för utbyte av meddelanden.

4) Kryptering i applikationsskikt: kryptering av XML-innehåll, samt 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” klienter kan ansluta sig till VPN-servern.

3.2.2. Virtuellt privat nätverk (VPN)

All kommunikation mellan parterna ska skyddas med hjälp av teknik för virtuellt privat nätverk (VPN). VPN-tekniken ger möjlighet att skapa en ”tunnel” mellan två punkter i ett nätverk som till exempel internet för att skydda all kommunikation. Innan VPN-tunneln skapas utfärdas ett digitalt certifikat för en blivande klients ändpunkter, 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.

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

Europeiska unionen använder generellt de säkra transeuropeiska telematiktjänsterna för myndigheter (s-Testa) som ett privat IP-baserat nätverk. Det är därför lämpligt att använda detta nätverk till den permanenta registerkopplingen.

3.2.3. Implementering av IPSec

Användning av IPSec-protokollet för VPN-infrastruktur plats-till-plats kommer att möjliggöra autentisering, dataintegritet och datakryptering. 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 sekretess garanteras genom IPSec-kryptering.

3.2.4. Säkert meddelandeöverföringsprotokoll

Den permanenta registerkopplingen använder flera krypteringsskikt för att parterna säkert ska kunna utbyta data. Båda systemen och deras olika miljöer är sammankopplade på nätverksnivå genom VPN-tunnlar. 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 identitet 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 i EU:s system (EUA).

    — Utsläppsrätter för luftfart i EU:s system (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 tidsluckorna 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 initiera 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 prov och besvaras av den andra ändpunkten vid mottagandet.

3.4. Kraven för registrering av data

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 specifikt 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, innehållande avstämnings-id, tidsstämpel och avstämningens resultat: avstämningsstatus ”Godkänd” (”Pass”) eller ”Avvikelser” (”Discrepancies”). I den permanenta registerkopplingen är avstämningsmeddelanden ett väsentligt inslag i utbytet av meddelanden och sparas därför på det sätt som beskrivs i avsnittet om meddelandearkivet.

Båda parterna ska registrera 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.

3.5. Driftskrav

Utbytet av uppgifter mellan de båda systemen är inte helt autonoma i den permanenta registerkopplingen, vilket innebär att det krävs operatörer och förfaranden för att praktiskt genomföra sammankopplingen. Ett flertal roller och verktyg beskrivs därför i den här processen.

4. TILLGÄNGLIGHET

4.1. Utformning för tillgänglig kommunikation

Arkitekturen för den permanenta registerkopplingen 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 sekretess för detta dataflöde vid utformningen av 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 block. När det gäller IKT-infrastrukturen upprättar den permanenta registerkopplingen ett motståndskraftigt VPN-nät 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 permanenta registerkopplingen utbyter parterna data med fördefinierade intervaller. 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 tidsluckor för varje steg,

— bygger programmodulerna för den permanenta registerkopplingen 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 permanenta registerkopplingens arkitektur ska genomgå en rad individuella och kollektiva test för att bekräfta att plattformen är redo på nivån för IKT-infrastruktur och informationssystem. Dessa driftprov är en nödvändig förutsättning varje gång den permanenta registerkopplingen övergår från pausat läge (*Suspended*) till driftsläge (*Operational*) på plattformen.

För att kopplingen ska kunna tas i drift måste följaktligen en fördefinierad provningsplan framgångsrikt genomföras. Denna ska bekräfta att varje register först har genomfört en rad interna provningar, följda av en validering av förbindelsen ändpunkt-till-ändpunkt, 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 registrering 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 parters registerförvaltare vid respektive 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 någondera parten och avslutande av provningarna kräver 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 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 (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

Dessa provningar ska utföras och/eller utlösas av registerförvaltare 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 permanenta registerkopplingen anses vara i driftläge.

Resurser för provning

Varje part ska använda specifika resurser för provning (specifik 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 ändpunkterna. De automatiska provningarna omfattar infrastrukturens olika delar och kommunikationskanalernas tillgänglighet.

— Applikationsövervakning: den permanenta registerkopplingens programmoduler genomför övervakning av systemkommunikationen på applikationsnivå (antingen manuellt och/eller med regelbundna intervall) som provar kopplingens tillgänglighet 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 verkliga data och behandlar verkliga transaktioner.

— Acceptans (ACC): denna miljö omfattar fiktiva eller anonymiserade, representativa data. I denna miljö validerar båda parters systemoperatörer nya releaser.

— Prov (TEST): denna miljö omfattar fiktiva eller anonymiserade, representativa data. Miljön är endast avsedd för registerförvaltare och ska användas av båda parter för integrationsprov.

Med undantag för VPN 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.

När det gäller VPN måste kommunikationen mellan de tre miljöerna vara helt oberoende, vilket säkerställs genom att använda s-Testa.

5. KONFIDENTIALITET OCH INTEGRITET

Säkerhetsmekanismerna och säkerhetsförfarandena bygger på en metod med två personer (fyra ögon) för verksamhet som sker 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 processer 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 acceptansmiljöerna (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) säkerhetsprovas.

Infrastrukturen för provning måste vara skild från produktionsmiljön på både nätverks- och infrastrukturnivå. Det är infrastrukturen för provning som möjliggör den provning av säkerheten som krävs för att kontrollera överensstämmelsen med säkerhetskraven.

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

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

— av 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 inkommande och utgående förbindelser helt eller delvis).

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 sekretess 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 och märkas med ”SPECIALHANTERING (SPECIAL HANDLING: *ETS Critical*)” 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 releaser 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 release 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 enligt samma princip som anges i föregående avsnitt med hjälp av en aktuell 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 ”SPECIALHANTERING (SPECIAL HANDLING: ETS Critical)” i enlighet med hanteringsanvisningarna.