EUROPESE
COMMISSIE

Brussel, 30.6.2020
COM(2020) 271 final

ANNEX

BIJLAGE

bij

Voorstel voor een besluit van de Raad

betreffende het standpunt dat namens de Europese Unie moet worden ingenomen in het Gemengd Comité dat is opgericht bij de overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten, wat de wijziging van de bijlagen I en II bij de koppelingsovereenkomst en de aanneming van koppelingstechnische normen betreft

BESLUIT Nr. 2/2020 VAN HET GEMENGD COMITÉ DAT IS OPGERICHT BIJ DE OVEREENKOMST TUSSEN DE EUROPESE UNIE EN DE ZWITSERSE BONDSSTAAT INZAKE DE KOPPELING VAN HUN REGELINGEN VOOR DE HANDEL IN BROEIKASGASEMISSIERECHTEN

van ...

met betrekking tot de wijziging van de bijlagen I en II bij de overeenkomst en tot koppelingstechnische normen (LTS)

HET GEMENGD COMITÉ,

Gezien de Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten[1] (hierna "de overeenkomst"), en met name artikel 3, lid 7, en artikel 13, lid 2,

Overwegende hetgeen volgt:

(1) Bij Besluit nr. 2/2019 van het Gemengd Comité van 5 december 2019[2] zijn de bijlagen I en II bij de overeenkomst gewijzigd waardoor de in de overeenkomst gestelde voorwaarden voor de koppeling zijn vervuld.

(2) Na de vaststelling van Besluit nr. 2/2019 van het Gemengd Comité en overeenkomstig artikel 21, lid 3, van de overeenkomst hebben de partijen hun akten van ratificatie uitgewisseld, aangezien zij van oordeel zijn dat alle in de overeenkomst gestelde voorwaarden voor de koppeling zijn vervuld.

(3) Overeenkomstig artikel 21, lid 4, van de overeenkomst is de overeenkomst op 1 januari 2020 in werking getreden.

(4) Bijlage I bij de overeenkomst moet worden gewijzigd overeenkomstig artikel 13, lid 2, van de overeenkomst om te zorgen voor de soepele administratieve overgang van vliegtuigexploitanten die voor het eerst aan Zwitserland worden toegewezen, door rekening te houden met de vooruitgang die is geboekt bij de uitvoering van de registerkoppeling.

(5) Om rekening te houden met recente ontwikkelingen en om te zorgen voor een grotere mate van flexibiliteit om de door de overeenkomst vereiste registerkoppeling vast te stellen, moet bijlage II bij de overeenkomst overeenkomstig artikel 13, lid 2, van de overeenkomst worden gewijzigd om te voorzien in een grotere maar gelijkwaardige reeks technologieën voor het opzetten van de registerkoppeling.

(6) Overeenkomstig artikel 3, lid 7, van de overeenkomst ontwikkelen de Zwitserse registeradministrateur en de centrale administrateur van de Unie de koppelingstechnische normen op basis van de in bijlage II bij de overeenkomst uiteengezette beginselen. In de koppelingstechnische normen worden de gedetailleerde eisen voor het tot stand brengen van een robuuste en veilige verbinding tussen het Zwitserse aanvullende transactielogboek (SSTL) en het EU-transactielogboek (EUTL) beschreven. De koppelingstechnische normen moeten in werking treden wanneer zij bij besluit van het Gemengd Comité zijn vastgesteld.

(7) Overeenkomstig artikel 13, lid 1, van de overeenkomst kan het Gemengd Comité technische richtsnoeren goedkeuren om de correcte uitvoering van de overeenkomst te verzekeren, waaronder de totstandbrenging van een robuuste en veilige verbinding

[1] PB L 322 van 7.12.2017, blz. 3.

[2] PB XXXX.

tussen het SSTL en het EUTL. Technische richtsnoeren kunnen worden ontwikkeld door een overeenkomstig artikel 12, lid 5, van de overeenkomst opgerichte werkgroep. De werkgroep moet ten minste de Zwitserse registeradministrateur en de centrale administrateur van het EU-register omvatten en moet het Gemengd Comité bijstaan in zijn functies uit hoofde van artikel 13 van de overeenkomst.

(8) Gezien de technische aard van de richtsnoeren en de noodzaak deze aan te passen aan de lopende ontwikkelingen, moeten de technische richtsnoeren die door de Zwitserse registeradministrateur en de centrale administrateur van de Unie zijn ontwikkeld, ter informatie of, in voorkomend geval, ter goedkeuring aan het Gemengd Comité worden voorgelegd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Bijlage I, deel B, punt 17, tweede alinea, bij de overeenkomst wordt vervangen door de volgende tekst:

Vliegtuigexploitanten die voor het eerst na de inwerkingtreding van deze overeenkomst aan Zwitserland worden toegewezen, zullen na 30 april van het jaar van toewijzing en zodra de voorlopige registerkoppeling is gerealiseerd, door Zwitserland worden beheerd.

Artikel 2

In bijlage II bij de overeenkomst wordt de vierde alinea vervangen door:

"In de LTS moet worden aangegeven dat de communicatie tussen het SSTL en het EUTL verloopt via de beveiligde uitwisseling van webdienstberichten op basis van de volgende technologieën[3] of equivalenten ervan:

- webdiensten die gebruik maken van Simple Object Access Protocol (SOAP);
- virtueel particulier netwerk (VPN) met eigen hardware;
- XML (Extensible Markup Language);
- digitale handtekening, en
- Network Time Protocol."

Artikel 3

De aan dit besluit gehechte koppelingstechnische normen (LTS) worden vastgesteld.

Artikel 4

Overeenkomstig artikel 12, lid 5, van de overeenkomst wordt hierbij een werkgroep opgericht. De werkgroep assisteert het Gemengd Comité ter waarborging van de correcte uitvoering van de overeenkomst, met inbegrip van de ontwikkeling van technische richtsnoeren voor de uitvoering van de LTS.

[3] Die technologieën worden momenteel toegepast voor het maken van een verbinding tussen het EU-register en het internationale transactielogboek, alsook tussen het Zwitserse register en het internationale transactielogboek.

De werkgroep omvat ten minste de Zwitserse registeradministrateur en de centrale administrateur van de Unie.

Artikel 5

Dit besluit treedt in werking op de dag waarop het wordt vastgesteld.

Opgemaakt in het Engels te Brussel op XX 2020.

Voor het Gemengd Comité

Secretaris voor de Europese Unie	*De voorzitter*	*Secretaris voor Zwitserland*

BIJLAGE

KOPPELINGSTECHNISCHE NORMEN (LTS)

uit hoofde van artikel 3, lid 7, van de overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten

Norm voor voorlopige oplossing

1. VERKLARENDE WOORDENLIJST

Tabel 1-1 Bedrijfsacroniemen en definities

Acroniem/term	Definitie
CH	Zwitserse Bondsstaat.
CHU	Zwitserse algemene emissierechten (de term "CHU2" wordt gebruikt als afkorting voor de CHU-emissierechten voor de vastleggingsperiode 2).
CHUA	Emissierechten van de Zwitserse luchtvaart.
Emissierecht	Een emissierecht om gedurende een bepaalde periode één ton kooldioxide-equivalent uit te stoten, dat alleen geldig is om te voldoen aan de vereisten van het EU-ETS of de ETS van Zwitserland.
ETR	Emissiehandelsregister.
ETS	Emissiehandelssysteem/emissiehandelsregeling.
EU	Europese Unie.
EUA	Algemene emissierechten van de EU.
EUAA	Luchtvaartemissierechten van de EU.
EUCR	Geconsolideerd register van de Europese Unie.
EUTL	Het EU-transactielogboek.
GOP	Gemeenschappelijke operationele procedures die gezamenlijk door de partijen bij de overeenkomst zijn ontwikkeld om de koppeling tussen het EU-ETS en de ETS van Zwitserland te realiseren.
Register	Een boekhoudsysteem voor emissierechten die zijn verleend in het kader van de ETS, waarin eigendom van rechten in elektronische accounts wordt bijgehouden.
SSTL	Zwitsers aanvullend transactielogboek.

Transactie	Een proces in een register waarbij een emissierecht van een rekening naar een andere rekening wordt overgedragen.
Transactielogboek	Het transactielogboek bevat een register van elke voorgestelde transactie die van de ene Griffie naar de andere wordt verzonden.

Tabel 1-2 Technische acroniemen en definities

Acroniem	Definitie
Afstemmingsproces	Proces om ervoor te zorgen dat twee reeksen gegevens met elkaar overeenstemmen.
Asymmetrische cryptografie	Maakt gebruik van publieke en private sleutels voor het versleutelen en ontsleutelen van gegevens.
Bestandopname	Het proces waarbij een bestand wordt gelezen.
Certificerings-autoriteit (CA)	Entiteit die digitale certificaten uitgeeft.
Cryptografische sleutel	Een stuk informatie dat de functionele output van een cryptografisch algoritme bepaalt.
Digitale handtekening	Een mathematische techniek die wordt gebruikt om de authenticiteit en integriteit van een bericht, software of digitaal document te valideren.
Firewall	Apparatuur of software voor netwerkbeveiliging die het inkomende en uitgaande netwerkverkeer monitort en controleert op basis van vooraf vastgestelde regels.
Heartbeatmonitoring	Periodiek door hardware of software gegenereerd en bewaakt signaal om de normale werking aan te geven of om andere delen van een computersysteem te synchroniseren.
IPsec	IP SECurity (IP-beveiliging). Netwerkprotocolsuite die de gegevenspakketten authenticeert en versleutelt om te zorgen voor een beveiligde, versleutelde communicatie tussen twee computers over een internetprotocolnetwerk.
Ontsleuteling	Omgekeerd proces van versleuteling.
Penetratietest	Praktijk van het testen van een computersysteem, netwerk of webtoepassing om beveiligingskwetsbaarheden op te sporen die een aanvaller zou kunnen exploiteren.
Versleuteling	Het omzetten van informatie of gegevens in een code, met name om ongeoorloofde toegang te voorkomen.
VPN	Virtueel particulier netwerk.

XML	Extensible Mark-up Language. Biedt ontwerpers de mogelijkheid om hun eigen specifieke tags te creëren, waardoor de gegevens tussen de verschillende toepassingen en tussen de verschillende organisaties kunnen worden gedefinieerd, verzonden, gevalideerd en geïnterpreteerd.

2. INLEIDING

De Overeenkomst tussen de Europese Unie en de Zwitserse Bondsstaat inzake de koppeling van hun regelingen voor de handel in broeikasgasemissierechten van 23 november 2017 (hierna "de overeenkomst" genoemd) voorziet in de wederzijdse erkenning van emissierechten die in het kader van het emissiehandelssysteem van de Europese Unie ("EU-ETS") of de emissiehandelsregeling van Zwitserland ("ETS van Zwitserland") kunnen worden gebruikt. Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, wordt een directe koppeling tussen het EU-transactielogboek (EUTL) van het register van de Unie en het Zwitserse aanvullende transactielogboek (SSTL) van het Zwitserse register tot stand gebracht, waardoor onder een van beide regelingen verleende emissierechten van de ene naar de andere ETS zullen kunnen worden overgedragen (artikel 3, lid 2, van de overeenkomst). Om de koppeling tussen het EU-ETS en de ETS van Zwitserland operationeel te maken, wordt tegen mei 2020 of zo spoedig mogelijk daarna in een voorlopige oplossing voorzien. De partijen werken samen om de voorlopige oplossing zo spoedig mogelijk door een permanente registerkoppeling te vervangen (bijlage II bij de overeenkomst).

Overeenkomstig artikel 3, lid 7, van de overeenkomst stellen de Zwitserse registeradministrateur en de centrale administrateur van de Unie op basis van de beginselen in bijlage II van de overeenkomst koppelingstechnische normen vast waarin de gedetailleerde eisen voor het tot stand brengen van een robuuste en veilige verbinding tussen het SSTL en het EUTL worden beschreven. De door de administrateurs ontwikkelde koppelingstechnische normen treden in werking wanneer zij bij besluit van het Gemengd Comité zijn aangenomen.

De in dit document opgenomen LTS moeten door het Gemengd Comité bij Besluit nr. 2/2020 worden vastgesteld. Overeenkomstig dat besluit verzoekt het Gemengd Comité de Zwitserse registeradministrateur en de centrale administrateur van de Unie om verdere technische richtsnoeren te ontwikkelen om de link te realiseren en ervoor te zorgen dat deze voortdurend worden aangepast aan de technische vooruitgang en aan nieuwe eisen met betrekking tot de veiligheid en beveiliging van de verbinding en tot de doeltreffende en efficiënte werking ervan.

2.1. Toepassingsgebied

Dit document omvat het akkoord tussen de partijen bij de overeenkomst over de totstandbrenging van de technische grondslag van de koppeling tussen de registers van het EU-ETS en de ETS van Zwitserland. Dit document vormt de basis voor de technische specificaties met betrekking tot eisen op het gebied van architectuur, dienstverlening en beveiliging, maar enkele verdere gedetailleerde richtsnoeren zijn nodig om koppeling operationeel te maken.

Voor de goede werking van de koppeling zullen processen en procedures nodig zijn om de koppeling verder te realiseren. Overeenkomstig artikel 3, lid 6, van de overeenkomst worden deze kwesties in detail beschreven in een apart document betreffende gemeenschappelijke operationele procedures (GOP), dat afzonderlijk bij besluit van het Gemengd Comité moet worden aangenomen.

2.2. Adressaten

Dit document is gericht tot de Zwitserse registeradministrateur en de centrale administrateur van het EU-register.

3. ALGEMENE BEPALINGEN

3.1. Architectuur van de communicatiekoppeling

Het doel van dit hoofdstuk is een beschrijving te geven van de algemene architectuur van de realisering van de koppeling tussen het EU-ETS en de ETS van Zwitserland en de verschillende onderdelen ervan.

Beveiliging is een essentieel onderdeel van een robuuste architectuur, en daartoe zijn alle nodige maatregelen genomen. Hoewel de geplande permanente registerkoppeling op webdiensten gebaseerd zal zijn, wordt voor de voorlopige oplossing een mechanisme voor het uitwisselen van bestanden worden gebruikt.

Voor de technische oplossing wordt gebruikgemaakt van:

- een beveiligd protocol voor de uitwisseling van berichten;
- XML-berichten;
- op XML gebaseerde digitale ondertekening en versleuteling;
- VPN-diensten of een gelijkwaardig beveiligd datatransportnetwerk.

3.1.1. Uitwisseling van berichten

De communicatie tussen het EU-register en het Zwitserse register wordt gebaseerd op een mechanisme voor de uitwisseling van berichten via beveiligde kanalen. Elke partij bewaard de ontvangen berichten in een eigen register.

De partijen houden een logboek van de ontvangen berichten bij, alsmede van de gegevens betreffende de verwerking.

Fouten of onverwachte statussen moeten als waarschuwing worden gemeld, waarna menselijk contact tussen de ondersteunende teams moet plaatsvinden.

Fouten en onverwachte gebeurtenissen worden behandeld met inachtneming van de in het kader van het incidentenbeheerproces van de GOP vastgestelde operationele procedures.

3.1.2. XML-bericht — Beschrijving op hoog niveau

Een XML-bericht bevat een van de volgende elementen:

- een of meer transactieverzoeken en/of een of meerdere transactierespons;
- één actie/respons in verband met de afstemming;
- één testbericht.

Elk bericht bevat een header met:

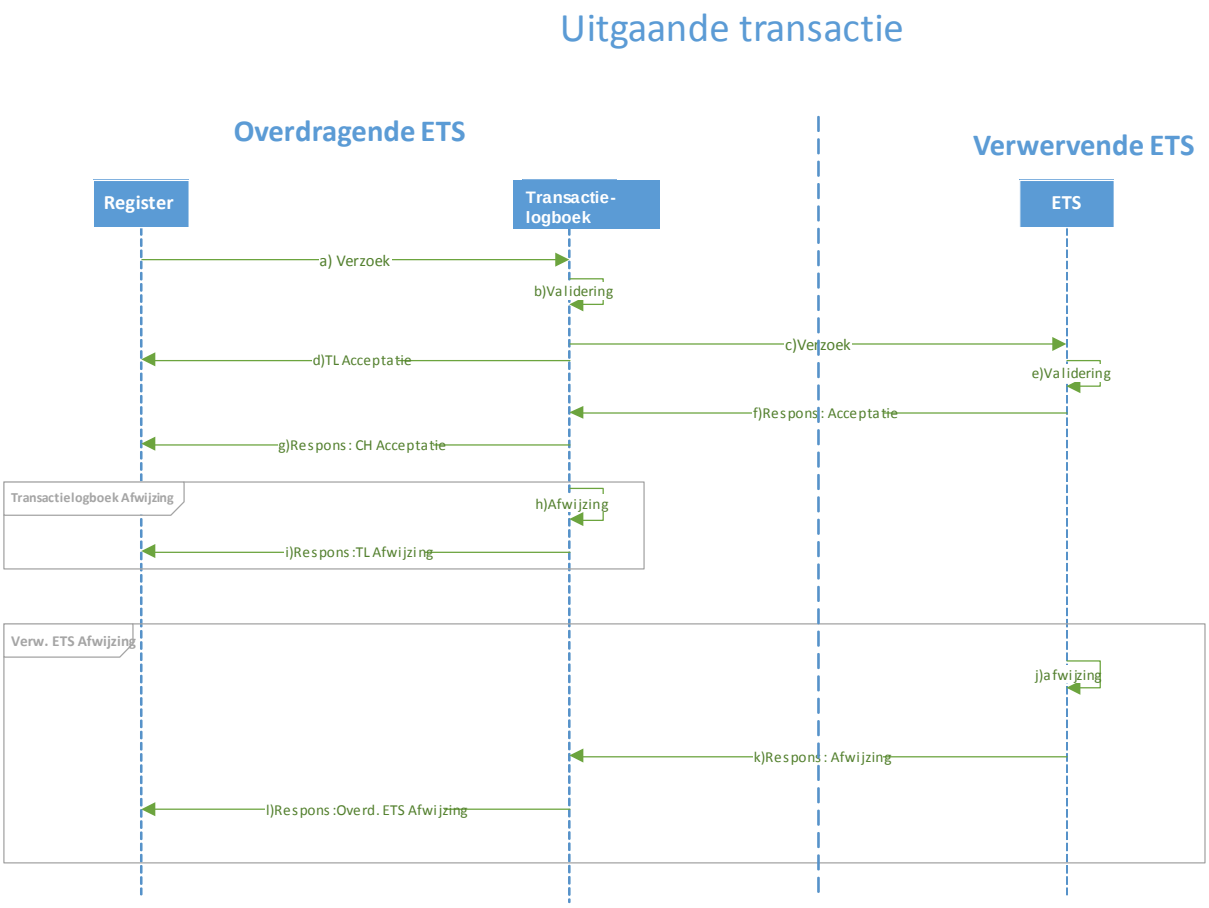
- het ETS-systeem waarvan het afkomstig is;
- een volgnummer

3.1.3. Opnamevensters

De voorlopige oplossing is gebaseerd op vooraf gedefinieerde opnamevensters die worden gevolgd door een reeks van benoemde gebeurtenissen ("named events"). De via de verbinding ontvangen transactieverzoeken worden uitsluitend tijdens van tevoren vastgestelde vensters opgenomen. Voor uitgaande en inkomende transacties wordt een technische validatie verricht. Daarnaast kunnen afstemmingen dagelijks worden uitgevoerd en manueel worden geactiveerd.

Wijzigingen in de frequentie en/of timing van een of meer van deze gebeurtenissen worden behandeld met inachtneming van de in het kader van de inwilliging van verzoeken van de GOP vastgestelde operationele procedures.

3.1.4. Transactieberichtenstroom



Uitgaande transacties

Dit is een weergave van het perspectief van de ETS die de overdracht doet. Het bovenstaande schema toont alle specifieke uitgaande transactiestromen.

Hoofdstroom "Normale transactie" (met de in het schema aangegeven stappen):

a) Bij de ETS die de overdracht doet, wordt het transactieverzoek van het register naar het transactielogboek verzonden zodra de bedrijfsvertraging voorbij is (24 uur vertraging, indien van toepassing).

b) Het transactielogboek valideert het transactieverzoek.

c) Het verzoek om een transactie wordt naar de ETS van bestemming verzonden.

d) De acceptatierespons wordt naar het register van de ETS van oorsprong verzonden.

e) De ETS van bestemming valideert het transactieverzoek.

f) De ETS van bestemming stuurt de acceptatierespons terug naar het transactielogboek van de ETS van oorsprong.

g) Het transactielogboek stuurt de acceptatierespons naar het register.

Alternatieve stroom “Afwijzing door transactielogboek” (met de in het schema aangegeven stappen, beginnend bij a)):

a) In het systeem van oorsprong wordt het transactieverzoek van het register naar het transactielogboek verzonden zodra de bedrijfsvertraging voorbij is (24 uur vertraging, indien van toepassing).

Gevolgd door:

b) Het transactielogboek valideert het verzoek niet.

c) Het afwijzingsbericht wordt verzonden naar het register van oorsprong.

Alternatieve stroom “Afwijzing door ETS” (met de in het schema aangegeven stappen, beginnend bij a)):

a) In de ETS van oorsprong wordt het transactieverzoek van het register naar het transactielogboek verzonden zodra de bedrijfsvertraging voorbij is (24 uur vertraging, indien van toepassing).

b) Het transactielogboek valideert de transactie.

c) Het verzoek om een transactie wordt naar de ETS van bestemming verzonden.

d) De acceptatierespons wordt naar het register van de ETS van oorsprong verzonden.

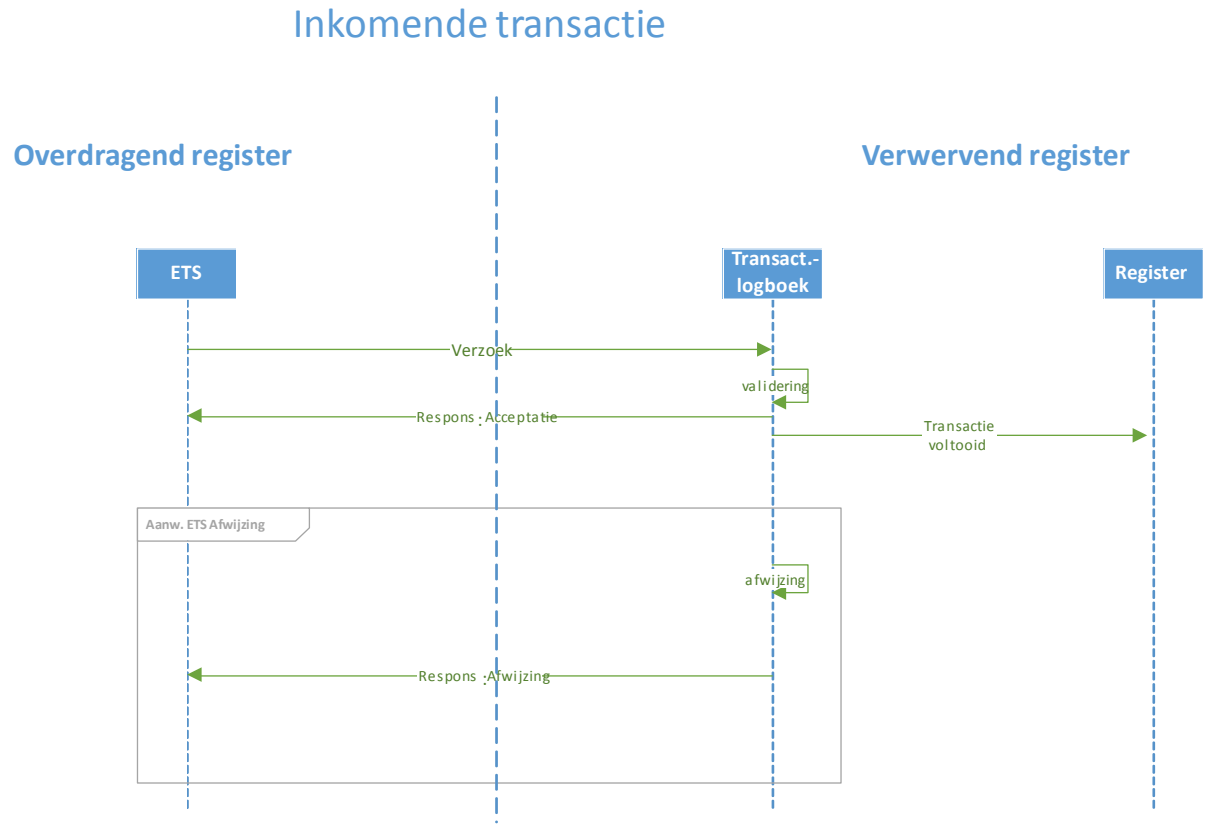
Gevolgd door:

e) De het transactielogboek van de verwervende ETS valideert de transactie niet.

f) De verwervende ETS stuurt de afwijzingsrespons naar het transactielogboek van de overdragende ETS.

g) Het transactielogboek stuurt de afwijzing naar het register.

Inkomende transacties



Dit is een weergave van het perspectief van de verwervende ETS. De specifieke stroom wordt weergegeven in het volgende schema:

Het schema toont:

1. Wanneer het transactielogboek van de verwervende ETS het verzoek valideert, stuurt het de acceptatierespons naar de overdragende ETS en een bericht "transactie voltooid" naar het register van de verwervende ETS.
2. Wanneer een inkomend verzoek binnenkomt op het verwervende transactielogboek en wordt geweigerd, wordt het transactieverzoek niet naar het register van de verwervende ETS gestuurd.

Protocol

De transactieberichtencyclus omvat slechts twee berichten:

- Overdragende ETS→ Verwervende ETS: transactievoorstel
- Verwervende ETS→ Overdragende ETS: transactierespons: acceptatie of afwijzing (met vermelding van de reden voor afwijzing).
  - Acceptatie: de transactie is voltooid.
  - Afwijzing: de transactie is beëindigd.

Transactiestatus

- De transactiestatus van de overdragende ETS wordt veranderd in "voorgesteld" wanneer het verzoek wordt verzonden.
- De transactiestatus van de verwervende ETS wordt veranderd in "voorgesteld" wanneer het verzoek wordt ontvangen en wordt behandeld.

- De transactiestatus van de verwervende ETS wordt veranderd in "voltooid"/"beëindigd" nadat het voorstel is verwerkt. De verwervende ETS stuurt vervolgens het bijbehorende bericht van acceptatie/afwijzing.
- De transactiestatus van de overdragende ETS wordt veranderd in "voltooid/beëindigd" nadat het bericht van acceptatie/afwijzing wordt ontvangen en verwerkt.
- In de overdragende ETS blijft de transactiestatus "voorgesteld" indien geen respons wordt ontvangen.
- De verwervende ETS geeft elke transactie die langer dan 30 minuten op "voorgesteld" staat, de status "beëindigd".

Incidenten in verband met transacties worden behandeld met inachtneming van de in het kader van het incidentenbeheerproces van de GOP vastgestelde operationele procedures.

3.2. Beveiliging van gegevensoverdracht

Verstuurde gegevens worden onderworpen aan vier beveiligingsniveaus:

1) Controle van de toegang tot het netwerk: firewall en netwerkinterconnectie.
2) Versleuteling tijdens het vervoer: VPN of gelijkwaardig beveiligd datatransportnetwerk.
3) Versleuteling tijdens sessie: overdrachtprotocol voor beveiligde uitwisseling van berichten.
4) Versleuteling op niveau van de toepassing: XML-inhoudversleuteling en -ondertekening.

3.2.1. Firewall en netwerkinterconnectie

De verbinding wordt gelegd over een netwerk dat wordt beschermd door een op hardware gebaseerde firewall. De firewall moet zodanig worden geconfigureerd dat alleen "geregistreerde" clients verbindingen met de VPN-server kunnen maken.

3.2.2. Virtueel particulier netwerk (VPN)

Alle communicatie tussen de partijen wordt beschermd door middel van een beveiligde technologie voor dataverkeer. In het geval van een virtueel particulier netwerk (VPN) moet de infrastructuur gebaseerd zijn op hardware of virtuele appliances. VPN-technologieën bieden de mogelijkheid om via een netwerk zoals het internet van de ene plaats naar de andere te "tunnelen", waarbij alle communicatie wordt beschermd. Voorafgaand aan de oprichting van de VPN-tunnel wordt een digitaal certificaat afgegeven aan het eindpunt van een mogelijke client, zodat de client bij het verbinden het bewijs van de identiteit kan overleggen. Elke partij is verantwoordelijk voor de installatie van het certificaat in het eigen VPN-eindpunt. Door gebruik te maken van digitale certificaten krijgt elke VPN-server toegang tot een centrale autoriteit voor het uitwisselen van authenticatiegegevens. Bij het opzetten van de tunnel wordt versleuteling uitgevoerd, zodat alle communicatie via de tunnel wordt beschermd.

De VPN-eindpunten van de clients zijn zodanig geconfigureerd dat de VPN-tunnel permanent in stand wordt gehouden, zodat te allen tijde betrouwbare communicatie in realtime en in beide richtingen tussen de partijen mogelijk is.

Elke andere gelijkwaardige oplossing moet voldoen aan bovengenoemde beginselen.

3.2.3. Uitvoering van IPSec

Indien een VPN-oplossing wordt gebruikt, zal het gebruik van het IPSec-protocol om de site-to-site VPN-infrastructuur te vormen, zorgen voor site-to-site authenticatie, de integriteit van de gegevens en gegevensversleuteling. IPsec-VPN-configuraties zorgen voor de juiste authenticatie tussen twee eindpunten in een VPN-verbinding. De partijen identificeren en authenticeren de client op afstand via de IPSec-verbinding door middel van digitale certificaten die worden verstrekt door een door het andere einde erkende certificeringsautoriteit.

IPsec waarborgt ook de integriteit van alle communicatie via de VPN-tunnel. Gegevenspakketten worden gehashed en ondertekend door middel van de authenticatie-informatie die door het VPN is ingevoerd. De vertrouwelijkheid van de gegevens wordt ook gewaarborgd door IPSec-versleuteling mogelijk te maken.

3.2.4. Overdrachtprotocol voor beveiligde uitwisseling van berichten

De voorlopige oplossing berust op meerdere versleutelingslagen voor de beveiligde uitwisseling van gegevens tussen de partijen. Beide systemen en hun verschillende omgevingen zijn op het niveau van het netwerk met elkaar verbonden door middel van VPN-tunnels of gelijkwaardige beveiligde datatransportnetwerken. Op het niveau van de applicatie worden de bestanden overgedragen met behulp van een overdrachtprotocol voor de beveiligde uitwisseling van berichten op het niveau van de sessie.

3.2.5. XML-versleuteling en -ondertekening

In XML-bestanden vindt ondertekening en versleuteling plaats op twee niveaus. Elk(e) transactieverzoek, transactierespons en afstemmingsbericht wordt afzonderlijk digitaal ondertekend.

In een tweede stap wordt elk subelement van het “bericht”-element afzonderlijk versleuteld.

Als derde stap en om de integriteit en onweerlegbaarheid van het volledige bericht te waarborgen, wordt het kernelementbericht digitaal ondertekend. Dit resulteert in een hoog niveau van bescherming voor de in XML ingebedde gegevens. Bij de technische uitvoering worden de normen van het World Wide Web Consortium in acht genomen.

Voor het ontsleutelen en verifiëren van het bericht wordt het proces in omgekeerde volgorde uitgevoerd.

3.2.6. Cryptografische sleutels

Voor versleuteling en ondertekening wordt gebruik gemaakt van een openbare cryptographische sleutel.

Voor IPSec worden alleen digitale certificaten gebruikt die zijn afgegeven door een door beide partijen vertrouwde certificeringsautoriteit (CA). Deze CA is verantwoordelijk voor identiteitscontrole en de afgifte van certificaten die worden gebruikt om een organisatie te identificeren en beveiligde kanalen datacommunicatie tussen de partijen te op te zetten.

Cryptografische sleutels worden gebruikt voor het ondertekenen en versleutelen van communicatiekanalen en gegevensbestanden. De openbare certificaten worden door de partijen digitaal uitgewisseld door middel van beveiligde kanalen en geverifieerd buiten de band. Deze procedure maakt integraal deel uit van het proces informatiebeveiligingsbeheer van de GOP.

3.3. Lijst van functies in het kader van de koppeling

De koppeling specificeert het transmissiesysteem voor een reeks functies die de uit de overeenkomst voortvloeiende bedrijfsprocessen ten uitvoer leggen. De koppeling bevat eveneens de specificatie voor het afstemmingsproces en voor de testberichten die de uitvoering van een heartbeatmonitoring mogelijk maken.

3.3.1. Zakelijke transacties

Vanuit het bedrijfsperspectief behandelt de koppeling vier (4) soorten transactieverzoeken:

- Externe overdracht:
  - Na de inwerkingtreding van de ETS-koppeling zijn EU- en CH-emissierechten fungibel, en dus volledig overdraagbaar tussen de partijen.
  - Bij een overdracht via de koppeling zijn een overdragende rekening op de ene ETS en een verwervende rekening op de andere ETS betrokken.
  - De overdracht kan een of meer van de vier (4) soorten emissierechten omvatten:
    - Zwitserse algemene emissierechten (CHU)
    - Zwitserse luchtvaartemissierechten (CHUA)
    - Algemene EU-emissierechten (EUA)
    - EU-luchtvaartemissierechten (EUAA)
- Internationale toewijzing:

  Vliegtuigexploitanten die door de ene ETS worden geadministreerd met verplichtingen onder de andere ETS en recht hebben op kosteloze emissierechten van die tweede ETS, ontvangen kosteloze luchtvaartemissierechten van de tweede ETS via de internationale toewijzingstransactie.
- Terugdraaiing van de internationale toewijzing:

  Deze transactie vindt plaats in het geval dat de kosteloze toewijzing van emissierechten aan een vliegtuigexploitant door de andere ETS geheel moet worden teruggedraaid.
- Teruggave van overtollige toewijzing:

  Vergelijkbaar met terugdraaiing, maar de toewijzing hoeft niet geheel te worden teruggedraaid, en alleen de teveel toegewezen emissierechten moeten worden teruggegeven aan de toewijzende ETS.

3.3.2. Afstemmingsprotocol

Afstemmingen vinden pas plaats nadat de vensters voor de opname, validering en verwerking van berichten gesloten zijn.

Afstemmingen maken integraal deel uit van de beveiligings- en consistentiemaatregelen van de koppeling. De partijen moeten het exacte tijdstip van de afstemming overeenkomen alvorens een tijdschema op te stellen. Een dagelijks geplande afstemming kan plaatsvinden indien beide partijen daarmee instemmen. Na opname van berichten wordt echter ten minste een geplande afstemming uitgevoerd.

De partijen kunnen evenwel te allen tijde handmatige afstemmingen initiëren.

Wijzigingen in de frequentie en timing van de geplande afstemming worden behandeld met inachtneming van de in het kader van de inwilliging van verzoeken van de GOP vastgestelde operationele procedures.

3.3.3. Testbericht

Voor het testen van het communicatietraject is een testbericht voorzien. Het bericht bevat gegevens waarmee het als test wordt herkend, en wordt na ontvangst door de andere partij beantwoord.

3.4. Normen voor webdiensten

Webdiensten zullen in de voorlopige oplossing niet worden gebruikt. Er zij echter op gewezen dat de vorm en het formaat van XML-berichten in grote mate ongewijzigd zullen blijven. Met de toekomstige invoering van de permanente registerkoppeling moeten de webdiensten de uitwisseling van XML-berichten in real-time mogelijk maken.

3.5. Specifieke definitie van webdiensten

Dit hoofdstuk is niet van toepassing op de voorlopige oplossing. Zoals vermeld in het vorige hoofdstuk, zullen de webdiensten alleen worden gebruikt in de toekomstige permanente registerkoppeling.

3.6. Vereisten voor gegevensregistratie

Om te beantwoorden aan de behoefte van beide partijen aan het bijhouden van accurate en consistente informatie en te voorzien in instrumenten voor het gebruik in het afstemmingsproces om inconsistenties op te weg te nemen, worden door beide partijen vier (4) soorten gegevensregisters bijgehouden:

- transactielogboeken;
- afstemmingslogboeken;
- berichtarchieven;
- logboeken van interne controle.

Alle gegevens in deze logbestanden worden ten minste gedurende drie (3) maanden bewaard ten behoeve van het oplossen van problemen, en de verdere bewaring ervan voor controledoeleinden hangt af van het voor elke partij toepasselijke recht. Logbestanden ouder dan drie (3) maanden kunnen worden gearchiveerd in een beveiligde locatie in een onafhankelijk IT-systeem, op voorwaarde dat zij een redelijke termijn kunnen worden opgevraagd of toegankelijk zijn.

Transactielogboeken

De subsystemen van het EUTL en het SSTL bevatten transactielogboeken.

De transactielogboeken bevatten een registratie van elke voorgestelde transactie die naar de andere ETS wordt verzonden. Elke registratie bevat alle gegevensvelden van de transactie en de daaropvolgende uitkomst ervan (de respons van de ontvangende ETS). In de transactielogboeken wordt eveneens een register bijgehouden voor inkomende transacties alsmede voor de naar de ETS van oorsprong gestuurde respons.

Afstemmingslogboeken

Het afstemmingslogboek bevat een registratie van elk afstemmingsbericht dat tussen de partijen wordt uitgewisseld, met inbegrip van de afstemmingsidentificatiecode, het tijdstempel en het resultaat van de afstemming: de afstemmingsstatus "Pass" of "Discrepancies". Afstemmingsberichten maken in de voorlopige oplossing integraal deel uit van de uitgewisselde berichten.

Beide partijen registreren elk verzoek en de respons daarop in het afstemmingslogboek. Hoewel de informatie in het afstemmingslogboek tijdens de afstemming niet rechtstreeks wordt gedeeld, kan de toegang tot deze informatie noodzakelijk zijn om inconsistenties weg te nemen.

Archivering van berichten

Beide partijen moeten een kopie van de uitgewisselde (zowel verzonden als ontvangen) gegevens (de XML-bestanden) archiveren, met een vermelding of de XML-berichten in het juiste formaat waren verstuurd of niet.

Het belangrijkste doel van het archief is om in het kader van controles te kunnen nagaan wat van naar en van de andere partij is verzonden en ontvangen. Daartoe moeten behalve de dossiers ook de desbetreffende certificaten worden gearchiveerd.

Deze dossiers zullen ook aanvullende informatie opleveren voor het oplossen van problemen.

Logboeken van interne controle

Deze logboeken worden door elke partij afzonderlijk gedefinieerd en gebruikt.

3.7. Operationele vereisten

De uitwisseling van gegevens tussen beide systemen is in de voorlopige oplossing niet volledig autonoom; dit betekent dat exploitanten en procedures moeten worden ingeschakeld om de koppeling operationeel te maken.

4. BESCHIKBAARHEIDSBEPALINGEN

4.1. Ontwerp voor de beschikbaarheid van de communicatie

De architectuur voor de voorlopige oplossing is een ICT-infrastructuur en software die de communicatie tussen de ETS van Zwitserland en het EU-ETS mogelijk maakt. Het waarborgen van een hoog niveau van beschikbaarheid, integriteit en vertrouwelijkheid van deze gegevensstroom is dan ook een essentieel aspect dat moet worden meegenomen bij het ontwerp van de voorlopige oplossing en de permanente registerkoppeling. Aangezien de ICT-infrastructuur, de op maat gemaakte software en de processen een integrale rol in dit project spelen, moeten alle drie de elementen in aanmerking worden genomen om een bestendig systeem te ontwerpen.

Bestendigheid van de ICT-infrastructuur

In het hoofdstuk betreffende algemene bepalingen worden de bouwblokken van de architectuur beschreven. Wat de ICT-infrastructuur betreft, wordt in de voorlopige verbinding een veerkrachtig VPN-netwerk (of gelijkwaardig netwerk) opgezet dat veilige communicatietunnels creëert waarin beveiligde berichtenuitwisseling kan plaatsvinden. Andere elementen worden geconfigureerd voor een hoge beschikbaarheidsgraad en/of maken gebruik van terugvalmechanismen.

Bestendigheid van op maat gemaakte software

De op maat gemaakte softwaremodules vergroten de bestendigheid door de communicatie met de andere partij gedurende een bepaalde periode te trachten te herstellen indien die om welke reden dan ook niet beschikbaar is.

Bestendigheid van de dienst

De gegevensuitwisseling tussen de partij gebeurt in de voorlopige oplossing op vooraf bepaalde tijdstippen, het hele jaar door. Sommige van de stappen die vereist zijn in vooraf geplande gegevensuitwisseling vereisen handmatige tussenkomst van systeembeheerders en/of registeradministrateurs. Rekening houdend met dit aspect en met het oog op het vergroten van de beschikbaarheid en het succes van de uitwisselingen, worden de volgende maatregelen getroffen:

- De operationele procedures voorzien in significante tijdvensters voor de uitvoering van elke stap.
- De softwaremodules voor de voorlopige oplossing passen asynchrone communicatie toe.
- In het kader van het automatische afstemmingsproces zal worden vastgesteld of er problemen zijn geweest bij de opname van gegevensbestanden aan beide zijden.
- De monitoringprocessen (ICT-infrastructuren en op maat gemaakte softwaremodules) worden in overweging genomen bij incidentbeheerprocedures en activeren deze (zoals gedefinieerd in de gemeenschappelijke operationele procedures). Deze procedures die gericht zijn op het verkorten van de tijd die nodig is om de normale werking te herstellen na incidenten, zijn essentieel om een hoge beschikbaarheidsgraad te waarborgen.

4.2. Initialisatie, communicatie, heractivering en testplan

Alle verschillende elementen van de architectuur van de voorlopige oplossing moeten een reeks individuele en collectieve tests doorstaan om te bevestigen dat het platform klaar is wat de ICT-infrastructuur en het informatiesysteem betreft. Deze operationele tests zijn een verplichte voorwaarde telkens wanneer het platform overgaat van de onderbreking van de voorlopige oplossing naar de operationele status.

De activering van de operationele status van de koppeling vereist vervolgens de succesvolle uitvoering van een vooraf bepaald testplan. Dit bevestigt dat elk register eerst een reeks interne tests heeft uitgevoerd, gevolgd door een validering van de eind-tot-eindconnectiviteit voordat een begin wordt gemaakt met de indiening van productietransacties tussen beide partijen.

In het testplan moeten de algemene teststrategie en details over de testinfrastructuur worden vermeld. Voor elk element in elk testblok moet het testplan met name het volgende omvatten:

- de testcriteria en -instrumenten;
- de functies die voor de uitvoering van de test zijn aangewezen;
- de verwachte resultaten (positief en negatief);
- het testschema;
- de voorschriften voor het registreren van de testresultaten;

- documentatie over het oplossen van problemen;
- bepalingen inzake escalatie.

Als proces kunnen de activeringstests voor de operationele status worden opgesplitst in vier (4) conceptuele blokken of fasen:

4.2.1. Interne tests van de ICT-infrastructuur

Deze tests moeten door beide partijen aan elk einde afzonderlijk worden uitgevoerd en/of gecontroleerd.

Elk onderdeel van de ICT-infrastructuur aan elk einde wordt afzonderlijk getest. Dit omvat elk afzonderlijk onderdeel van de infrastructuur. Deze tests kunnen automatisch of manueel worden uitgevoerd, maar controleren of elk element van de infrastructuur operationeel is.

4.2.2. Communicatietests

Deze tests beginnen elk afzonderlijk bij elke partij en worden beëindigd in samenwerking met het andere einde.

Zodra individuele elementen operationeel zijn, moeten de communicatiekanalen tussen de beide registers worden getest. Daartoe controleert elke partij of de toegang tot het internet werkt, de VPN-tunnels (of een gelijkwaardig beveiligd transportnetwerk) zijn opgezet, en de IP-verbinding tussen de partijen werkt. De bereikbaarheid van de lokale infrastructuurelementen en die op afstand en de IP-connectiviteit moeten bij het andere einde worden bevestigd.

4.2.3. Volledige systeemtest (eind-tot-eind)

Deze tests moeten aan beide einden worden uitgevoerd en de resultaten moeten met de andere partij worden gedeeld.

Zodra de communicatiekanalen en elk afzonderlijk onderdeel van beide registers zijn getest, moet elk einde een reeks gesimuleerde transacties en afstemming daarvan voorbereiden die representatief zijn voor alle functies die binnen de koppeling moeten worden uitgevoerd.

4.2.4. Beveiligingstests

Deze tests dienen te worden uitgevoerd en/of te worden geactiveerd door beide partijen aan elk einde en zoals beschreven in de hoofdstukken “Richtsnoeren voor het testen van de beveiliging” en “Bepalingen inzake risicobeoordeling”.

Pas nadat elk van de vier fasen/blokken met voorspelbare resultaten zijn voltooid kan de voorlopige koppeling de operationele status worden toegekend.

Testmiddelen

Elke partij hanteert specifieke testmiddelen (specifieke ICT-infrastructuursoftware en -hardware) en ontwikkelt testfuncties in hun respectieve systemen ter ondersteuning van de handmatige en doorlopende validatie van het platform. Handmatige individuele of coöperatieve testprocedures kunnen te allen tijde door registeradministrateurs worden uitgevoerd. Activering van de operationele status is van nature een handmatig proces.

Het is eveneens de bedoeling dat het platform op gezette tijden automatische controles uitvoert. Deze controles zijn erop gericht de beschikbaarheid van het platform te vergroten door potentiële problemen met de infrastructuur of software in een vroeg stadium op te sporen. Dit platformmonitoringplan bestaat uit twee elementen:

- Toezicht op ICT-infrastructuren: aan beide einden wordt de infrastructuur gemonitord door de aanbieders van de ICT-diensten. De automatische tests hebben betrekking op de verschillende infrastructuurelementen en de beschikbaarheid van de communicatiekanalen.
- Monitoring van de toepassing: bij de softwaremodulen van de voorlopige koppeling wordt het communicatiesysteem gemonitord op het niveau van de applicatie (manueel en/of met regelmatige tussenpozen), waarbij de eind-tot-eind-beschikbaarheid van de koppeling wordt getest door een deel van de transacties over de verbinding te simuleren.

4.3. Acceptatie-/testomgevingen

De architectuur van het EU-register en het Zwitserse register bestaat uit de volgende drie omgevingen:

- Productie (PROD): Deze omgeving bevat de daadwerkelijke gegevens en verwerkt daadwerkelijke transacties.
- Acceptatie (ACC): Deze omgeving bevat niet-echte of geanonimiseerde, representatieve gegevens. Het is de omgeving waar systeembeheerders van beide partijen nieuwe releases valideren.
- Test (TEST): Deze omgeving bevat niet-echte of geanonimiseerde, representatieve gegevens. Deze omgeving is beperkt tot registeradministrateurs en is bedoeld voor het uitvoeren van integratietests door beide partijen.

Met uitzondering van het VPN (of een gelijkwaardig netwerk) zijn de drie omgevingen volledig van elkaar onafhankelijk, dat wil zeggen dat hardware, software, databanken, virtuele omgevingen, IP-adressen en poorten onafhankelijk van elkaar worden opgezet en functioneren.

Wat de indeling van het VPN betreft, wordt dit in twee verschillende omgevingen opgezet, een voor PROD en een andere, onafhankelijke voor ACC en van TEST.

5. BEPALINGEN INZAKE VERTROUWELIJKHEID EN INTEGRITEIT

Beveiligingsmechanismen en -procedures voorzien in een taak voor twee personen (4-ogen) voor verrichtingen in de koppeling tussen het EU-register en het Zwitserse register. De tweeledige functie is van toepassing waar dat nodig is, maar is evenwel niet per definitie van toepassing op alle door de registeradministrateurs ondernomen stappen.

De beveiligingseisen worden in overweging genomen en behandeld in het beveiligingsbeheerplan, dat ook processen omvat die verband houden met de behandeling van beveiligingsincidenten als gevolg van een eventuele inbreuk op de beveiliging. Het operationele deel van deze processen wordt beschreven in de GOP.

5.1. Infrastructuur voor beveiligingstests

Elke partij verbindt zich ertoe een beveiligingstestinfrastructuur op te zetten (door gebruik te maken van de gemeenschappelijke reeks van software en hardware die wordt gebruikt bij de opsporing van kwetsbaarheden in de ontwikkelings- en operatiefase):

- die is gescheiden van de productieomgeving;
- waar de beveiliging wordt geanalyseerd door een team dat onafhankelijk is van de ontwikkeling en de werking van het systeem.

Elke partij verbindt zich ertoe zowel statische als dynamische analyses uit te voeren.

In het geval van een dynamische analyse (zoals penetratietests) verbinden beide partijen zich ertoe de beoordelingen te beperken tot de test- en acceptatieomgevingen (zoals gedefinieerd in het hoofdstuk "Acceptatie-/testomgevingen"). Uitzonderingen op dit beleid moeten door beide partijen worden goedgekeurd.

Alvorens in de productieomgeving te worden uitgerold, moet de beveiliging van elke softwaremodule van de koppeling (zoals gedefinieerd in de afdeling "Architectuur van de communicatieverbinding") worden getest.

De testinfrastructuur moet zowel op het niveau van het netwerk als op het niveau van de infrastructuur worden gescheiden van de productie-infrastructuur en moet het mogelijk maken de beveiligingstests uit te voeren die nodig zijn om de naleving van de beveiligingsvereisten te controleren.

5.2. Onderbreking van de koppeling en bepalingen betreffende heractivering

Indien het vermoeden bestaat dat de veiligheid van het Zwitserse register, het SSTL, het EU-register of het EUTL in het gedrang is gekomen, moeten beide partijen elkaar daarvan onverwijld in kennis stellen en de koppeling tussen het SSTL en het EUTL onderbreken.

De procedures voor het delen van informatie, het besluit tot onderbreking en het besluit tot heractivering, maken deel uit van het proces voor de inwilliging van verzoeken van de GOP.

Onderbreking

Onderbreking van de registerkoppeling overeenkomstig bijlage II bij de overeenkomst kan plaatsvinden omwille van:

- administratieve redenen (onderhoud,...) en dus gepland;
- veiligheidsoverwegingen (of storingen in de IT-infrastructuur), en dus niet gepland.

In noodgevallen stelt de ene partij de andere in kennis en onderbreekt zij de registerkoppeling unilateraal.

Indien wordt besloten de registerkoppeling te onderbreken, zorgt elke partij ervoor dat de koppeling op netwerkniveau wordt onderbroken (door onderdelen of alle inkomende en uitgaande verbindingen te blokkeren).

Het besluit tot al dan niet geplande onderbreking van de registerkoppeling wordt genomen volgens de procedure voor wijzigingsbeheer of beveiligingsincidentbeheer van de GOP.

Heractivering van de communicatie

Het besluit tot heractivering zal worden genomen zoals uiteengezet in de GOP en in geen geval voordat de procedures voor het testen van de beveiliging met succes zijn afgerond, zoals beschreven in de hoofdstukken "Richtsnoeren voor veiligheidstests" en "Initialisatie, heractivering, communicatie en testplan".

5.3. Bepalingen inzake beveiligingsinbreuk

Een beveiligingsinbreuk wordt beschouwd als een beveiligingsincident met gevolgen voor de vertrouwelijkheid en integriteit van alle gevoelige informatie en/of de beschikbaarheid van het systeem dat die informatie verwerkt.

Gevoelige informatie wordt in de lijst van gevoelige informatie vermeld en kan in het systeem of in enig daaraan gerelateerd onderdeel worden verwerkt.

Informatie die rechtstreeks verband houdt met de beveiligingsinbreuk wordt als gevoelig beschouwd, met de vermelding "ETS Critical" aangemerkt en behandeld volgens de desbetreffende instructies, tenzij anders is bepaald.

Elke beveiligingsinbreuk wordt behandeld volgens het hoofdstuk betreffende beveiligingsincidentbeheer van de GOP.

5.4. Richtsnoeren voor het testen van de beveiliging

5.4.1. Software

Beveiligingstests, in voorkomend geval met inbegrip van de penetratietests, worden ten minste op alle nieuwe belangrijke softwarereleases uitgevoerd volgens de in de LTS vastgestelde beveiligingseisen om de beveiliging van de verbinding en de daaraan verbonden risico's te beoordelen.

Indien in de afgelopen 12 maanden geen belangrijke release is uitgekomen, wordt een beveiligingstest verricht op het huidige systeem, rekening houdend met de ontwikkelingen in de cyberdreiging die zich in de voorgaande 12 maanden hebben voorgedaan.

De beveiligingstest van de registerkoppeling wordt uitgevoerd in de acceptatieomgeving en, indien vereist, in de productieomgeving en met de coördinatie en wederzijdse overeenstemming van beide partijen.

Bij het testen van webapplicaties worden internationale open normen, zoals die welke zijn ontwikkeld door het Open Web Application Security Project (OWASP), in acht genomen.

5.4.2. Infrastructuur

De infrastructuur ter ondersteuning van het productiesysteem wordt regelmatig (ten minste eens per maand) gecontroleerd op kwetsbaarheden, en vastgestelde kwetsbaarheden worden hersteld volgens hetzelfde beginsel dat in het vorige hoofdstuk is uiteengezet, met gebruikmaking van een actueel register van kwetsbaarheden.

5.5. Bepalingen inzake risicobeoordeling

Indien de penetratietest van toepassing is, moet deze worden opgenomen in de beveiligingstest.

Elke partij kan voor de uitvoering van de beveiligingstests een beroep doen op een gespecialiseerde externe onderneming, mits deze onderneming:

- beschikt over de vaardigheden en ervaring op het gebied van dergelijke beveiligingstests;
- niet rechtstreeks is verbonden aan de ontwikkelaar en/of zijn contractant, noch betrokken bij de ontwikkeling van de software van de verbinding, noch onderaannemer van de ontwikkelaar;
- een geheimhoudingsovereenkomst heeft ondertekend om de resultaten vertrouwelijk te houden en deze te behandelen op het niveau van de "ETS CRITICAL" overeenkomstig de instructies voor behandeling.