EUROOPAN UNIONIN JA SVEITSIN VALALIITON VÄLISELLÄ NIIDEN KASVIHUONEKAASUJEN PÄÄSTÖKAUPPAJÄRJESTELMIEN VÄLISTÄ YHTEYTTÄ KOSKEVALLA SOPIMUKSELLA PERUSTETUN SEKAKOMITEAN PÄÄTÖS N:o 2/2020,

annettu 5 päivänä marraskuuta 2020,

sopimuksen liitteiden I ja II muuttamisesta sekä yhteyttä koskevien teknisten standardien (LTS) hyväksymisestä [2021/1034]

SEKAKOMITEA, joka

ottaa huomioon Euroopan unionin ja Sveitsin valaliiton välisen sopimuksen niiden kasvihuonekaasujen päästökauppajärjestelmien välisestä yhteydestä ([1]), jäljempänä 'sopimus', ja erityisesti sen 3 artiklan 7 kohdan ja 13 artiklan 2 kohdan,

sekä katsoo seuraavaa:

(1) Sekakomitean 5 päivänä joulukuuta 2019 tekemällä päätöksellä N:o 2/2019 ([2]) muutettiin sopimuksen liitteitä I ja II ja täytettiin siten sopimuksessa vahvistetut yhteyden muodostamista koskevat edellytykset.

(2) Sekakomitean päätöksen N:o 2/2019 hyväksymisen jälkeen ja sopimuksen 21 artiklan 3 kohdan nojalla osapuolet vaihtoivat ratifioimis- tai hyväksymiskirjansa, koska ne katsovat kaikkien sopimuksessa vahvistettujen yhteyden muodostamista koskevien edellytysten täyttyvän.

(3) Sopimuksen 21 artiklan 4 kohdan mukaisesti sopimus tuli voimaan 1 päivänä tammikuuta 2020.

(4) Sopimuksen liitettä I olisi muutettava sopimuksen 13 artiklan 2 kohdan mukaisesti, jotta voidaan ottaa huomioon edistyminen rekisteriyhteyden luomisessa ja varmistaa sujuva siirtymä Sveitsille ensimmäistä kertaa osoitettujen ilma-alusten käyttäjien hallinnoinnissa.

(5) Jotta voidaan ottaa huomioon viimeaikainen kehitys ja varmistaa suurempi joustavuus sopimuksen edellyttämän rekisteriyhteyden luomisessa, sopimuksen liitettä II olisi muutettava sopimuksen 13 artiklan 2 kohdan mukaisesti siten, että siinä säädetään laajemmasta mutta vastaavasta valikoimasta teknologioita rekisteriyhteyden luomiseksi.

(6) Sopimuksen 3 artiklan 7 kohdan mukaan Sveitsin rekisterinvalvojan ja unionin keskusvalvojan olisi laadittava yhteyttä koskevat tekniset standardit, jäljempänä 'LTS-standardit', sopimuksen liitteessä II vahvistettujen periaatteiden perusteella. LTS-standardeissa olisi kuvattava yksityiskohtaiset vaatimukset vakaan ja turvallisen yhteyden luomiselle Sveitsin täydentävän tapahtumalokin (SSTL) ja Euroopan unionin tapahtumalokin (EUTL) välille. LTS-standardien olisi tultava voimaan, kun ne hyväksytään sekakomitean päätöksellä.

(7) Sopimuksen 13 artiklan 1 kohdan mukaisesti sekakomitea varmistaa sopimuksen moitteettoman täytäntöönpanon, ja sekakomitean olisi tässä tarkoituksessa annettava tekniset ohjeet, myös SSTL:n ja EUTL:n välisen vakaan ja turvallisen yhteyden luomisen osalta. Tekniset ohjeet voidaan laatia sopimuksen 12 artiklan 5 kohdan mukaisesti perustetussa työryhmässä. Työryhmään olisi kuuluttava ainakin Sveitsin rekisterinvalvoja ja unionin keskusvalvoja, ja sen olisi avustettava sekakomiteaa tehtävissä, joita tällä on sopimuksen 13 artiklan mukaisesti.

(8) Koska ohjeet ovat luonteeltaan teknisiä ja koska niitä on tarpeen mukauttaa meneillään olevaan kehitykseen, Sveitsin rekisterinvalvojan ja unionin keskusvalvojan laatimat tekniset ohjeet olisi toimitettava sekakomitealle tiedoksi tai tarvittaessa hyväksyttäviksi,

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

([2]) Euroopan unionin ja Sveitsin valaliiton välisellä niiden kasvihuonekaasujen päästökauppajärjestelmien välistä yhteyttä koskevalla sopimuksella perustetun sekakomitean päätös N:o 2/2019, annettu 5 päivänä joulukuuta 2019, Euroopan unionin ja Sveitsin valaliiton välisen niiden kasvihuonekaasujen päästökauppajärjestelmien välistä yhteyttä koskevan sopimuksen liitteiden I ja II muuttamisesta (EUVL L 314, 29.9.2020, s. 68).

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Korvataan sopimuksen liitteessä I olevan B osan 17 kohdan toinen alakohta seuraavasti:

”Ilma-alusten käyttäjiä, joiden hallinnointi on osoitettu Sveitsille ensimmäisen kerran tämän sopimuksen tultua voimaan, hallinnoi Sveitsi osoittamisvuoden 30 päivän huhtikuuta jälkeen ja heti, kun väliaikainen rekisteriyhteys on toiminnassa.”

2 artikla

Korvataan sopimuksen liitteessä II oleva neljäs alakohta seuraavasti:

”LTS-standardeissa on määritettävä, että tiedonsiirto SSTL:n ja EUTL:n välillä tapahtuu verkkopalveluviestien suojatun vaihdon muodossa seuraavien (*) tai vastaavien teknologioiden pohjalta:

— SOAP-protokollaa (Simple Object Access Protocol) käyttävät verkkopalvelut

— laitteistoon perustuva virtuaalinen yksityisverkko (VPN)

— XML-merkintäkieli (Extensible Markup Language)

— Digitaalinen allekirjoitus sekä

— NTP-aikaprotokollat (Network Time Protocol).

(*) Näitä teknologioita käytetään tällä hetkellä yhteyden luomiseen unionin rekisterin ja kansainvälisen tapahtumalokin välillä sekä Sveitsin rekisterin ja kansainvälisen tapahtumalokin välillä.”

3 artikla

Hyväksytään tämän päätöksen liitteenä olevat yhteyttä koskevat tekniset standardit (LTS).

4 artikla

Perustetaan työryhmä sopimuksen 12 artiklan 5 kohdan nojalla. Työryhmä avustaa sekakomiteaa sopimuksen moitteettoman täytäntöönpanon varmistamisessa, mukaan lukien teknisten ohjeiden laatiminen LTS-standardien täytäntöönpanoa varten.

Työryhmään kuuluvat ainakin Sveitsin rekisterinvalvoja ja unionin keskusvalvoja.

5 artikla

Tämä päätös tulee voimaan päivänä, jona se hyväksytään.

Tehty Brysselissä 5 päivänä marraskuuta 2020.

Sekakomitean puolesta	Puheenjohtaja	Sihteeri Sveitsin puolesta
Sihteeri Euroopan unionin puolesta	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

LIITE

Euroopan unionin ja Sveitsin valaliiton välisen niiden kasvihuonekaasujen päätökauppajärjestelmien välisestä yhteydestä tehdyn sopimuksen 3 artiklan 7 kohdassa tarkoitetut yhteyttä koskevat tekniset standardit (LTS).

VÄLIAIKAISTA RATKAISUA KOSKEVA STANDARDI

1. **Sanasto**

Taulukko 1-1

Toiminnalliset lyhenteet ja määritelmät

Lyhenne/termi	Määritelmä
Päästöoikeus	Oikeus päästää yksi tonni hiilidioksidiekvivalenttia tietyssä ajanjaksossa. Tämä oikeus on voimassa ainoastaan unionin päästökauppajärjestelmän (unionin ETS) tai Sveitsin päästökauppajärjestelmän (Sveitsin ETS) vaatimusten täyttämiseksi.
CH	Sveitsin valaliitto
CHU	Sveitsin yleiset päästöoikeudet (CHU2 = toisen velvoitekauden CHU-päästöoikeudet)
CHUA	Sveitsin ilmailun päästöoikeus
COP	Yhteiset toiminnalliset menettelyt, jotka sopimuksen osapuolet ovat laatineet yhdessä EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välisen yhteyden toteuttamiseksi.
ETR	Päästökaupparekisteri
ETS	Päästökauppajärjestelmä
EU	Euroopan unioni
EUA	EU:n yleinen päästöoikeus
EUAA	EU:n ilmailun päästöoikeus
EUCR	Euroopan unionin konsolidoitu rekisteri
EUTL	Euroopan unionin tapahtumaloki
Rekisteri	Päästökauppajärjestelmässä myönnettyjen päästöoikeuksien tilinpitojärjestelmä, jonka avulla seurataan sähköisillä tileillä pidettävien päästöoikeuksien omistusta.
SSTL	Sveitsin täydentävä tapahtumaloki
Tapahtuma	Rekisterissä tapahtuva prosessi, joka sisältää päästöoikeuden siirron tililtä toiselle.
Tapahtumalokijärjestelmä	Tapahtumaloki sisältää kirjauksen kustakin ehdotetusta tapahtumasta, joka on lähetetty rekisteristä toiseen.

Taulukko 1-2

Tekniset lyhenteet ja määritelmät

Lyhenne	Määritelmä
Epäsymmetrinen salaus	Käyttää julkisia ja yksityisiä avaimia tietojen salaamiseen ja salauksen purkamiseen.
Varmenneviranomainen (CA)	Taho, joka myöntää digitaalisia varmenteita.

Lyhenne	Määritelmä
Salausavain	Informaatio, joka määrittää salausalgoritmin funktionaalisen tuotoksen.
Salauksen purku	Käänteinen salausprosessi.
Digitaalinen allekirjoitus	Matemaattinen menetelmä, jolla validoidaan viestin, ohjelmiston tai digitaalisen asiakirjan aitous ja eheys.
Salaus	Prosessi, jossa informaatiota tai dataa muunnetaan koodiksi, erityisesti luvattoman käytön estämiseksi.
Tiedoston tulkinta	Tiedoston lukeminen.
Palomuuri	Verkkoturvalaite tai -ohjelmisto, joka seuraa ja valvoo saapuvaa ja lähtevää verkkoliikennettä ennalta määriteltyjen sääntöjen mukaisesti.
Heartbeat-viesti	Laitteen tai ohjelmiston luoma ja seuraama jaksoittainen signaali, joka testaa normaalia toimintaa tai mahdollistaa synkronoinnin tietokonejärjestelmän muiden osien kanssa.
IPSec	IP SECurity. Verkkoprotokollaperhe, joka varmentaa ja salaa datapaketit suojatun salatun tiedonsiirron mahdollistamiseksi kahden tietokoneen välillä internetprotokollaverkon kautta.
Penetraatiotestaus	Menetelmä, jolla testataan tietokonejärjestelmä, verkko tai verkkosovellus sellaisten turvallisuuspuutteiden varalta, joita hyökkääjä voisi hyödyntää.
Täsmäytysprosessi	Prosessi, jolla varmistetaan kahden kirjauksen yhteensopivuus.
VPN	Virtuaalinen yksityisverkko (Virtual Private Network)
XML-kieli	(Extensible Mark-up Language). XML-kielen avulla kehittäjät voivat luoda omia räätälöityjä tunnisteita ja mahdollistaa datan määrittelyn, siirron, validoinnin ja tulkinnan sovellusten ja organisaatioiden välillä.

2. **Johdanto**

Euroopan unionin ja Sveitsin valaliiton välisessä niiden kasvihuonekaasujen päästökauppajärjestelmien välistä yhteyttä koskevassa sopimuksessa, joka on tehty 23 päivänä marraskuuta 2017, jäljempänä ’sopimus’, määrätään sellaisten päästöoikeuksien keskinäisestä tunnustamisesta, joita voidaan käyttää vaatimusten noudattamiseen EU:n päästökauppajärjestelmässä, jäljempänä ’unionin ETS’, tai Sveitsin päästökauppajärjestelmässä, jäljempänä ’Sveitsin ETS’. Jotta unionin ETS:n ja Sveitsin ETS:n välinen yhteys saadaan toimintakykyiseksi, Euroopan unionin tapahtumalokin (EUTL) ja Sveitsin täydentävän tapahtumalokin (SSTL) välille luodaan suora yhteys, joka mahdollistaa kyseisissä päästökauppajärjestelmissä myönnettyjen päästöoikeuksien siirron rekisteristä toiseen (sopimuksen 3 artiklan 2 kohta). Jotta unionin ETS:n ja Sveitsin ETS:n välinen yhteys saadaan toimintakykyiseksi, on otettava käyttöön väliaikainen ratkaisu toukokuuhun 2020 mennessä tai mahdollisimman pian sen jälkeen. Osapuolten on tehtävä yhteistyötä, jotta väliaikainen ratkaisu voidaan korvata pysyvällä rekisteriyhteydellä mahdollisimman pian (sopimuksen liite II).

Sopimuksen 3 artiklan 7 kohdan mukaan Sveitsin rekisterinvalvojan ja unionin keskusvalvojan on laadittava yhteyttä koskevat tekniset standardit (LTS-standardit), jotka perustuvat sopimuksen liitteessä II määrättyihin periaatteisiin ja joissa kuvataan yksityiskohtaiset vaatimukset vakaan ja turvallisen yhteyden luomiselle SSTL:n ja EUTL:n välille. Valvojien laatimat LTS-standardit tulevat voimaan, kun ne on hyväksytty sekakomitean päätöksellä.

Tässä asiakirjassa dokumentoidut LTS-standardit on määrä hyväksyä sekakomitean päätöksellä N:o 2/2020. Tämän päätöksen mukaisesti sekakomitea pyytää Sveitsin rekisterinvalvojaa ja unionin keskusvalvojaa laatimaan tarkemmat tekniset ohjeet, joilla yhteydestä tehdään toimintakykyinen ja varmistetaan, että näitä ohjeita mukautetaan jatkuvasti tekniseen kehitykseen ja uusiin vaatimuksiin yhteyden tietoturvan ja suojauksen alalla sekä tehokkaan ja tarkoituksenmukaisen toiminnan ylläpitämiseksi.

2.1 *Soveltamisala*

Tässä asiakirjassa esitetään sopimuksen osapuolten välinen yhteisymmärrys teknisen perustan luomisesta unionin ETS:n ja Sveitsin ETS:n rekistereiden väliselle yhteydelle. Siinä esitetään teknisten eritelmien perustaso arkkitehtuuri-, palvelu- ja suojausvaatimusten osalta, mutta tarvitaan tarkempia lisäohjeita, jotta yhteydestä tulee toimintakykyinen.

Tässä tarkoituksessa ja yhteyden moitteettoman toiminnan varmistamiseksi on hyväksyttävä yksityiskohtaisempia prosesseja ja menettelytapoja. Sopimuksen 3 artiklan 6 kohdan mukaan nämä seikat täsmennetään yhteisiä toiminnallisia menettelyitä (COP) koskevassa asiakirjassa, joka hyväksytään erikseen sekakomitean päätöksellä.

2.2 *Osoitus*

Tämä asiakirja on osoitettu Sveitsin rekisterinvalvojalle ja unionin keskusvalvojalle.

3. **Yleiset määräykset**

3.1 *Tiedonsiirtoyhteyden arkkitehtuuri*

Tässä jaksossa on tarkoitus kuvata unionin ETS:n ja Sveitsin ETS:n välisen yhteyden ja sen eri osatekijöiden yleisarkkitehtuuri.

Koska tietoturva on keskeinen osa rekisteriyhteyden arkkitehtuurivaatimuksia, arkkitehtuurista on pyritty tekemään kaikin mahdollisin tavoin vakaa ja suojattu. Tuleva pysyvä rekisteriyhteys perustuu verkkopalveluihin, mutta väliaikaisessa ratkaisussa käytetään tiedostojenvaihtomekanismia.

Teknisessä ratkaisussa käytetään seuraavia:

— Suojatun viestinvälityksen siirtoprotokolla.

— XML-viestit.

— XML-pohjainen digitaalinen allekirjoitus ja salaus.

— VPN-laite tai vastaava suojattu tiedonsiirtoverkko.

3.1.1 Viestinvaihto

Unionin rekisterin ja Sveitsin rekisterin välinen tiedonsiirto perustuu suojattujen kanavien kautta tapahtuvaan viestienvaihtomekanismiin. Molemmilla päillä on oma vastaanotettujen viestien tallennuspaikka.

Molemmat osapuolet pitävät kirjaa vastaanotetuista viesteistä käsittelytietoineen.

Virheistä ja odottamattomista poikkeamista ilmoitetaan varoituksilla, minkä jälkeen tukitiimit puuttuvan manuaalisesti toimintaan.

Virheet ja odottamattomat tapahtumat käsitellään noudattaen toiminnallisia menettelyjä, jotka on vahvistettu COP:n häiriönhallintaprosessissa.

3.1.2 XML-viesti – Korkean tason kuvaus

XML-viesti sisältää jonkin seuraavista:

— vähintään yksi tapahtumapyyntö ja/tai vähintään yksi tapahtumavastaus;

— yksitoimenpide/vastaus, joka liittyy täsmäytykseen;

— yksi testiviesti.

Jokainen viesti sisältää otsikon, jossa mainitaan

— alkuperä-ETS;

— sarjanumero.

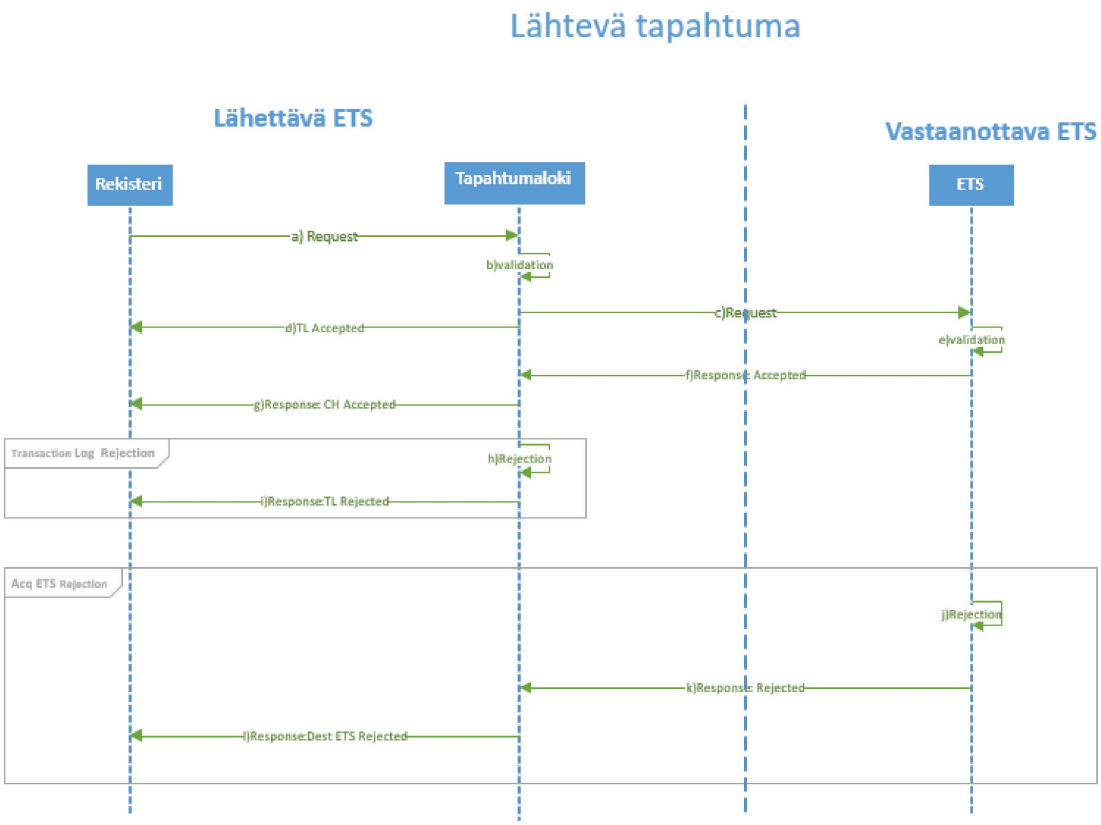
3.1.3 Syöttöikkunat

Väliaikainen ratkaisu perustuu ennalta määritettyihin syöttöikkunoihin, joita seuraa joukko nimettyjä tapahtumia. Yhteyden kautta vastaanotetut tapahtumapyynnöt tulkitaan ennalta määritetyin väliajoin. Lähtevät ja saapuvat tapahtumat validoidaan teknisesti. Täsmäytyksiä voi olla päivittäin, ja ne voidaan käynnistää manuaalisesti.

Muutoksia näiden tapahtumien ajoituksessa ja/tai tiheydessä käsitellään noudattaen toiminnallisia menettelyjä, jotka on vahvistettu COP:n palvelupyyntöprosessissa.

3.1.4 Tapahtumaviestivirrat

Lähtevät tapahtumat



Tässä vaiheet on kuvattu lähettävän ETS:n näkökulmasta. Edellä oleva kaavio kuvaa kaikki yksittäiset lähtevät tapahtumavirrat.

Päävirta ”Normal Transaction” (vaiheineen, jotka esitetään edellä olevassa piirroksessa):

a) Lähettävässä ETS:ssä tapahtumapyyntö lähetetään rekisteristä tapahtumalokiin heti, kun kaikki toiminnalliset viiveet ovat ohi (soveltuvin osin 24 tunnin viive).

b) Tapahtumaloki validoi tapahtumapyynnön.

c) Tapahtumapyyntö lähetetään kohde-ETS:ään.

d) Hyväksymisvastaus lähetetään alkuperä-ETS:n rekisteriin.

e) Kohde-ETS validoi tapahtumapyynnön.

f) Kohde-ETS lähettää hyväksymisvastauksen takaisin alkuperä-ETS:n tapahtumalokiin.

g) Tapahtumaloki lähettää hyväksymisvastauksen rekisteriin.

Vaihtoehtoinen virta ”Transaction Log Rejection” (vaiheineen, jotka esitetään edellä olevassa piirroksessa alkaen kohdasta a):

a) Alkuperä-ETS:ssä tapahtumapyyntö lähetetään rekisteristä tapahtumalokiin heti, kun kaikki toiminnalliset viiveet ovat ohi (soveltuvin osin 24 tunnin viive).

Seuraava vaihe:

b) Tapahtumaloki ei validoi pyyntöä

c) Hylkäämisviesti lähetetään alkuperäiseen rekisteriin.

Vaihtoehtoinen virta ”ETS Rejection” (vaiheineen, jotka esitetään edellä olevassa piirroksessa alkaen kohdasta a):

a) Alkuperä-ETS:ssä tapahtumapyyntö lähetetään rekisteristä tapahtumalokiin heti, kun kaikki toiminnalliset viiveet ovat ohi (soveltuvin osin 24 tunnin viive).

b) Tapahtumaloki validoi tapahtuman.

c) Tapahtumapyyntö lähetetään kohde-ETS:ään.

d) Hyväksymisviesti lähetetään alkuperä-ETS:n rekisteriin.

Seuraava vaihe:

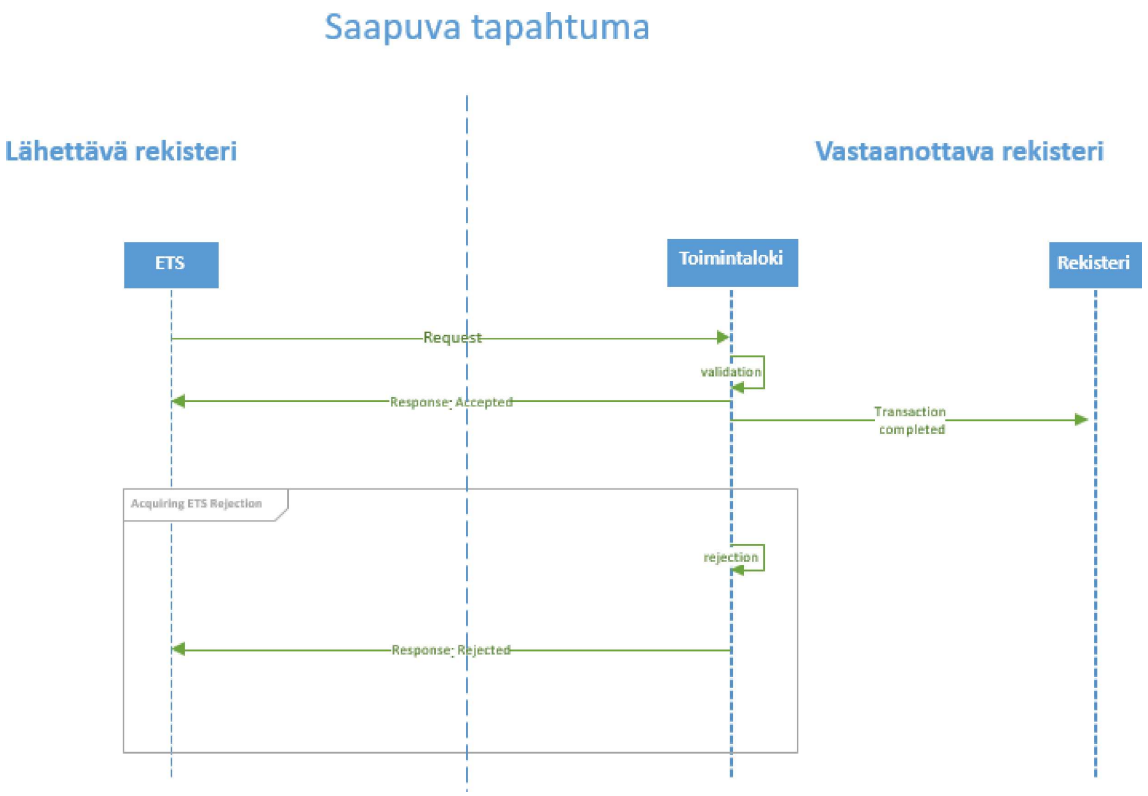
e) Vastaanottavan ETS:n tapahtumaloki ei validoi tapahtumaa.

f) Vastaanottava ETS lähettää hylkäämisvastauksen pyynnön lähettäneen ETS:n tapahtumalokiin.

g) Tapahtumaloki lähettää hylkäämisen rekisteriin.

Saapuvat tapahtumat

Tässä vaiheet on kuvattu vastaanottavan ETS:n näkökulmasta. Viestivirta kuvataan seuraavassa kaaviossa:



Kaavio:

1. Kun vastaanottavan ETS:n tapahtumaloki validoi pyynnön, se lähettää hyväksymisviestin pyynnön lähettäneelle ETS:lle ja viestin ”transaction completed” vastaanottavan ETS:n rekisteriin.

2. Kun saapuva pyyntö hylätään vastaanottavassa tapahtumalokissa, tapahtumapyyntöä ei lähetetä vastaanottavan ETS:n rekisteriin.

Protokolla

Tapahtumaviestisyklissä on vain kaksi viestiä:

— Transferring ETS Acquiring ETS Transaction Proposal.

— Acquiring ETS Transferring ETS Transaction Response: Joko hyväksytty (”Accepted”) tai hylätty (”Rejected”) (mukaan lukien hylkäämisen syy).

  — Accepted: Tapahtuma on toteutettu onnistuneesti.

  — Rejected: Tapahtuma on keskeytetty.

Tapahtumatila

— Lähettävässä ETS:ssä tapahtumatilaksi asetetaan ”proposed”, kun pyyntö lähetetään.

— Vastaanottavassa ETS:ssä tapahtumatilaksi asetetaan ”proposed”, kun pyyntö on vastaanotettu ja kun sitä käsitellään.

— Vastaanottavassa ETS:ssä tapahtumatilaksi asetetaan ”completed”/”terminated”, kun ehdotus on käsitelty. Vastaanottava ETS lähettää tämän jälkeen vastaavan hyväksymis-/hylkäämisviestin.

— Pyynnön lähettäneessä ETS:ssä tapahtumatilaksi asetetaan ”completed”/”terminated”, kun hyväksymis-/hylkäämisviesti on vastaanotettu ja käsitelty.

— Pyynnön lähettäneessä ETS:ssä tapahtumatilana pysyy ”proposed” myös siinä tapauksessa, että vastausta ei saada.

— Vastaanottavassa ETS:ssä tapahtumatilaksi tulee ”terminated”, jos ehdotettu tapahtuma pysyy tilassa ”proposed” yli 30 minuuttia.

Tapahtumiin liittyvät poikkeamat käsitellään noudattaen toiminnallisia menettelyjä, jotka on vahvistettu COP:n häiriönhallintaprosessissa.

3.2 *Tiedonsiirron turvallisuus*

Siirrettäviin tietoihin sovelletaan neljää turvallisuustasoa:

1) Verkkoon pääsyn valvonta: palomuuri ja verkkojen yhteenliityntäkerros.

2) Liikennetason salaus: VPN tai vastaava suojattu tiedonsiirtoverkko.

3) Istuntotason salaus: Suojatun viestinvälityksen siirtoprotokolla.

4) Sovellustason salaus: XML-sisällön salaus ja allekirjoitus.

3.2.1 Palomuuri ja verkkojen yhteenliitäntä

Yhteys luodaan sellaisen verkon kautta, joka on suojattu laitteistopohjaisella palomuurilla. Palomuuri on konfiguroitava sellaisilla säännöillä, että ainoastaan ”rekisteröidyt” asiakkaat voivat luoda yhteyksiä VPN-palvelimeen.

3.2.2 Virtuaalinen yksityisverkko (VPN)

Kaikki osapuolten välinen viestintä on suojattava käyttäen suojattua tiedonsiirtoteknologiaa. VPN:n tapauksessa infrastruktuurin olisi perustuttava laitteistoihin tai virtuaalisiin laitteisiin. VPN-teknologiat tarjoavat mahdollisuuden ”tunneloida” liikenteen internetin kaltaisen verkon läpi yhdestä pisteestä toiseen suojaten samalla kaiken viestinnän. Ennen kuin VPN-tunneli luodaan, mahdolliselle asiakaspäätepisteelle annetaan digitaalinen varmenne, jonka avulla asiakas voi todistaa identiteettinsä yhteysneuvottelun aikana. Kumpikin osapuoli vastaa varmenteen asentamisesta VPN-päätepisteeseensä. Digitaalisten varmenteiden avulla kukin VPN-palvelin saa pääsyn keskusjärjestelmään, jossa selvitetään neuvottelemalla tunnistautumistiedot. Tunnelin luomisen aikana salaus neuvotellaan, millä varmistetaan se, että kaikki tunnelin kautta kulkeva tiedonsiirto on suojattu.

Asiakkaiden VPN-päätepisteet on konfiguroitava siten, että VPN-tunnelia ylläpidetään pysyvästi, jotta luotettava, kahdensuuntainen ja reaaliaikainen tiedonsiirto on mahdollista osapuolten välillä kaikkina aikoina.

Muiden vastaavien ratkaisujen on oltava edellä mainittujen periaatteiden mukaisia.

3.2.3 IPSecin toteutus

Jos valitaan VPN-ratkaisu, erilliset verkot yhdistävä VPN-infrastruktuuri muodostetaan IPSec-protokollalla, mikä mahdollistaa erillisten verkkojen välisen todentamisen, siirretyn datan eheyden ja tietojen salauksen. IPSec-protokollan sisältävillä VPN-konfiguraatioilla varmistetaan asianmukainen todentaminen VPN-yhteyden kahden päätepisteen välillä. Osapuolet tunnistavat ja todentavat etäasiakkaan IPSec-yhteyden kautta käyttäen toisen pään tunnustaman varmenneviranomaisen myöntämiä digitaalisia varmenteita.

IPSec varmistaa myös tietojen eheyden kaikessa viestinnässä, joka kulkee VPN-tunnelin läpi. Datapaketit käsitellään hash-algoritmilla ja allekirjoitetaan käyttäen VPN:n luomia tunnistetietoja. Tietojen luottamuksellisuus varmistetaan vastaavasti mahdollistamalla IPSec-salaus.

3.2.4 Suojatun viestinvälityksen siirtoprotokolla

Väliaikainen ratkaisu perustuu useisiin salauskerroksiin, joiden avulla osapuolet voivat turvallisesti vaihtaa tietoja. Sekä järjestelmät ja niiden tekniset ympäristöt on yhteenliitetty verkkokerroksessa VPN-tunneleiden tai vastaavien suojattujen tiedonsiirtoverkkojen kautta. Sovelluskerroksessa tiedostot siirretään käyttäen suojattua viestiensiirto-protokollaa istuntotasolla.

3.2.5 XML-salaus ja -allekirjoitus

XML-tiedostoissa allekirjoitus ja salaus tapahtuu kahdella tasolla. Jokainen tapahtumapyyntö, tapahtumavastaus ja täsmäytysviesti allekirjoitetaan digitaalisesti erikseen.

Toisessa vaiheessa ”viestin” jokainen osaelementti salataan erikseen.

Lisäksi kolmannessa vaiheessa – ja koko viestin eheyden ja kiistämättömyyden varmistamiseksi – juurielementtiviesti allekirjoitetaan digitaalisesti. Tämän myötä XML-muotoiselle datalle saadaan aikaan korkeatasoinen suoja. Tekninen toteutus noudattaa World Wide Web -konsortion standardeja.

Viestin salauksen purkamiseksi ja viestin todentamiseksi sama prosessi tehdään käänteisessä järjestyksessä.

3.2.6 Salausavaimet

Salauksessa ja allekirjoituksessa käytetään julkisilla salausavaimilla toimivaa salaustekniikkaa.

IPSecin erityistapauksessa käytetään molempien osapuolten luottaman varmenneviranomaisen myöntämää digitaalista varmennetta. Tarkistettuaan varmenteen haltijan identiteetin varmenneviranomainen myöntää varmenteita, joita käytetään organisaation viralliseen tunnistamiseen ja suojattujen tiedonsiirtokanavien luomiseen osapuolten välillä.

Salausavaimia käytetään viestintäkanavien ja datatiedostojen allekirjoittamiseen ja salaamiseen. Julkiset varmenteet vaihdetaan digitaalisessa muodossa osapuolten välillä suojattujen kanavien kautta, ja ne todennetaan myös toisen erillisen viestintäkanavan kautta. Tämä menettely on erottamaton osa COP:n tietoturvan hallintaprosessia.

3.3 *Yhteyteen liittyvien toimintojen luettelo*

Yhteydessä täsmennetään tiedonsiirtojärjestelmä joukolle toimintoja, joilla pannaan täytäntöön sopimuksesta johtuvat toiminnalliset prosessit. Yhteys sisältää myös eritelmän täsmäytysprosessille ja testiviesteille, joilla toteutetaan heartbeat-testaus.

3.3.1 Käyttötapahtumat

Käyttötarkoituksen näkökulmasta katsottuna yhteyteen liittyy neljä (4) erilaista tapahtumapyyntöä:

— Ulkoinen siirto:

  — ETS-yhteyden oikeudellisen voimaantulon jälkeen EU:n ja Sveitsin päästöoikeudet ovat vaihdettavissa ja siten täysin siirrettävissä osapuolten välillä.

— Siirron tekeminen yhteyden kautta edellyttää, että yhdessä ETS:ssä on lähettävä tili ja toisessa ETS:ssä on vastaanottava tili.

— Siirto voi sisältää minkä tahansa määrän neljää (4) erilaista päästöoikeutta:

  — Sveitsin yleiset päästöoikeudet (CHU)

  — Sveitsin ilmailun päästöoikeudet (CHUA)

  — EU:n yleiset päästöoikeudet (EUA)

  — EU:n ilmailun päästöoikeudet (EUAA)

— Kansainvälinen jako:

  Yhdessä ETS:ssä hallinnoidut ilma-alusten käyttäjät, joilla on velvoitteita toisessa ETS:ssä ja oikeus saada maksutta päästöoikeuksia tästä toisesta ETS:stä, saavat maksutta ilmailun päästöoikeuksia toisesta ETS:stä kansainvälistä jakoa koskevan tapahtuman kautta.

— Kansainvälisen jaon peruuttaminen

  Tämä tapahtuma toteutetaan silloin, kun päästöoikeudet, jotka toinen ETS on jakanut ilma-aluksen käyttäjän päästöoikeustilille maksutta, on peruutettava kokonaisuudessaan.

— Liiallisen jaon palauttaminen:

  Tämä tapahtuma on samankaltainen kuin peruuttaminen, mutta jaettuja päästöoikeuksia ei tarvitse peruuttaa kokonaisuudessaan, vaan ainoastaan liiallisesti jaetut päästöoikeudet palautetaan ne jakaneelle ETS:lle.

3.3.2 Täsmäytysprotokolla

Täsmäytykset tehdään vasta sen jälkeen, kun viestien tulkinnan, validoinnin ja käsittelyn aikaikkunat ovat sulkeutuneet.

Täsmäytykset ovat erottamaton osa yhteyden turvallisuus- ja johdonmukaisuusvalvontaa. Molemmat osapuolet sopivat täsmäytyksen tarkasta ajoituksesta ennen aikataulutuksen luomista. Päivittäinen ajastettu täsmäytys on mahdollinen, jos osapuolet ovat sopineet siitä. Vähintään yksi ajastettu täsmäytys on toteutettava kunkin tulkinnan jälkeen.

Kumpi tahansa osapuoli voi milloin tahansa aloittaa manuaalisen täsmäytyksen.

Muutokset ajastetun täsmäytyksen ajoitukseen ja tiheyteen on tehtävä noudattaen toiminnallisia menettelyjä, jotka vahvistetaan COP:n palvelupyyntöprosessissa.

3.3.3 Testiviesti

Testiviestillä testataan päästä päähän -viestintää. Viesti sisältää dataa, joka osoittaa viestin testiksi, ja viestiin vastataan, kun se on vastaanotettu toisessa päässä.

3.4 *Verkkopalveluja koskevat standardit*

Väliaikaisessa ratkaisussa ei käytetä verkkopalveluja. On kuitenkin huomattava, että XML-viestien muoto ja formaatti tulee pysymään suurelta osin muuttumattomina. Kun tulevaisuudessa otetaan käyttöön pysyvä rekisteriyhteys, verkkopalvelujen pitäisi mahdollistaa XML-viestien reaaliaikainen vaihto.

3.5 *Verkkopalvelukohtaiset määrittelyt*

Tätä kohtaa ei sovelleta väliaikaiseen ratkaisuun. Kuten edellisessä jaksossa mainitaan, verkkopalveluja käytetään vain tulevassa pysyvässä rekisteriyhteydessä.

3.6 *Tietojen kirjaamista koskevat vaatimukset*

Jotta voidaan tukea molempien osapuolten tarvetta pitää yllä tarkkoja ja johdonmukaisia tietoja sekä tarjota välineitä käytettäviksi täsmäytysprosessissa epäjohdonmukaisuuksien ratkaisemiseksi, molempien osapuolten on ylläpidettävä neljää (4) erityyppistä tietolokia:

— Tapahtumalokit;

— Täsmäytyslokit;

— Viestiarkisto;

— Sisäisen tarkastuksen lokit.

Kaikki näissä lokitiedoissa olevat tiedot on säilytettävä vähintään kolmen (3) kuukauden ajan ongelmanratkaisua varten, ja niiden pidempi säilyttäminen riippuu kummassakin päässä tarkastustarkoituksiin sovellettavasta lainsäädännöstä. Lokitiedostot, jotka ovat vanhempia kuin kolme (3) kuukautta, voidaan arkistoida suojattuun paikkaan riippumattomassa IT-järjestelmässä sillä edellytyksellä, että ne ovat palautettavissa tai luettavissa kohtuullisessa ajassa.

Tapahtumalokit

Tapahtumalokit toteutetaan EUTL:n ja SSTL:n osajärjestelmissä.

Ne pitävät kirjaa kustakin toiselle ETS:lle lähetetystä ehdotetusta tapahtumasta. Kukin kirjaus sisältää kaikki tapahtumasisällön kentät ja tapahtuman myöhemmän tuloksen (vastaanottavan ETS:n vastauksen). Tapahtumalokit pitävät kirjaa myös saapuvista tapahtumista sekä vastauksista, jotka on lähetetty niiden alkuperä-ETS:lle.

Täsmäytyslokit

Täsmäytysloki sisältää kirjauksen jokaisesta osapuolten välillä vaihdetusta täsmäytysviestistä, mukaan lukien täsmäytystunnus, aikaleima ja täsmäytyksen tulos: Täsmäytystila on ”Pass” tai ”Discrepancies”. Väliaikaisessa ratkaisussa täsmäytysviestit ovat erottamaton osa vaihdettuja viestejä.

Molemmat osapuolet kirjaavat kunkin pyynnön ja sen vastauksen täsmäytyslokiin. Vaikka täsmäytyslokin tietoja ei jaeta suoraan osana itse täsmäytystä, pääsy näihin tietoihin voi olla tarpeen epäjohdonmukaisuuksien ratkaisemiseksi.

Viestiarkisto

Molempien osapuolten on arkistoitava kopio vaihdetuista tiedoista (XML-tiedostot), niin lähetetyistä kuin vastaanotetuistakin, ja siitä, olivatko ne tai XML-viestit muodoltaan oikeanlaisia.

Arkiston päätarkoitus on mahdollistaa jälkitarkastukset ja ylläpitää todisteita siitä, mitä on lähetetty toiselle osapuolelle ja mitä on vastaanotettu toiselta osapuolelta. Näin ollen tiedostojen ohella myös niihin liittyvät varmenteet on arkistoitava.

Näistä tiedostoista saadaan myös lisätietoja ongelmanratkaisua varten.

Sisäisen tarkastuksen loki

Näiden lokien määrittelystä ja käytöstä vastaa kumpikin osapuoli itse.

3.7 *Toiminnalliset vaatimukset*

Tietojenvaihto näiden kahden järjestelmän välillä ei väliaikaisessa ratkaisussa ole täysin automatisoitua, joten yhteys edellyttää manuaalisia toimenpiteitä ja menettelyjä.

4. **Saatavuutta koskevat määräykset**

4.1 *Tiedonsiirron saatavuuden suunnittelu*

Väliaikaisen ratkaisun arkkitehtuuri koostuu pohjimmiltaan tieto- ja viestintäteknisestä infrastruktuurista ja ohjelmistosta, joka mahdollistaa tiedonsiirron Sveitsin ETS:n ja unionin ETS:n välillä. Tämän tietovirran korkeatasoisen saatavuuden, eheyden ja luottamuksellisuuden takaaminen on siten keskeinen näkökohta, joka on otettava huomioon väliaikaisen ratkaisun ja pysyvän rekisteriyhteyden suunnittelussa. Tässä hankkeessa tieto- ja viestintätekninen infrastruktuuri, räätälöity ohjelmisto ja prosessit ovat olennaisen tärkeitä, joten kaikki nämä kolme osatekijää on otettava huomioon vakaan järjestelmän aikaansaamiseksi.

Tieto- ja viestintäteknisen infrastruktuurin vakaus

Tämän asiakirjan yleisiä määräyksiä koskevassa luvussa täsmennetään arkkitehtuurin rakenneosat. Tieto- ja viestintäteknisen infrastruktuurin puolella väliaikaisessa yhteydessä otetaan käyttöön vakaa VPN-verkko (tai vastaava), joka luo suojatun viestinvaihdon mahdollistavia tietoturvallisia viestintätunneleita. Muut infrastruktuurin osat on konfiguroitu korkean saatavuuden ja/tai varamekanismien pohjalta.

Räätälöidyn ohjelmiston vakaus

Räätälöidyt ohjelmistomoduulit lisäävät vakautta yrittämällä tietyn ajan muodostaa yhteytä uudelleen toisen pään kanssa, jos tämä jostakin syystä ei ole saatavilla.

Palvelun vakaus

Väliaikaisessa ratkaisussa tietoja vaihdetaan osapuolten välillä ennalta määrättyinä ajankohtina kautta vuoden. Jotkin ajastetun tietojenvaihdon vaiheista edellyttävät manuaalisia toimenpiteitä järjestelmän ylläpitäjiltä ja/tai rekisterienvalvojilta. Jotta voidaan ottaa huomioon tämä näkökohta sekä parantaa tiedonvaihtomahdollisuuden saatavuutta ja onnistumisastetta,

— toiminnallisissa menettelysäännöissä annetaan huomattavan suuret aika-ikkunat kunkin vaiheen suorittamista varten;

— väliaikaisen ratkaisun ohjelmistomoduuleissa käytetään asynkronista tiedonsiirtoa;

— automaattinen täsmäytysprosessi havaitsee, jos tiedostojen tulkinnassa on ongelmia jommassakummassa päässä;

— seurantaprosessit (tieto- ja viestintäteknisissä infrastruktuurissa ja räätälöidyissä ohjelmistomoduuleissa) otetaan huomioon häiriönhallintamenettelyissä, ja ne käynnistävät tiettyjä menettelyitä (jotka on määritelty COP-asiakirjassa). Menettelyt, joilla pyritään vähentämään aikaa, joka kuluu normaalin toiminnan palauttamiseen häiriöiden jälkeen, ovat keskeisiä korkean käytettävyyden kannalta.

4.2 *Käynnistys-, tiedonsiirto-, uudelleenaktivointi- ja testaussuunnitelma*

Kaikkien väliaikaisen ratkaisun arkkitehtuuriin liittyvien osatekijöiden on läpäistävä sarja osatekijäkohtaisia ja yhteisiä testejä sen varmistamiseksi, että alusta on valmis tieto- ja viestintätekniikan infrastruktuurin ja tietojärjestelmien tasolla. Nämä toiminnalliset testit ovat pakollinen ennakkoedellytys aina, kun alusta siirtää väliaikaisen ratkaisun keskeytetystä tilasta toiminnalliseen tilaan.

Yhteyden toiminnallisen tilan aktivointi edellyttää, että ennalta määritelty testaussuunnitelma toteutetaan onnistuneesti. Näin varmistetaan, että kukin rekisteri on ensin suorittanut joukon sisäisiä testejä ja sen jälkeen validoinut päästä päähän -liitettävyyden ennen kuin tapahtumien toteuttaminen aloitetaan osapuolten välillä.

Testisuunnitelmassa olisi mainittava yleinen testausstrategia ja yksityiskohtaiset tiedot testausinfrastruktuurista. Siinä olisi mainittava kunkin testilohkon kunkin elementin osalta erityisesti seuraavat tiedot:

— Testauskriteerit ja -välineet;

— Testin suorittamiseen osoitetut roolit;

— Odotetut tulokset (positiiviset ja negatiiviset);

— Testiaikataulu;

— Testituloksia koskevien vaatimusten kirjaaminen;

— Ongelmanratkaisudokumentaatio;

— Eskalointiperiaatteet.

Toimintatilan aktivointitestit voitaisiin prosessina jakaa neljään (4) käsitteelliseen lohkoon tai vaiheeseen:

4.2.1 Sisäisen tieto- ja viestintätekniikan infrastruktuurin testit

Kumpikin osapuoli suorittaa ja/tai tarkistaa nämä testit itsenäisesti.

Kukin tieto- ja viestintätekniikan infrastruktuurin osatekijä kummassakin päässä testataan erikseen. Tämä koskee infrastruktuurin jokaista komponenttia. Testit voidaan suorittaa automatisoidusti tai manuaalisesti, mutta niissä on aina tarkistettava, että infrastruktuurin kukin osatekijä on toimintakykyinen.

4.2.2 Tiedonsiirtotestit

Kumpikin osapuoli aloittaa nämä testit itsenäisesti, mutta testien saattaminen päätökseen edellyttää yhteistyötä toisen pään kanssa.

Kun yksittäiset elementit ovat toimintakykyisiä, testataan rekisterien väliset tiedonsiirtokanavat. Tätä varten kumpikin osapuoli tarkistaa, että internetyhteys toimii, VPN-tunnelit (tai vastaavat suojatut liikennekerroksen verkkoyhteydet) on luotu ja erilliset verkot yhdistävä IP-yhteys toimii. Infrastruktuurin paikallisten ja etäelementtien saavutettavuus ja IP-yhteys olisi tämän jälkeen vahvistettava toiselle osapuolelle.

4.2.3 Täyden järjestelmän testit (päästä päähän -testit)

Nämä testit on tarkoitus suorittaa kummassakin päässä, ja tulokset toimitetaan toiselle osapuolelle.

Heti kun tiedonsiirtokanavat ja kummankin rekisterin kukin yksittäinen komponentti on testattu, kumpikin pää valmistelee sarjan simuloituja tapahtumia ja täsmäytyksen, jotka edustavat kaikkia yhteyden puitteissa toteutettavia toimintoja.

4.2.4 Tietoturvatestit

Molemmat osapuolet suorittavat ja/tai käynnistävät nämä testit kummassakin päässä osiossa 5.4 ”Tietoturvatestausta koskevat ohjeet” ja osiossa 5.5 ”Riskinarviointia koskevat määräykset” täsmennetyillä tavoilla.

Vasta sen jälkeen, kun kukin neljästä vaiheesta/lohkosta on toteutettu ennakkoon oletetuin tuloksin, väliaikaisen yhteyden voidaan katsoa olevan toimintakykyinen.

Testausresurssit

Kummallakin osapuolella on oltava erityiset testausresurssit (tieto- ja viestintäteknisen infrastruktuurin ohjelmistot ja laitteistot), ja niiden on kehitettävä testaustoimintoja järjestelmiään varten, jotta voidaan tukea alustan manuaalista ja jatkuvaa validointia. Rekisterinvalvojat voivat toteuttaa manuaalisia testausmenettelyjä yksittäin tai yhteistyössä milloin tahansa. Toiminnallisen tilan aktivointi on jo itsessään manuaalinen prosessi.

Lisäksi alustan odotetaan suorittavan automatisoituja tarkistuksia säännöllisin väliajoin. Tarkistuksilla pyritään lisäämään alustan saatavuutta havaitsemalla ajoissa mahdollisia infrastruktuuri- tai ohjelmisto-ongelmia. Tämä alustanseurantasuunnitelma koostuu seuraavista kahdesta osatekijästä:

— Tieto- ja viestintäteknisten infrastruktuurien seuranta: molemmissa päissä infrastruktuurin seurannasta huolehtivat tieto- ja viestintäteknisen infrastruktuurin palveluntarjoajat; automatisoidut testit kattavat eri infrastruktuuriosatekijät sekä tiedonsiirtokanavien saatavuuden.

— Sovellusten seuranta: väliaikaisen yhteyden ohjelmistomoduulit toteuttavat järjestelmän tiedonsiirtoseurannan sovellustasolla (manuaalisesti ja/tai säännöllisin väliajoin), mikä mahdollistaa yhteyden saatavuuden testaamisen päästä päähän simuloimalla tiettyjä tapahtumia yhteyden kautta.

4.3 *Hyväksyntä-/testausympäristöt*

Unionin rekisterin ja Sveitsin rekisterin arkkitehtuuri koostuu seuraavista kolmesta ympäristöstä:

— Tuotanto (PROD): Tämä ympäristö sisältää aitoja tietoja ja käsittelee aitoja tapahtumia.

— Hyväksyntä (ACC): Tämä ympäristö sisältää edustavia tietoja, jotka ovat epäaitoja tai anonymisoituja. Kyseessä on ympäristö, jossa molempien osapuolten järjestelmän ylläpitäjät validoivat uusia järjestelmä- ja ohjelmisto-versioita.

— Testaus (TEST): Tämä ympäristö sisältää edustavia tietoja, jotka ovat epäaitoja tai anonymisoituja. Tämä ympäristö on rajattu ainoastaan rekisterinvalvojille, ja se on tarkoitettu käytettäväksi molempien osapuolten toteuttamissa integraatiotesteissä.

Lukuun ottamatta VPN:ää (tai vastaavaa verkkoa) nämä kolme ympäristöä ovat täysin toisistaan riippumattomia, mikä tarkoittaa sitä, että laitteistot, ohjelmistot, tietokannat, virtuaaliympäristöt, IP-osoitteet ja portit on määritelty toisistaan erillisiksi ja toimivat toisistaan riippumattomasti.

VPN-kokoonpano määritellään kahdelle eri ympäristölle: yksi PROD-ympäristölle ja toinen edellisestä riippumaton ACC- ja TEST-ympäristöille.

5. **Luottamuksellisuutta ja eheyttä koskevat määräykset**

Turvallisuusjärjestelyissä ja -menettelyissä sovelletaan kahden henkilön roolin mallia (kahden silmäparin periaatetta) operaatioissa, jotka toteutetaan unionin rekisterin ja Sveitsin rekisterin välisellä yhteydellä. Kahden silmäparin periaatetta sovelletaan aina tarvittaessa. Sitä ei kuitenkaan välttämättä voida soveltaa kaikkiin rekisterinvalvojien toteuttamiin vaiheisiin.

Tietoturvavaatimuksia tarkastellaan ja kuvaillaan tietoturvan hallintasuunnitelmassa, johon sisältyy myös prosesseja, jotka liittyvät tietoturvapoikkeamien käsittelyyn mahdollisten tietoturvaloukkausten seurauksena. Näiden prosessien operatiivista osaa kuvataan COP:ssä.

5.1 *Tietoturvan testausinfrastruktuuri*

Kumpikin osapuoli sitoutuu ottamaan käyttöön tietoturvan testausinfrastruktuurin (käyttämällä haavoittuvuuksien havaitsemiseen kehitys- ja käyttövaiheissa käytettyjä yhteisiä ohjelmistoja ja laitteistoja),

— joka on erillinen tuotantoympäristöstä;

— jossa tietoturvan analysoinnista vastaa ryhmä, joka on riippumaton järjestelmän kehittämisestä ja käytöstä.

Kumpikin osapuoli sitoutuu tekemään sekä staattisia että dynaamisia analyysejä.

Dynaamisten analyysien (kuten penetraatiotestauksen) tapauksessa molemmat osapuolet sitoutuvat rajoittamaan arvioinnit koskemaan pääsääntöisesti hyväksyntä- ja testausympäristöjä (jotka on määritetty osiossa 4.3 ”Hyväksyntä-/Testausympäristöt”). Tähän periaatteeseen voidaan tehdä poikkeuksia molempien osapuolten suostumuksella.

Yhteyden kukin ohjelmistomoduuli (ks. osio 3.1 ”Tiedonsiirtoyhteyden arkkitehtuuri”) on testattava tietoturvan osalta ennen käyttöönottoa tuotantoympäristössä.

Testausinfrastruktuuri on erotettava sekä verkko- että infrastruktuurikerroksessa tuotantoympäristöstä. Siinä on voitava suorittaa tietoturvatestit, joita vaaditaan tietoturvavaatimusten noudattamisen tarkistamiseksi.

5.2 *Yhteyden keskeyttämistä ja uudelleenaktivointia koskevat määräykset*

Jos on syytä epäillä, että Sveitsin rekisterin, SSTL:n, unionin rekisterin tai EUTL:n tietoturva on vaarantunut, kyseessä olevan osapuolen on välittömästi ilmoitettava asiasta toiselle osapuolelle ja keskeytettävä SSTL:n ja EUTL:n välinen yhteys.

Tietojenvaihtoa, keskeyttämispäätöstä ja uudelleenaktivointipäätöstä koskevat menettelyt ovat osa COP:n palvelupyyntöprosessia.

Keskeyttämiset

Rekisteriyhteys voidaan keskeyttää sopimuksen liitteen II mukaisesti seuraavista syistä:

— Hallinnolliset syyt (ylläpito jne.) eli suunnitellut syyt;

— Turvallisuussyyt (tai tietoteknisen infrastruktuurin häiriöt) eli suunnittelemattomat syyt.

Hätätilanteessa osapuoli ilmoittaa asiasta toiselle osapuolelle ja keskeyttää rekisteriyhteyden yksipuolisesti.

Jos rekisteriyhteys päätetään keskeyttää, molemmat osapuolet varmistavat, että yhteys katkaistaan verkkokerroksessa (estämällä kaikki saapuvat ja lähtevät yhteydet tai osan niistä).

Päätös rekisteriyhteyden keskeyttämisestä, niin suunnitellusta kuin suunnittelemattomastakin, tehdään COP:n muutoksenhallintamenettelyn tai tietoturvahäiriöiden hallintamenettelyn mukaisesti.

Viestinnän uudelleenaktivointi

Päätös rekisteriyhteyden uudelleenaktivoinnista tehdään COP:ssä täsmennetyn mukaisesti, ei kuitenkaan ennen kuin tietoturvatestausta koskevat menettelyt, jotka täsmennetään osiossa 5.4 ”Tietoturvatestausta koskevat ohjeet” ja osiossa 4.2 ”Käynnistys-, tiedonsiirto-, uudelleenaktivointi- ja testaussuunnitelma”, on toteutettu onnistuneesti.

5.3 *Tietoturvaloukkauksia koskevat määräykset*

Tietoturvaloukkaukseksi katsotaan tietoturvapoikkeama, joka vaikuttaa arkaluonteisten tietojen luottamuksellisuuteen ja koskemattomuuteen ja/tai niitä käsittelevän järjestelmän saatavuuteen.

Arkaluonteiset tiedot määritellään arkaluonteisten tietojen luettelossa, ja niitä saatetaan käsitellä järjestelmässä tai missä tahansa siihen liittyvässä järjestelmän osassa.

Tietoturvaloukkaukseen suoraan liittyviä tietoja pidetään arkaluonteisina, ne merkitään kuuluvaksi ”ETS CRITICAL” -tasolle ja niitä käsitellään käsittelyohjeiden mukaisesti, ellei toisin mainita.

Jokaista tietoturvaloukkausta käsitellään COP:n tietoturvapoikkeamien hallintaa koskevan luvun mukaisesti.

5.4 *Tietoturvatestausta koskevat ohjeet*

5.4.1 Ohjelmisto

Tietoturvatestaus, mukaan lukien tarvittaessa penetraatiotestaus, on suoritettava vähintään ohjelmiston kaikille merkittäville uusille versioille LTS-standardeissa säädettyjen tietoturvavaatimusten mukaisesti, jotta voidaan arvioida yhteyden turvallisuutta ja asiaan liittyviä riskejä.

Jos merkittävää versiota ei ole tuotettu viimeksi kuluneiden 12 kuukauden aikana, tietoturvatestaus on suoritettava nykyiselle järjestelmälle siten, että otetaan huomioon kyberuhkien kehitys viimeksi kuluneiden 12 kuukauden aikana.

Rekisteriyhteyden turvallisuustestaus on suoritettava hyväksyntäympäristössä ja tarvittaessa tuotantoympäristössä koordinoidusti ja molempien osapuolten keskinäisellä sopimuksella.

Verkkosovellusten testauksessa noudatetaan kansainvälisiä avoimia standardeja, kuten niitä, jotka on kehitetty OWASP-hankkeessa (Open Web Application Security Project).

5.4.2 Infrastruktuuri

Tuotantojärjestelmää tukeva infrastruktuuri on skannattava säännöllisesti (vähintään kerran kuukaudessa) haavoittuvuuksien varalta ja havaitut haavoittuvuudet on korjattava. Testi suoritetaan samalla periaatteella, joka määritellään osiossa 5.4.1, käyttäen ajantasaista haavoittuvuustietokantaa.

5.5 *Riskinarviointia koskevat määräykset*

Jos penetraatiotestausta käytetään, se on sisällytettävä osaksi tietoturvatestausta.

Osapuoli voi tehdä testauksesta sopimuksen tietoturvatestaukseen erikoistuneen yrityksen kanssa edellyttäen, että

— kyseisellä yrityksellä on osaamista ja kokemusta tällaisesta tietoturvatestauksesta;

— kyseinen yritys ei toimi suoraan kehittäjän ja/tai tämän toimeksisaajan alaisuudessa, ei osallistu yhteyden ohjelmiston kehittämiseen eikä ole kehittäjän alihankkija;

— kyseinen yritys on allekirjoittanut salassapitosopimuksen, jossa se sitoutuu pitämään tulokset luottamuksellisina ja käsittelemään niitä tasolla ”ETS CRITICAL” käsittelyohjeiden mukaisesti.