EUROOPAN
KOMISSIO

Bryssel 20.3.2024
COM(2024) 125 final

ANNEX

LIITE

ehdotukseen

Neuvoston päätökseksi

Euroopan unionin ja Sveitsin valaliiton välisellä niiden kasvihuonekaasujen päästökauppajärjestelmien välisestä yhteydestä tehdyllä sopimuksella perustetussa sekakomiteassa Euroopan unionin puolesta otettavasta kannasta sopimuksen liitteen II, yhteisten toiminnallisten menettelyjen ja yhteyttä koskevien teknisten standardien muuttamiseen

EUROOPAN UNIONIN JA SVEITSIN VALALIITON VÄLISELLÄ NIIDEN KASVIHUONEKAASUJEN PÄÄSTÖKAUPPAJÄRJESTELMIEN VÄLISTÄ YHTEYTTÄ KOSKEVALLA SOPIMUKSELLA PERUSTETUN SEKAKOMITEAN PÄÄTÖS N:O 1/2024,
annettu... päivänä...kuuta...
sopimuksen liitteen II, yhteisten toiminnallisten menettelyjen ja yhteyttä koskevien teknisten standardien muuttamisesta

SEKAKOMITEA, joka

ottaa huomioon Euroopan unionin ja Sveitsin valaliiton välisen sopimuksen niiden kasvihuonekaasujen päästökauppajärjestelmien välisestä yhteydestä[1], jäljempänä ’sopimus’, ja erityisesti sen 9 artiklan ja 13 artiklan 2 kohdan,

sekä katsoo seuraavaa:

(1) Sekakomitean päätöksessä N:o 2/2019[2] säädettiin väliaikaisesta ratkaisusta siihen, miten EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välinen yhteys saatetaan toiminnalliseksi.

(2) Kolmannessa kokouksessaan sekakomitea katsoi, että on tarpeen analysoida unionin rekisterin ja Sveitsin rekisterin välisen pysyvän yhteyden kustannustehokkuutta.

(3) Sekakomitea hyväksyi viidennessä kokouksessaan sekakomitean päätöksillä 1/2020[3] ja 2/2020[4] perustetun työryhmän toimittaman raportin, jossa työryhmä analysoi ja suositteli lähestymistapaa unionin rekisterin ja Sveitsin rekisterin välisen pysyvän yhteyden toteuttamiseksi.

(4) Jotta voidaan ottaa huomioon unionin rekisterin ja Sveitsin rekisterin välistä pysyvää yhteyttä koskevat tekniset vaatimukset sekä virtaviivaistaa sopimuksen liitteen II määräyksiä teknologian kehityksen perusteella, olisi muutettava sopimuksen liitettä II.

(5) Jotta voidaan varmistaa yhteisten toiminnallisten menettelyjen ja yhteyttä koskevien teknisten standardien yhdenmukaisuus sopimuksen liitteen II kanssa, myös näitä asiakirjoja olisi muutettava,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

1. Korvataan sopimuksen liite II tämän päätöksen liitteessä I olevalla tekstillä.

2. Sopimuksen 3 artiklan 6 kohdassa tarkoitetut yhteiset toiminnalliset menettelyt esitetään tämän päätöksen liitteessä II.

3. Sopimuksen 3 artiklan 7 kohdassa tarkoitetut yhteyttä koskevat tekniset standardit esitetään tämän päätöksen liitteessä III.

2 artikla

Tämä päätös tulee voimaan päivänä, jona se hyväksytään.

---

1 EUVL L 322, 7.12.2017, s. 3.
2 EUVL L 314, 29.9.2020, s. 68.
3 EUVL L 226, 25.6.2021, s. 2
4 EUVL L 226, 25.6.2021, s. 16.

Tehty englannin kielellä [Brysselissä][Bernissä] [xx 2024].

Sekakomitean puolesta

Sihteeri Euroopan unionin puolesta	*Puheenjohtaja*	*Sihteeri Sveitsin puolesta*

LIITE I

”LIITE II

YHTEYTTÄ KOSKEVAT TEKNISET STANDARDIT

EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välisen yhteyden toteuttamiseksi otettiin käyttöön väliaikainen ratkaisu vuonna 2020. Vuodesta 2023 alkaen näiden kahden päästökauppajärjestelmän välinen rekisteriyhteys on vähitellen kehittynyt pysyväksi rekisteriyhteydeksi, joka on tarkoitus panna täytäntöön viimeistään vuonna 2024 ja joka mahdollistaa toisiinsa yhteydessä olevien markkinoiden toiminnan markkinoiden likviditeetistä saatavien hyötyjen ja kahden toisiinsa liitetyn järjestelmän välisten tapahtumien toteuttamisen osalta tavalla, joka vastaa kahdesta järjestelmästä koostuvia yksittäisiä markkinoita ja antaa markkinaosapuolille mahdollisuuden toimia ikään kuin yksillä markkinoilla, jollei osapuolten erillisistä säännöksistä muuta johdu. Yhteyttä koskevissa teknisissä standardeissa (LTS) on määritettävä

– tiedonsiirtoyhteyden arkkitehtuuri

– Sveitsin rekisterin täydentävän tapahtumalokin (SSTL) ja Euroopan unionin tapahtumalokin (EUTL) välinen viestintä

– tiedonsiirron turvallisuus

– luettelo toiminnoista (tapahtumat, täsmäytys…)

– kuljetuskerroksen määritelmä

– tietojen kirjausta koskevat vaatimukset

– operatiiviset järjestelyt (neuvontapalvelu, tuki)

– tiedonsiirron käyttöönottosuunnitelma ja testausmenettely

– turvallisuuden testausmenettely.

LTS-standardeissa on määritettävä, että valvojien on toteutettava kohtuulliset toimet sen varmistamiseksi, että SSTL, EUTL ja niiden välinen yhteys ovat toiminnassa 24 tuntia päivässä ja 7 päivää viikossa ja että SSTL:n ja EUTL:n toiminnan ja niiden välisen yhteyden toimintahäiriöt on pidettävä mahdollisimman vähäisinä.

LTS-standardeissa on asetettava turvallisuutta koskevia lisävaatimuksia Sveitsin rekisterille, SSTL:lle, unionin rekisterille ja EUTL:lle, ja nämä on dokumentoitava turvallisuuden hallintasuunnitelmaan. Erityisesti LTS-standardeissa on määritettävä seuraavaa:

– jos on syytä epäillä, että Sveitsin rekisterin, SSTL:n, unionin rekisterin tai EUTL:n tietoturva on vaarantunut, molempien osapuolten on välittömästi ilmoitettava asiasta toisilleen ja keskeytettävä SSTL:n ja EUTL:n välinen yhteys

– tietoturvaloukkauksen tapahtuessa osapuolten on sitouduttava jakamaan välittömästi tiedot keskenään. Siinä määrin kuin tekniset tiedot ovat käytettävissä, häiriötä kuvaava raportti (päiväys, syy, vaikutus, korjaustoimet) lähetetään Sveitsin rekisterinvalvojan ja unionin

keskusvalvojan välillä 24 tunnin kuluessa siitä, kun turvallisuushäiriö tunnistetaan tietoturvaloukkaukseksi.

LTS-standardeissa säädetty tietoturvan testausmenettely on saatettava päätökseen ennen kuin SSTL:n ja EUTL:n välinen tiedonsiirtoyhteys luodaan ja aina, kun tarvitaan SSTL:n tai EUTL:n uusi versio.

LTS-standardeissa säädetään kahdesta testausympäristöstä tuotantoympäristön lisäksi: kehityksen testausympäristöstä ja hyväksymisympäristöstä.

Osapuolten on Sveitsin rekisterinvalvojan ja unionin keskusvalvojan kautta osoitettava, että niiden järjestelmistä on suoritettu riippumaton tietoturva-arviointi edeltävän kahdentoista kuukauden aikana LTS-standardeissa säädettyjen tietoturvavaatimusten mukaisesti. Tietoturvatestaus ja erityisesti penetraatiotestaus on suoritettava ohjelmiston kaikista merkittävistä uusista versioista LTS-standardeissa säädettyjen tietoturvavaatimusten mukaisesti. Penetraatiotestausta ei saa suorittaa ohjelmiston kehittäjä tai ohjelmiston kehittäjän alihankkija.

LIITE II

YHTEISET TOIMINNALLISET MENETTELYT

Euroopan unionin ja Sveitsin valaliiton välisen niiden kasvihuonekaasujen päästökauppajärjestelmien välistä yhteyttä koskevan sopimuksen 3 artiklan 6 kohdan mukaisesti

Pysyvää rekisteriyhteyttä koskevat menettelyt

Sisällysluettelo

1. Sanasto 10
2. Johdanto 11
2.1. Soveltamisala 11
2.2. Kohderyhmä 12
3. Lähestymistapa ja standardit 12
4. Häiriönhallinta 13
4.1. Häiriöiden havaitseminen ja kirjaaminen 13
4.2. Luokittelu ja ensi vaiheen tuki 13
4.3. Tutkinta ja diagnoosi 14
4.4. Ratkaisu ja palvelun toipuminen 14
4.5. Häiriön sulkeminen 14
5. Ongelmanhallinta 16
5.1. Ongelman tunnistaminen ja kirjaaminen 16
5.2. Ongelmien priorisointi 16
5.3. Ongelmien selvittäminen ja diagnoosi 16
5.4. Ratkaisu 16
5.5. Ongelman sulkeminen 16
6. Palvelupyyntöprosessi 17
6.1. Pyynnön käynnistäminen 17
6.2. Pyynnön kirjaaminen ja analysointi 17
6.3. Pyynnön hyväksyntä 17
6.4. Pyynnön toteuttaminen 17
6.5. Pyynnön eskalointi 17
6.6. Pyynnön toteuttamisen tarkastelu 18
6.7. Pyynnön sulkeminen 18
7. Muutoksenhallinta 19

7.1. Muutospyyntö 19
7.2. Muutosten arviointi ja suunnittelu 19
7.3. Muutosten hyväksyminen 19
7.4. Muutosten toteuttaminen 19
8. Julkaisunhallinta 19
8.1. Julkaisun suunnittelu 20
8.2. Julkaisupaketin kokoonpano ja testaus 20
8.3. Käyttöönoton valmistelu 21
8.4. Julkaisun takaisinkierto 21
8.5. Julkaisun tarkastelu ja sulkeminen 21
9. Turvallisuushäiriöiden hallinta 21
9.1. Tietoturvahäiriöiden luokittelu 22
9.2. Tietoturvahäiriöiden käsittely 22
9.3. Turvallisuushäiriöiden tunnistaminen 22
9.4. Turvallisuushäiriöiden analysointi 22
9.5. Turvallisuushäiriöiden vakavuuden arviointi, eskalointi ja raportointi 22
9.6. Turvallisuuteen liittyvistä toimenpiteistä raportointi 22
9.7. Valvonta, valmiuksien kehittäminen ja jatkuva parantaminen 23
10. Tietoturvan hallinta 23
10.1. Arkaluonteisten tietojen määrittäminen 23
10.2. Tieto-omaisuuden turvallisuustasot 23
10.3. Tieto-omaisuuden omistajan nimeäminen 24
10.4. Arkaluonteisten tietojen kirjaaminen 24
10.5. Arkaluonteisten tietojen käsittely 24
10.6. Pääsynhallinta 25
10.7. Varmenteiden/avainten hallinta 25

1. SANASTO

Taulukko 1-1. Lyhenteet ja määritelmät

Lyhenne/termi	Määritelmä
Varmentaja (Certification Authority)	Taho, joka myöntää digitaalisia varmenteita
CH	Sveitsin valaliitto
ETS	Päästökauppajärjestelmä
EU	Euroopan unioni
IMT	Häiriönhallintatiimi (Incident Management Team)
Tieto-omaisuus (Information Asset)	Yritykselle tai organisaatiolle arvokkaiden tietojen kokonaisuus
IT	Tietotekniikka
ITIL	Tietotekniikan infrastruktuurikirjasto
ITSM	IT-palvelunhallinta (IT Service Management)
LTS	Yhteyttä koskevat tekniset standardit (Linking Technical Standards)
Rekisteri	Päästökauppajärjestelmässä myönnettyjen päästöoikeuksien kirjanpitojärjestelmä, jolla seurataan, kuka omistaa sähköisillä tileillä olevat päästöoikeudet.
RFC	Muutospyyntö (Request for Change)
SIL	Arkaluonteisten tietojen luettelo (Sensitive Information List)
SR	Palvelupyyntö (Service Request)
Wiki	Verkkosivu, jolla käyttäjät voivat vaihtaa tietoja lisäämällä tai muokkaamalla sisältöä suoraan verkkoselaimen kautta

2. JOHDANTO

Euroopan unionin ja Sveitsin valaliiton välisessä niiden kasvihuonekaasujen päästökauppajärjestelmien välistä yhteyttä koskevassa 23 päivänä marraskuuta 2017 tehdyssä sopimuksessa, jäljempänä ’sopimus’, määrätään sellaisten päästöoikeuksien vastavuoroisesta tunnustamisesta, joita voidaan käyttää vaatimusten noudattamiseen Euroopan unionin päästökauppajärjestelmässä, jäljempänä ’EU ETS’, tai Sveitsin päästökauppajärjestelmässä, jäljempänä ’Sveitsin ETS’. EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välisen yhteyden toteuttamiseksi luodaan suora yhteys unionin rekisterin Euroopan unionin tapahtumalokin (EUTL) ja Sveitsin rekisterin täydentävän tapahtumalokin (SSTL) välillä, mikä mahdollistaa kummassa tahansa osapuolten päästökauppajärjestelmässä myönnettyjen päästöoikeuksien siirron rekisterien välillä (sopimuksen 3 artiklan 2 kohta). EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välisen yhteyden toteuttamiseksi otettiin käyttöön väliaikainen ratkaisu vuonna 2020. Vuodesta 2023 alkaen näiden kahden päästökauppajärjestelmän välinen rekisteriyhteys kehittyy asteittain pysyväksi rekisteriyhteydeksi, joka on tarkoitus panna täytäntöön viimeistään vuonna 2024 ja joka mahdollistaa toisiinsa yhteydessä olevien markkinoiden toiminnan markkinoiden likviditeetistä saatavien hyötyjen ja kahden toisiinsa liitetyn järjestelmän välisten tapahtumien toteuttamisen osalta tavalla, joka vastaa kahdesta järjestelmästä koostuvia yksittäisiä markkinoita ja antaa markkinaosapuolille mahdollisuuden toimia ikään kuin yksillä markkinoilla, jollei osapuolten erillisistä säännöksistä muuta johdu. (Sopimuksen liite II)

Sopimuksen 3 artiklan 6 kohdan mukaan Sveitsin rekisterivalvojan ja unionin keskusvalvojan on määritettävä yhteiset toiminnalliset menettelyt, jotka liittyvät teknisiin tai muihin seikkoihin, jotka ovat tarpeen järjestelmien yhteen kytkemisen sekä kansallisen lainsäädännön painopisteiden huomioon ottamisen kannalta. Valvojien laatimat yhteiset toiminnalliset menettelyt tulevat voimaan, kun sekakomitea on tehnyt päätöksen.

Sekakomitea hyväksyi yhteiset toiminnalliset menettelyt päätöksellään N:o 1/2020. Sekakomitea hyväksyy tässä asiakirjassa esitetyt päivitetyt yhteiset toiminnalliset menettelyt päätöksellään N:o 1/2024. Tämän päätöksen ja sekakomitean pyyntöjen mukaisesti Sveitsin rekisterinvalvoja ja unionin keskusvalvoja ovat laatineet tarkemmat tekniset ohjeet, jotka pidetään ajan tasalla ja 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 yhteinen käsitys EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän rekistereiden välisen yhteyden menettelyllisen perustan luomisesta. Asiakirjasta käyvät ilmi toimintaa koskevat yleiset menettelyitä koskevat vaatimukset, mutta yhteyden saattamiseen toiminnalliseksi tarvitaan eräitä teknisiä lisäohjeita.

Yhteyden moitteeton toiminta edellyttää teknisiä vaatimuksia, joiden avulla yhteyden toteutusta kehitetään. Sopimuksen 3 artiklan 7 kohdan mukaisesti nämä seikat esitetään yksityiskohtaisesti yhteyttä koskevia teknisiä standardeja (LTS) kuvaavassa asiakirjassa, jonka sekakomitea hyväksyy erillisellä päätöksellä.

Yhteisillä toiminnallisilla menettelyillä pyritään varmistamaan, että EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän rekisterien välisen yhteyden toimintaan liittyvät tietotekniikkapalvelut tuotetaan tehokkaasti ja tuloksellisesti. Tämä koskee etenkin palvelupyyntöprosessia, palvelun vikojen korjaamista, ongelmien ratkaisemista sekä tavanomaiseen toimintaan liittyvien tehtävien hoitamista tietoteknisten palvelujen hallintaa koskevien kansainvälisten standardien mukaisesti.

Sovitun pysyvän rekisteriyhteyden osalta on määriteltävä ainoastaan seuraavat yhteiset toiminnalliset menettelyt, jotka ovat osa tätä asiakirjaa:

- Häiriönhallinta
- Ongelmanhallinta
- Palvelupyyntöprosessi
- Muutoksenhallinta
- Julkaisunhallinta
- Turvallisuushäiriöiden hallinta
- Tietoturvan hallinta.

2.2. Kohderyhmä

Näiden yhteisten toiminnallisten menettelyjen kohderyhmänä ovat EU:n ja Sveitsin rekisterien tukitiimit.

3. LÄHESTYMISTAPA JA STANDARDIT

Kaikkiin yhteisiin toiminnallisiin menettelyihin sovelletaan seuraavia periaatteita:

- EU ja Sveitsi sopivat, että yhteiset toiminnalliset menettelyt määritellään ITIL:n version 4 pohjalta. Tähän standardiin perustuvia käytäntöjä toistetaan ja niitä mukautetaan pysyvään rekisteriyhteyteen liittyvien yksittäisten tarpeiden mukaisiksi.
- Viestintä ja koordinointi, joita yhteisten toiminnallisten menettelyjen käsittely osapuolten kesken edellyttää, tapahtuu Sveitsin ja EU:n rekisteripalvelupisteiden välityksellä. Tehtävät kohdennetaan aina toiselle osapuolista.
- Jos yhteisten toiminnallisten menettelyjen käsittelystä on erimielisyyttä, asian tutkivat ja ratkaisevat palvelupisteet yhdessä. Jos yksimielisyyteen ei päästä, yhteisen ratkaisun etsiminen eskaloidaan seuraavalle käsittelytasolle.

Eskalointitasot	EU	CH
1. taso	EU:n palvelupiste	Sveitsin palvelupiste
2. taso	EU:n operatiivinen päällikkö	Sveitsin rekisterin sovelluspäällikkö
3. taso	Sekakomitea (voi delegoida tehtävän sopimuksen 12 artiklan 5 kohdan mukaisesti)	
4. taso	Sekakomitea, jos 3. taso on delegoitu	

- Kumpikin osapuoli voi määrittää oman rekisterijärjestelmänsä toimintaa koskevat menettelyt, kunhan se ottaa tässä huomioon näihin yhteisiin toiminnallisiin menettelyihin liittyvät vaatimukset ja rajapinnat.
- Yhteisten toiminnallisten menettelyjen tukena käytetään IT-palvelunhallintatyökalua etenkin häiriönhallinnassa, ongelmanhallinnassa ja palvelupyyntöprosessissa sekä osapuolten välisessä viestinnässä.
- Sallittua on myös tietojen vaihtaminen sähköpostilla.
- Kumpikin osapuoli huolehtii käsittelyohjeiden mukaisten tietoturvaa koskevien vaatimusten noudattamisesta.

4. HÄIRIÖNHALLINTA

Häiriönhallintaprosessin tarkoituksena on palauttaa tietotekniset palvelut normaalille palvelutasolle mahdollisimman nopeasti häiriön jälkeen ja siten, että tavanomaiselle toiminnalle aiheutuu mahdollisimman vähän häiriötä.

Häiriönhallintaan kuuluu myös kirjanpito häiriöistä raportointia varten sekä häiriönhallinnan integroiminen muihin prosesseihin, jotta toimintaa voidaan parantaa jatkuvasti.

Yleisesti häiriönhallintaan kuuluvat seuraavat toimet:

- Häiriöiden havaitseminen ja kirjaaminen
- Luokittelu ja ensi vaiheen tuki
- Tutkinta ja diagnoosi
- Ratkaisu ja palvelun toipuminen
- Häiriön sulkeminen.

Koko häiriötilanteen keston ajan omistajuuden jatkuva käsitteleminen sekä valvonta, seuraaminen ja tiedottaminen kuuluvat häiriönhallintaprosessille.

4.1. Häiriöiden havaitseminen ja kirjaaminen

Häiriön havaitsija voi olla tukiryhmä tai jokapäiväistä valvontaa suorittava tekninen henkilöstö, tai se voidaan havaita automaattisilla seurantavälineillä.

Kun häiriö on havaittu, se on kirjattava ja sille on annettava yksilöllinen tunniste, jolloin häiriötä voidaan valvoa ja seurata asianmukaisesti. Häiriön yksilöllinen tunniste on tunniste, jonka häiriön havainneen osapuolen (joko EU:n tai Sveitsin) palvelupiste sille antaa tikettijärjestelmässä. Sitä on käytettävä kaikessa tähän häiriöön liittyvässä viestinnässä.

Kaikkien häiriöiden osalta yhteyspisteenä olisi oltava tiketin kirjannut osapuolen palvelupiste.

4.2. Luokittelu ja ensi vaiheen tuki

Häiriöiden luokittelun tarkoituksena on ymmärtää ja tunnistaa, mihin järjestelmään ja/tai palveluun häiriö vaikuttaa ja kuinka paljon. Luokittelu on tehokasta, jos se ohjaa häiriön oikealle resurssille ensimmäisellä yrittämällä, jolloin myös häiriöiden ratkaisu nopeutuu.

Luokitteluvaiheessa häiriö olisi luokiteltava ja sen tärkeysjärjestys määriteltävä vaikutuksen ja kiireellisyyden perusteella, jolloin se voidaan käsitellä tärkeysjärjestyksen mukaisessa ajassa.

Jos häiriö voi mahdollisesti vaikuttaa arkaluonteisten tietojen luottamuksellisuuteen tai eheyteen ja/tai järjestelmän saatavuuteen, häiriö olisi todettava myös turvallisuushäiriöksi, minkä jälkeen sitä

olisi käsiteltävä tämän asiakirjan luvussa ”Turvallisuushäiriöiden hallinta” määritellyn prosessin mukaisesti.

Ensi vaiheen diagnoosin tekee mahdollisuuksien mukaan tiketin kirjannut palvelupiste. Tätä varten palvelupisteessä tutkitaan, onko häiriö tunnettu virhe. Tässä tapauksessa ratkaisupolku tai väliaikaisratkaisu on jo tiedossa ja dokumentoitu.

Jos palvelupiste onnistuu ratkaisemaan häiriön, se sulkee häiriön tässä vaiheessa, koska häiriönhallinnan ensisijainen tavoite eli palvelun ripeä palautus loppukäyttäjille on toteutettu. Jos palvelupiste ei onnistu ratkaisemaan häiriötä, se eskaloi häiriön oikealle selvitysryhmälle lisätutkintaa ja diagnoosia varten.

4.3. Tutkinta ja diagnoosi

Häiriöiden tutkintaa ja diagnoosia sovelletaan, kun palvelupiste ei pysty ratkaisemaan häiriötä ensi vaiheen diagnoosin kuluessa, minkä jälkeen häiriö eskaloidaan oikealle taholle. Häiriöiden eskalointi on keskeinen osa tutkinta- ja diagnoosiprosessia.

Yleisenä käytäntönä tutkinta- ja diagnoosivaiheessa on, että häiriö yritetään saada uudelleen aikaan valvotuissa olosuhteissa. Häiriön tutkintaa ja diagnoosia tehtäessä on tärkeää ymmärtää häiriöön johtaneiden tapahtumien oikea järjestys.

Eskalointi tarkoittaa sen tunnustamista, ettei häiriötä kyetä ratkaisemaan senhetkisellä tuen tasolla, vaan sen käsittely on siirrettävä ylemmän tason tukiryhmälle tai toiselle osapuolelle. Eskalointi voi olla: joko horisontaalista (funktionaalista) tai vertikaalista (hierarkkista)

Häiriön tallentanut ja siitä ilmoituksen tehnyt palvelupiste vastaa häiriön eskaloinnista oikealle resurssille sekä häiriön kokonaistilanteen ja kohdentamisen seurannasta.

Osapuoli, jolle häiriö on kohdennettu, vastaa pyydettyjen toimien toteuttamisesta oikea-aikaisesti sekä palautteen antamisesta oman osapuolensa palvelupisteelle.

4.4. Ratkaisu ja palvelun toipuminen

Häiriön ratkaisu ja palvelun toipuminen suoritetaan, kun häiriö on ymmärretty täysin. Häiriön ratkaisun löytäminen tarkoittaa, että selvitettävän asian korjaamiseen on löytynyt tapa. Toipumisvaihe tarkoittaa aikaa, jolloin ratkaisua sovelletaan.

Kun oikeat resurssit ovat korjanneet palvelun vian, häiriö ohjataan takaisin oikealle palvelupisteelle, joka kirjasi häiriön ja joka varmistaa häiriön käsittelyn käynnistäjältä, että virhe on korjattu ja häiriö voidaan sulkea. Häiriön käsittelyn kuluessa tehdyt havainnot kirjataan tulevaa käyttöä varten.

Toipumisen voi suorittaa IT-tukihenkilöstö, tai loppukäyttäjälle voidaan antaa ohjeet, joita hänen on noudatettava.

4.5. Häiriön sulkeminen

Sulkeminen on häiriönhallintaprosessin viimeinen vaihe, joka tapahtuu pian häiriön ratkaisun jälkeen.

Sulkemisvaiheessa suoritettavat toimet on kirjattu tarkistuslistaan, josta mainitaan erityisesti seuraavat kohdat:

- häiriölle annetun alustavan luokituksen todentaminen
- kaikkien häiriöön liittyvien tietojen asianmukainen tallentaminen

- häiriön asianmukainen dokumentointi sekä tietämyskannan päivittäminen
- riittävä viestintä kaikille sidosryhmille, joihin häiriö on vaikuttanut suoraan tai välillisesti.

Häiriö suljetaan virallisesti, kun palvelupiste on suorittanut koko häiriön sulkemisvaiheen ja tiedottanut siitä toiselle osapuolelle.

Kun häiriö on suljettu, sitä ei avata uudelleen. Jos häiriö toistuu pian uudelleen, alkuperäistä häiriötä ei avata uudestaan, vaan kirjataan uusi häiriö.

Jos sekä EU:n että Sveitsin palvelupisteet seuraavat häiriötä, lopullisesta sulkemisesta vastaa tiketin kirjannut palvelupiste.

5. ONGELMANHALLINTA

Tätä menettelyä olisi noudatettava aina, kun havaitaan ongelma, joka käynnistää ongelmanhallintaprosessin. Ongelmanhallinnassa keskitytään laadun parantamiseen ja havaittujen häiriöiden määrän vähentämiseen. Ongelma saattaa aiheuttaa yhden tai useampia häiriöitä. Häiriön ilmoittamisen jälkeen häiriönhallinnan tavoitteena on palauttaa palvelu mahdollisimman nopeasti, mahdollisesti väliaikaratkaisuja käyttäen. Kun ongelma on kirjattu, tavoitteena on selvittää asian perussyy, jotta voidaan määrittää muutos, jolla varmistetaan, että ongelmaa ja siihen liittyviä häiriöitä ei enää esiinny.

5.1. Ongelman tunnistaminen ja kirjaaminen

Sen perusteella, kumpi osapuoli käynnisti tiketin, joko EU:n tai Sveitsin palvelupiste toimii yhteyspisteenä ongelmaan liittyvissä asioissa.

Ongelman yksilöllinen tunniste on IT-palvelunhallinnan antama tunniste. Sitä on käytettävä kaikessa ongelmaan liittyvässä viestinnässä.

Ongelma voi syntyä häiriön seurauksena, tai se voidaan milloin tahansa avata järjestelmässä oma-aloitteisena toimena havaittujen selvitettävien asioiden korjaamiseksi.

5.2. Ongelmien priorisointi

Ongelmat voidaan seurannan helpottamiseksi luokitella häiriöiden tavoin niiden vakavuuden ja tärkeysjärjestyksen perusteella. Tässä on otettava huomioon ongelmaan liittyvien häiriöiden vaikutus ja esiintymistiheys.

5.3. Ongelmien selvittäminen ja diagnoosi

Kumpikin osapuoli voi todeta ongelman. Käsittelyn käynnistäneen osapuolen palvelupiste vastaa ongelman kirjaamisesta, sen kohdentamisesta oikealle resurssille ja ongelman kokonaistilanteen seurannasta.

Selvitysryhmä, jolle ongelma eskaloitiin, vastaa ongelman oikea-aikaisesta käsittelemisestä sekä viestinnästä palvelupisteen kanssa.

Kumpikin osapuoli voi pyynnöstä vastata sen varmistamisesta, että kohdennetut toimet suoritetaan, sekä palautteen antamisesta omalle palvelupisteelleen.

5.4. Ratkaisu

Selvitysryhmä, jolle ongelma on kohdennettu, vastaa ongelman ratkaisemisesta ja asiaa koskevien tietojen toimittamisesta oman osapuolensa palvelupisteelle.

Ongelman käsittelyn kuluessa tehdyt havainnot kirjataan tulevaa käyttöä varten.

5.5. Ongelman sulkeminen

Ongelma suljetaan virallisesti, kun ongelma on korjattu tekemällä tarvittava muutos. Ongelman sulkemisvaiheen suorittaa palvelupiste, joka kirjasi ongelman ja ilmoitti siitä toisen osapuolen palvelupisteelle.

6. PALVELUPYYNTÖPROSESSI

Palvelupyyntöprosessi tarkoittaa uutta tai olemassa olevaa palvelua koskevan pyynnön päästä päähän hallintaa sen rekisteröinti- ja hyväksymishetkestä aina sulkemiseen saakka. Palvelupyynnöt ovat yleensä pieniä, ennalta määriteltyjä, toistuvia, ennalta hyväksyttyjä tai menettelytapoja koskevia pyyntöjä.

Tärkeimmät noudatettavat vaiheet esitetään seuraavassa:

6.1. Pyynnön käynnistäminen

Palvelupyyntöön liittyvät tiedot toimitetaan EU:n tai Sveitsin palvelupisteelle sähköpostitse, puhelimitse, tai IT-palvelunhallintatyökalun tai minkä tahansa muun sovitun viestintäkanavan kautta.

6.2. Pyynnön kirjaaminen ja analysointi

Kaikissa palvelupyynnöissä yhteyspisteenä olisi oltava EU:n tai Sveitsin palvelupiste sen mukaan, kumpi osapuoli teki palvelupyynnön. Kyseinen palvelupiste vastaa palvelupyynnön kirjaamisesta ja analysoinnista riittävää huolellisuutta noudattaen.

6.3. Pyynnön hyväksyntä

Palvelupyynnön tehneen osapuolen palvelupisteen työntekijä tarkistaa, tarvitaanko toiselta osapuolelta jotain hyväksyntää, ja ryhtyy tarvittaessa hankkimaan sitä. Jos palvelupyyntöä ei hyväksytä, palvelupiste päivittää tiketin ja sulkee sen.

6.4. Pyynnön toteuttaminen

Tämä vaihe kattaa palvelupyyntöjen tehokkaan ja tuloksellisen käsittelyn. Seuraavat tilanteet olisi erotettava toisistaan:

- Palvelupyynnön toteuttaminen vaikuttaa vain yhteen osapuoleen. Tässä tapauksessa kyseinen osapuoli tekee työtilaukset ja koordinoi toteutusta.
- Palvelupyynnön toteuttaminen vaikuttaa sekä EU:hun että Sveitsiin. Tässä tapauksessa palvelupisteet antavat omia vastuualueitaan koskevat työtilaukset. Molemmat palvelupisteet koordinoivat palvelupyynnön toteuttamisen käsittelyä. Kokonaisvastuu on palvelupisteellä, joka vastaanotti palvelupyynnön ja käynnisti sen käsittelyn.

Kun palvelupyyntö on ratkaistu, se on muutettava tilaan ”Ratkaistu”.

6.5. Pyynnön eskalointi

Palvelupiste voi tarvittaessa eskaloida ratkaisemattoman palvelupyynnön oikealle resurssille (kolmannelle osapuolelle).

Osapuolet tekevät eskaloinnit omille kolmansille osapuolilleen: esimerkiksi EU:n palvelupisteen on otettava yhteyttä Sveitsin palvelupisteeseen, jotta asia voidaan eskaloida Sveitsin kolmannelle osapuolelle, ja päinvastoin.

Kolmas osapuoli, jolle palvelupyyntö eskaloitiin, vastaa palvelupyynnön oikea-aikaisesta käsittelemisestä sekä viestinnästä palvelupyynnön eskaloineen palvelupisteen kanssa.

Palvelupyynnön kirjannut palvelupiste vastaa palvelupyynnön kokonaistilanteen ja kohdentamisen seurannasta.

6.6. Pyynnön toteuttamisen tarkastelu

Asiasta vastaava palvelupiste toimittaa palvelupyyntötietueen lopulliseen laaduntarkastukseen ennen sulkemista. Tarkoituksena on varmistaa, että palvelupyyntö on todella käsitelty ja kaikki pyynnön elinkaaren kuvaamiseen tarvittavat tiedot on toimitettu riittävän yksityiskohtaisina. Pyynnön käsittelyn kuluessa tehdyt havainnot kirjataan lisäksi tulevaa käyttöä varten.

6.7. Pyynnön sulkeminen

Jos osapuolet, joille palvelupyyntö on kohdennettu, ovat yhtä mieltä siitä, että palvelupyyntö on toteutettu ja pyynnön esittäjä katsoo asian ratkaistuksi, pyyntö asetetaan tilaan ”Suljettu”.

Palvelupyyntö suljetaan virallisesti, kun palvelupyynnön kirjannut palvelupiste on suorittanut pyynnön sulkemisvaiheen ja ilmoittanut asiasta toisen osapuolen palvelupisteelle.

7. MUUTOKSENHALLINTA

Tavoitteena on varmistaa, että IT-infrastruktuurin hallitsemiseksi kaikkien muutosten tehokkaaseen ja viipymättä tapahtuvaan käsittelyyn käytetään standardoituja menetelmiä ja menettelyjä, jotta muutoksiin liittyvien häiriöiden määrä ja niiden vaikutus palveluun säilyy mahdollisimman pienenä. IT-infrastruktuuriin voidaan joutua tekemään muutoksia reaktiivisesti, jolloin niillä ratkaistaan ongelmia tai reagoidaan ulkopuolelta tuleviin vaatimuksiin, esimerkiksi lainsäädännön muutoksiin, tai proaktiivisesti, jolloin niillä pyritään tehostamaan toimintaa ja lisäämään sen tuloksellisuutta tai muuttamaan toimintaa liiketoimintaan perustuvien aloitteiden mukaiseksi.

Muutoksenhallintaprosessiin kuuluvissa vaiheissa tallennetaan kaikki muutospyynnön yksityiskohdat myöhempää seurantaa varten. Prosessilla varmistetaan, että muutos validoidaan ja testataan ennen käyttöönottoa. Käyttöönoton onnistumisesta vastaa julkaisunhallintaprosessi.

7.1. Muutospyyntö

Muutospyyntö toimitetaan muutoksenhallintatiimille validoitavaksi ja hyväksyttäväksi. Kaikissa muutospyynnöissä yhteyspisteenä olisi oltava EU:n tai Sveitsin palvelupiste sen mukaan, kumpi osapuoli teki muutospyynnön. Kyseinen palvelupiste vastaa muutospyynnön kirjaamisesta ja analysoinnista riittävää huolellisuutta noudattaen.

Muutospyynnön alkuperä voi olla jokin seuraavista:

- häiriö, joka aiheuttaa muutoksen
- olemassa oleva ongelma, jonka seurauksena tehdään muutos
- loppukäyttäjä, joka pyytää uutta muutosta
- käynnissä oleva huoltotyö, jonka seurauksena tehdään muutos
- lainsäädännön muuttaminen.

7.2. Muutosten arviointi ja suunnittelu

Tämä vaihe koskee muutosten arviointiin ja suunnitteluun liittyviä toimia. Siihen sisältyvät priorisointi sekä riskien ja vaikutusten minimoimiseksi tehdyt suunnittelutoimet.

Jos muutospyynnön toteuttaminen vaikuttaa sekä EU:hun että Sveitsiin, muutospyynnön kirjannut osapuoli pyytää toista osapuolta todentamaan muutoksen arvioinnin ja suunnittelun.

7.3. Muutosten hyväksyminen

Asiaan kuuluvan eskalointitason on hyväksyttävä kaikki rekisteröidyt muutospyynnöt.

7.4. Muutosten toteuttaminen

Muutosten toteuttaminen käsitellään julkaisunhallintaprosessissa Molempien osapuolten julkaisunhallintatiimit seuraavat omia prosessejaan, joihin kuuluu suunnittelua ja testausta. Muutoksen tarkastelu tehdään, kun toteutus on valmis. Olemassa olevaa muutoksenhallintaprosessia tarkastellaan jatkuvasti ja päivitetään aina tarvittaessa, millä varmistetaan, että kaikki tapahtuu suunnitelman mukaisesti.

8. JULKAISUNHALLINTA

Julkaisu edustaa yhtä tai useampaa IT-järjestelmään tehtyä muutosta, jotka on koottu julkaisusuunnitelmaan ja jotka on hyväksyttävä, valmisteltava, kokoonpantava, testattava ja otettava

käyttöön samalla kertaa. Julkaisu voi olla ohjelmavirheen korjaus, laitteisto- tai muu komponenttimuutos, ohjelmistomuutos, sovellusversion päivitys tai dokumentaatioon ja/tai prosesseihin tehtävä muutos. Kunkin julkaisun sisältöä hallinnoidaan ja se testataan ja otetaan käyttöön yhtenä kokonaisuutena.

Julkaisunhallinnan tavoitteena on suunnitella, kokoonpanna, testata ja validoida sekä tuottaa valmiudet tarjota suunniteltuja palveluja, jotka täyttävät sidosryhmien vaatimukset ja asetetut tavoitteet. Kaikkien palveluun tehtävien muutosten hyväksymisperusteet määritellään ja dokumentoidaan suunnittelun koordinoinnin yhteydessä ja toimitetaan julkaisunhallintatiimeille.

Julkaisu koostuu tyypillisesti useista ongelmiin tehdyistä korjauksista sekä palvelun parannuksista. Se sisältää tiedon hyväksyttyjen muutosten toteuttamiseen tarvittavista uusista tai muutetuista ohjelmistoista tai laitteistoista.

8.1. Julkaisun suunnittelu

Prosessin ensimmäisessä vaiheessa kohdennetaan hyväksytyt muutokset julkaisupaketteihin ja määritellään julkaisujen laajuus ja sisältö. Tämän tiedon perusteella julkaisun suunnittelun osaprosessissa laaditaan aikataulu julkaisun kokoonpanolle, testaukselle ja käyttöönotolle.

Suunnittelussa olisi määriteltävä seuraavat:

- julkaisun laajuus ja sisältö
- julkaisua koskeva riskinarviointi ja riskiprofiili
- asiakkaat/käyttäjät, joihin julkaisu vaikuttaa
- julkaisusta vastaava tiimi
- toimitus- ja käyttöönottostrategia
- julkaisuun ja käyttöönottoon tarvittavat resurssit.

Osapuolet ilmoittavat toisilleen julkaisujensa suunnittelusta ja huoltoikkunoista. Jos julkaisu vaikuttaa sekä EU:hun että Sveitsiin, ne koordinoivat suunnittelua ja määrittelevät yhteisen huoltoikkunan.

8.2. Julkaisupaketin kokoonpano ja testaus

Julkaisunhallintaprosessin kokoonpano- ja testausvaiheessa määritetään lähestymistapa, jota noudatetaan julkaisun tai julkaisupaketin toteutuksessa ja valvottujen ympäristöjen ylläpitämisessä ennen tuotannon muuttamista sekä kaikissa julkaistuissa ympäristöissä tehtävien muutosten testauksessa.

Jos julkaisu vaikuttaa sekä EU:hun että Sveitsiin, ne koordinoivat toimitussuunnitelmia ja testejä. Tähän sisältyvät seuraavat asiat:

- miten ja milloin julkaisuyksiköt ja palvelukomponentit toimitetaan
- mitkä ovat tyypilliset toimitusajat ja miten toimitaan viivästyksen sattuessa
- miten seurataan toimituksen edistymistä ja saadaan vahvistukset
- millä mittareilla julkaisun käyttöönottoon tähtääviä toimia valvotaan ja niiden onnistuminen määritetään
- asiaankuuluvien toimintojen ja muutosten yleiset testitapaukset.

Tämän osaprosessin päätteeksi kaikki tarvittavat julkaisun komponentit ovat valmiita otettavaksi käyttöön tuotantoympäristössä.

8.3. Käyttöönoton valmistelu

Valmistelun osaprosessilla varmistetaan, että viestintäsuunnitelmat on määritelty oikein ja ilmoitukset ovat valmiita lähetettäviksi kaikille sidosryhmille ja loppukäyttäjille, joihin julkaisu vaikuttaa, ja että julkaisu on integroitu muutoksenhallintaprosessiin sen varmistamiseksi, että kaikki muutokset tehdään hallitusti ja vaadittavat tahot hyväksyvät ne.

Jos julkaisu vaikuttaa sekä EU:hun että Sveitsiin, ne koordinoivat seuraavia toimia:

- aikatauluttamista ja tuotantoympäristössä käyttöönoton valmistelua koskevien merkintöjen tekeminen muutospyyntötietueeseen
- toteutussuunnitelman laatiminen
- takaisinkiertoa koskeva lähestymistapa, jolla voidaan palata takaisin aiempaan tilaan, jos käyttöönotto epäonnistuu
- ilmoitusten lähettäminen kaikille tarvittaville osapuolille
- hyväksynnän pyytäminen oikealta eskalointitasolta julkaisun toteuttamiselle.

8.4. Julkaisun takaisinkierto

Jos käyttöönotto epäonnistuu tai testauksessa todetaan, että käyttöönotto ei onnistunut tai se ei täytä sovittuja hyväksymis- tai laatuvaatimuksia, molempien osapuolten julkaisunhallintatiimien on tehtävä takaisinkierto aiempaan tilaan. Takaisinkierrosta on ilmoitettava kaikille tarvittaville sidosryhmille, myös niille loppukäyttäjille, joihin asia vaikuttaa. Ennen hyväksynnän saamista prosessi voidaan aloittaa uudelleen mistä tahansa edeltävästä vaiheesta.

8.5. Julkaisun tarkastelu ja sulkeminen

Käyttöönoton tarkasteluun olisi sisällytettävä seuraavat toimet:

- kerätään palautetta asiakkaiden, käyttäjien ja palveluntoimituksen tyytyväisyydestä käyttöönottoon (kerätään palaute ja otetaan se huomioon palvelun jatkuvassa parantamisessa)
- tarkastellaan mahdollisesti täyttymättä jääneitä laatuvaatimuksia
- tarkistetaan, että kaikki toimet, tarpeelliset korjaukset ja muutokset on suoritettu loppuun
- varmistetaan, ettei käyttöönoton lopussa ole valmiuksiin, resursseihin, kapasiteettiin tai suorituskykyyn liittyviä selvitettäviä asioita
- tarkistetaan, että mahdolliset ongelmat, tunnetut virheet ja väliaikaisratkaisut on dokumentoitu ja että asiakas, loppukäyttäjät, operatiivinen tuki ja muut osapuolet, joihin ne vaikuttavat, hyväksyvät ne
- valvotaan käyttöönotosta aiheutuneita häiriöitä ja ongelmia, ja annetaan alkuvaiheen tukea operatiivisille tiimeille, jos niiden työmäärä lisääntyy julkaisun vuoksi
- päivitetään tukidokumentaatio eli teknisiä tietoja sisältävät asiakirjat
- luovutetaan julkaisun käyttöönotto muodollisesti palvelutoiminnoille
- dokumentoidaan saadut kokemukset
- kerätään julkaisun yhteenvetoasiakirjat toteutustiimeiltä
- suljetaan julkaisu virallisesti muutospyyntötietueen todentamisen jälkeen.

9. TURVALLISUUSHÄIRIÖIDEN HALLINTA

Turvallisuushäiriöiden hallinnalla tarkoitetaan turvallisuushäiriöiden käsittelyprosessia, jonka tarkoituksena on tehdä mahdolliseksi häiriöstä ilmoittaminen niille sidosryhmille, joihin häiriö on

mahdollisesti vaikuttanut, häiriön arviointi ja priorisointi ja häiriöön reagointi, jolla selvitetään arkaluonteisen tieto-omaisuuden luottamuksellisuuteen, saatavuuteen tai eheyteen kohdistuneet tapahtuneet, epäillyt tai mahdolliset loukkaukset.

9.1. Tietoturvahäiriöiden luokittelu

Kaikki häiriöt, jotka vaikuttavat unionin rekisterin ja Sveitsin rekisterin väliseen yhteyteen, on analysoitava sen määrittämiseksi, onko arkaluonteisten tietojen luetteloon tallennettujen arkaluonteisten tietojen luottamuksellisuutta, eheyttä tai saatavuutta mahdollisesti loukattu.

Jos näin on tapahtunut, häiriö on kuvattava tietoturvahäiriöksi, kirjattava välittömästi IT-palvelunhallintatyökaluun ja käsiteltävä tietoturvahäiriönä.

9.2. Tietoturvahäiriöiden käsittely

Turvallisuushäiriöt siirretään kolmannen eskalointitason vastuulle, ja häiriöiden ratkaisemisesta huolehtii erityinen häiriönhallintatiimi.

Häiriönhallintatiimi vastaa seuraavista tehtävistä:

- ensimmäisen analyysin suorittaminen, häiriön luokittelu ja sen vakavuuden arviointi
- toimien koordinointi kaikkien sidosryhmien välillä, mukaan lukien häiriön analyysin täydellinen dokumentointi, häiriöön puuttumiseksi tehdyt päätökset sekä mahdolliset havaitut heikkoudet
- turvallisuushäiriön vakavuuden mukaan sen oikea-aikainen eskalointi sopivalle tasolle tiedoksi antamista ja/tai päätöksen tekemistä varten.

Tietoturvan hallintaprosessissa kaikki häiriöitä koskevat tiedot luokitellaan tiedon korkeimman turvallisuusluokan mukaan, mutta vähintään tasolle SENSITIVE: *ETS*.

Jos tutkinta on edelleen käynnissä ja/tai kyseessä on heikkous, jota voidaan käyttää hyväksi, tieto luokitellaan häiriön korjaamiseen saakka tasolle SPECIAL HANDLING: *ETS Critical*.

9.3. Turvallisuushäiriöiden tunnistaminen

Turvallisuustapahtuman tyypin perusteella tietoturvavastaava päättää, mitkä organisaatiot on otettava mukaan tapahtuman käsittelyyn ja häiriönhallintatiimiin.

9.4. Turvallisuushäiriöiden analysointi

Häiriönhallintatiimi pitää yhteyttä kaikkiin mukana oleviin organisaatioihin ja niiden tiimien asiaankuuluviin jäseniin, jotta häiriötä voidaan tarkastella. Analyysin aikana määritetään, missä määrin omaisuuden luottamuksellisuutta, eheyttä tai saatavuutta on menetetty, sekä arvioidaan tästä kaikille kohteeksi joutuneille osapuolille aiheutuneita seurauksia. Seuraavaksi määritellään häiriön ratkaisemiseksi ja sen vaikutuksen hallitsemiseksi tarvittavat ensi vaiheen toimet ja jatkotoimet, mukaan lukien näiden toimien vaikutus resursseihin.

9.5. Turvallisuushäiriöiden vakavuuden arviointi, eskalointi ja raportointi

Häiriönhallintatiimi arvioi kaikkien uusien turvallisuushäiriöiden vakavuuden sen jälkeen, kun ne on kuvattu turvallisuushäiriöksi, ja aloittaa välittömästi tarvittavat toimet häiriön vakavuuden mukaisesti.

9.6. Turvallisuuteen liittyvistä toimenpiteistä raportointi

Häiriönhallintatiimi sisällyttää häiriöiden rajaamiseksi tehtyjen toimenpiteiden sekä toipumisen tulokset tietoturvahäiriöihin liittyvistä toimenpiteistä laadittavaan raporttiin. Raportti toimitetaan

kolmannelle eskalointitasolle salattua sähköpostia tai muuta molempien osapuolten hyväksymää suojattua viestintämenetelmää käyttäen.

Tehtävästä vastaava osapuoli tarkastelee häiriön rajaamiseksi tehtyjen toimenpiteiden sekä toipumisen tuloksia, ja

- yhdistää rekisterin uudelleen, jos yhteys on jouduttu aiemmin katkaisemaan
- välittää häiriötä koskevat tiedonannot rekisteritiimeille
- sulkee häiriön.

Häiriönhallintatiimin olisi esitettävä tietoturvahäiriöistä laadittavassa raportissa suojatussa muodossa tarvittavat yksityiskohdat, joiden avulla varmistetaan kirjaamisen ja viestinnän johdonmukaisuus ja annetaan mahdollisuus rajata häiriö viipymättä suoritetuilla asianmukaisilla toimenpiteillä. Kun raportti on valmis, häiriönhallintatiimi toimittaa tietoturvahäiriöstä laadittavan loppuraportin hyvissä ajoin.

9.7. Valvonta, valmiuksien kehittäminen ja jatkuva parantaminen

Häiriönhallintatiimi toimittaa kaikista turvallisuushäiriöistä raportit kolmannelle eskalointitasolle. Kyseisellä eskalointitasolla määritetään raportin avulla seuraavat asiat:

- turvallisuuden valvonnan ja/tai toiminnan heikot kohdat, joita on vahvistettava
- mahdollinen tarve vahvistaa tätä menettelyä, jotta sillä voidaan parantaa häiriöihin liittyvien toimenpiteiden tehokkuutta
- koulutukseen ja valmiuksien kehittämiseen liittyvät mahdollisuudet, joilla vahvistetaan entisestään rekisterijärjestelmien tietoturvaan liittyvää häiriönsietokykyä, vähennetään tulevien häiriöiden riskiä ja minimoidaan niiden vaikutukset.

10. TIETOTURVAN HALLINTA

Tietoturvan hallinnan tavoitteena on varmistaa organisaation turvallisuusluokiteltujen tietojen, data-aineistojen ja IT-palveluiden luottamuksellisuus, eheys ja saatavuus. Teknisten komponenttien ja niiden suunnittelun ja testauksen (ks. LTS) lisäksi pysyvän rekisterilinkin turvallisuusvaatimusten täyttäminen edellyttää seuraavassa lueteltuja yhteisiä toiminnallisia menettelyjä.

10.1. Arkaluonteisten tietojen määrittäminen

Tiedon arkaluonteisuutta arvioidaan määrittämällä, kuinka suuria haittoja liiketoiminnalle (esimerkiksi taloudelliset tappiot, imagohaitta, lain rikkominen) tähän tietoon kohdistuvalla tietoturvaloukkauksella voisi olla.

Arkaluonteinen tieto-omaisuus määritellään sen perusteella, millainen vaikutus tiedolla on päästökauppajärjestelmien väliseen yhteyteen.

Tämän tiedon arkaluonteisuutta arvioidaan tämän asiakirjan kohdassa ”Tietoturvahäiriöiden käsittely” esitetyn, järjestelmien väliseen yhteyteen sovellettavan turvallisuusasteikon mukaisesti.

10.2. Tieto-omaisuuden turvallisuustasot

Kun tieto-omaisuuteen kuuluva tieto on tunnistettu arkaluonteiseksi, se luokitellaan seuraavia sääntöjä noudattaen:

- jos luottamuksellisuus-, eheys- tai saatavuustasoista vähintään yksi on HIGH (korkea), tiedon luokitus on SPECIAL HANDLING: *ETS Critical*;
- jos luottamuksellisuus-, eheys- tai saatavuustasoista vähintään yksi on MEDIUM (keskitasoinen), tiedon luokitus on SENSITIVE: *ETS*;
- jos kaikki luottamuksellisuus-, eheys- tai saatavuustasot ovat tasoa LOW (matala), tiedon luokitus on EU**:** SENSITIVE: *ETS Joint Procurement.* Sveitsin merkintä: LIMITED: ETS.

10.3. Tieto-omaisuuden omistajan nimeäminen

Kaikella tieto-omaisuudella on oltava nimetty omistaja. Päästökauppajärjestelmän tieto-omaisuus, joka kuuluu EUTL:n ja SSTL:n väliseen yhteyteen tai liittyy siihen, on sisällytettävä molempien osapuolten ylläpitämään yhteiseen omaisuusluetteloon. Päästökauppajärjestelmän tieto-omaisuus, joka ei liity EUTL:n ja SSTL:n väliseen yhteyteen, on sisällytettävä kyseisen osapuolen ylläpitämään omaisuusluetteloon.

Yksittäisten tieto-omaisuuteen kuuluvien tietojen, jotka kuuluvat EUTL:n ja SSTL:n väliseen yhteyteen tai liittyvät siihen, omistajuudesta sovitaan osapuolten kesken. Tieto-omaisuuden omistaja vastaa sen arkaluonteisuuden arvioinnista.

Omistajan olisi oltava riittävän korkeassa asemassa hänelle osoitetun tieto-omaisuuden arvoon nähden. Omistajan vastuusta tieto-omaisuudesta sekä vaaditun luottamuksellisuus-, eheys- ja saatavuustason ylläpitämistä koskevasta velvollisuudesta olisi sovittava virallisesti.

10.4. Arkaluonteisten tietojen kirjaaminen

Kaikki arkaluonteiset tiedot on kirjattava arkaluonteisten tietojen luetteloon.

Jos arkaluonteisten tietojen yhdistämisellä voi olla suurempi vaikutus kuin yksittäisellä tiedolla, tämä on otettava tarvittaessa huomioon ja kirjattava arkaluonteisten tietojen luetteloon (esimerkiksi järjestelmän tietokantaan tallennettu tietokokonaisuus).

Arkaluonteisten tietojen luetteloa voidaan muuttaa. Tieto-omaisuuteen kohdistuvat uhkat ja haavoittuvuudet sekä turvallisuushäiriöiden todennäköisyys tai seuraukset voivat muuttua etukäteen ilmoittamatta, ja rekisterijärjestelmien toimintaan saatetaan liittää mukaan uutta tieto-omaisuutta.

Arkaluonteisten tietojen luetteloa on tarkasteltava säännöllisesti uudelleen, ja mahdolliset uudet, arkaluonteisiksi määritellyt tiedot on viipymättä kirjattava arkaluonteisten tietojen luetteloon.

Arkaluonteisten tietojen luettelossa on oltava kaikista tietueista vähintään seuraavat tiedot:

- tiedon kuvaus
- tiedon omistaja
- turvallisuustaso
- maininta siitä, kuuluuko tietoon henkilötietoja
- tarvittaessa lisätietoja.

10.5. Arkaluonteisten tietojen käsittely

Kun arkaluonteisia tietoja käsitellään unionin rekisterin ja Sveitsin rekisterin välisen yhteyden ulkopuolella, niiden käsittelyssä on noudatettava käsittelyohjeiden määräyksiä.

Arkaluonteisia tietoja, joita käsitellään unionin rekisterin ja Sveitsin rekisterin välisessä yhteydessä, on käsiteltävä osapuolten turvallisuusvaatimusten mukaisesti.

10.6. Pääsynhallinta

Pääsynhallinnan tarkoituksena on antaa valtuutetuille käyttäjille oikeus käyttää palvelua ja samalla estää muita kuin valtuutettuja käyttäjiä käyttämästä sitä. Pääsynhallintaa kutsutaan myös (käyttö)oikeuksienhallinnaksi tai identiteetin hallinnaksi.

Pysyvä rekisteriyhteys ja sen toiminta edellyttävät, että molemmilla osapuolilla on pääsy seuraaviin komponentteihin:

- Wiki: yhteistyöympäristö, jossa voidaan vaihtaa yhteisiä tietoja esimerkiksi julkaisujen suunnittelusta
- IT-palvelunhallintatyökalu häiriönhallintaa ja ongelmanhallintaa varten (ks. luku ”Lähestymistapa ja standardit”)
- viestinvaihtojärjestelmä: kummankin osapuolen on otettava käyttöön suojattu viestinvaihtojärjestelmä, jossa voidaan välittää tapahtumien tietoja sisältäviä viestejä.

Sveitsin rekisterinvalvoja ja unionin keskusvalvoja varmistavat, että pääsyoikeudet ovat ajan tasalla, ja toimivat oman osapuolensa yhteyspisteenä pääsynhallintaan liittyvissä asioissa. Pääsyoikeuspyynnöt käsitellään pyynnön toteuttamista koskevien menettelyjen mukaisesti.

10.7. Varmenteiden/avainten hallinta

Kumpikin osapuoli vastaa itse omasta varmenteiden/avainten hallinnastaan (varmenteiden/avainten luominen, rekisteröinti, säilytys, asentaminen, käyttö, uusiminen, sulkeminen, varmuuskopiointi ja palautus). Yhteyttä koskevissa teknisissä standardeissa kuvatun mukaisesti on käytettävä vain varmentajan (Certification Authority) myöntämiä digitaalisia varmenteita, joihin kumpikin osapuoli luottaa. Varmenteiden/avainten käsittelyssä ja säilytyksessä on noudatettava käsittelyohjeiden määräyksiä.

Molemmat osapuolet koordinoivat varmenteiden ja avainten mahdollista sulkemista ja/tai uusimista. Tämä tapahtuu pyynnön toteuttamista koskevien menettelyjen mukaisesti.

Sveitsin rekisterinvalvoja ja unionin keskusvalvoja vaihtavat varmenteet/avaimet suojattuja viestintävälineitä käyttäen käsittelyohjeiden määräysten mukaisesti.

Varmenteiden/avainten todentamisessa osapuolten kesken millä tahansa keinolla on käytettävä kaksivaiheista varmennusta.

LIITE III

YHTEYTTÄ KOSKEVAT TEKNISET STANDARDIT (LTS)

Euroopan unionin ja Sveitsin valaliiton välisen niiden kasvihuonekaasujen päästökauppajärjestelmien välisestä yhteydestä tehdyn sopimuksen 3 artiklan 7 kohdan nojalla

Pysyvää rekisteriyhteyttä koskeva standardi

Sisällysluettelo

1. Sanasto 30
2. Johdanto 32
2.1. Soveltamisala 32
2.2. Osoitus 32
3. Yleiset määräykset 33
3.1. Tiedonsiirtoyhteyden arkkitehtuuri 33
3.1.1. Viestinvaihto 33
3.1.2. XML-viesti – Korkean tason kuvaus 33
3.1.3. Syöttöikkunat 33
3.1.4. Tapahtumaviestivirrat 34
3.2. Tiedonsiirron turvallisuus 36
3.2.1. Palomuuri ja verkkojen yhteenliitäntä 36
3.2.2. Virtuaalinen yksityisverkko (VPN) 36
3.2.3. IPSecin toteutus 37
3.2.4. Suojatun viestinvälityksen siirtoprotokolla. 37
3.2.5. XML-salaus ja -allekirjoitus 37
3.2.6. Salausavaimet 37
3.3. Yhteyteen liittyvien toimintojen luettelo 38
3.3.1. Käyttötapahtumat 38
3.3.2. Täsmäytysprotokolla 38
3.3.3. Testiviesti 39
3.4. Tietojen kirjaamista koskevat vaatimukset 39
3.5. Toiminnalliset vaatimukset 40
4. Saatavuutta koskevat määräykset 41
4.1. Tiedonsiirron saatavuuden suunnittelu 41
4.2. Käynnistys-, tiedonsiirto-, uudelleenaktivointi- ja testaussuunnitelma 41
4.2.1. Sisäisen tieto- ja viestintätekniikan infrastruktuurin testit 42

4.2.2. Tiedonsiirtotestit 42
4.2.3. Täyden järjestelmän testit (päästä päähän -testit) 42
4.2.4. Tietoturvatestit 42
4.3. Hyväksyntä-/testausympäristöt 43
5. Luottamuksellisuutta ja eheyttä koskevat määräykset 43
5.1. Tietoturvan testausinfrastruktuuri 43
5.2. Yhteyden keskeyttämistä ja uudelleenaktivointia koskevat määräykset 44
5.3. Tietoturvaloukkauksia koskevat määräykset 45
5.4. Tietoturvatestausta koskevat ohjeet 45
5.4.1. Ohjelmisto 45
5.4.2. Infrastruktuuri 45
5.5. Riskinarviointia koskevat määräykset 45

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 jommankumman osapuolen päästökauppajärjestelmän vaatimusten täyttämiseksi.
CH	Sveitsin valaliitto
CHU	Sveitsin myöntämä kiinteän laitoksen päästöoikeus, tunnetaan myös nimellä CHU2 (viittaus Kioton pöytäkirjan toiseen velvoitekauteen)
CHUA	Sveitsin ilmailun päästöoikeus
COP	Yhteiset toiminnalliset menettelyt Yhteisesti kehitetyt menettelyt, joilla EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välinen yhteys saadaan toiminnalliseksi.
ETR	Päästökaupparekisteri
ETS	Päästökauppajärjestelmä
EU	Euroopan unioni
EUA	EU:n yleinen päästöoikeus

Lyhenne/termi	Määritelmä
EUAA	EU:n ilmailun päästöoikeus
EUCR	Euroopan unionin konsolidoitu rekisteri
EUTL	Euroopan unionin tapahtumaloki
Rekisteri	Päästökauppajärjestelmässä myönnettyjen päästöoikeuksien kirjanpitojärjestelmä, jolla seurataan, kuka omistaa sähköisillä tileillä olevat päästöoikeudet.
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.
Varmentaja (Certification Authority)	Taho, joka myöntää digitaalisia varmenteita
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-tietoturva 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	XML-merkintäkieli (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’. EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välisen yhteyden toteuttamiseksi luodaan suora yhteys unionin rekisterin Euroopan unionin tapahtumalokin (EUTL) ja Sveitsin rekisterin täydentävän tapahtumalokin (SSTL) välillä, mikä mahdollistaa kummassa tahansa osapuolten päästökauppajärjestelmässä myönnettyjen päästöoikeuksien siirron rekisterien välillä (sopimuksen 3 artiklan 2 kohta). EU:n päästökauppajärjestelmän ja Sveitsin päästökauppajärjestelmän välisen yhteyden toteuttamiseksi otettiin käyttöön väliaikainen ratkaisu vuonna 2020. Vuodesta 2023 alkaen näiden kahden päästökauppajärjestelmän välinen rekisteriyhteys kehittyy asteittain pysyväksi rekisteriyhteydeksi, joka on tarkoitus panna täytäntöön viimeistään vuonna 2024 ja joka mahdollistaa toisiinsa yhteydessä olevien markkinoiden toiminnan markkinoiden likviditeetistä saatavien hyötyjen ja kahden toisiinsa liitetyn järjestelmän välisten tapahtumien toteuttamisen tavalla, joka vastaa kahdesta järjestelmästä koostuvia yksiä markkinoita ja antaa markkinaosapuolille mahdollisuuden toimia ikään kuin yksillä markkinoilla, jollei osapuolten erillisistä säännöksistä muuta johdu (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.

Sekakomitea hyväksyi LTS-standardit päätöksellään N:o 2/2020. Sekakomitea hyväksyy tässä asiakirjassa esitetyt päivitetyt LTS-standardit päätöksellään N:o 1/2024. Tämän päätöksen ja sekakomitean pyyntöjen mukaisesti Sveitsin rekisterinvalvoja ja unionin keskusvalvoja ovat laatineet tarkemmat tekniset ohjeet, jotka pidetään ajan tasalla ja 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 sekakomitean päätöksellä.

2.2. Osoitus

Tämä asiakirja on osoitettu Sveitsin rekisterinvalvojalle ja unionin rekisterin 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 toiminnallisuuden yleisarkkitehtuuri.

Koska tietoturva on keskeinen osa arkkitehtuurivaatimuksia, arkkitehtuurista on pyritty tekemään kaikin mahdollisin tavoin vakaa ja suojattu. Pysyvässä rekisteriyhteydessä käytetään tiedostojenvaihtomekanismia turvallisen ilmaväliyhteyden (Air Gap) avulla.

Teknisessä ratkaisussa käytetään seuraavia:

- Suojatun viestinvälityksen siirtoprotokolla.
- XML-viestit.
- XML-pohjainen digitaalinen allekirjoitus ja salaus.
- VPN.

Seuraavassa kaaviossa esitetään yleiskatsaus pysyvän rekisteriyhteyden arkkitehtuuriin:

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 puuttuvat 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

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

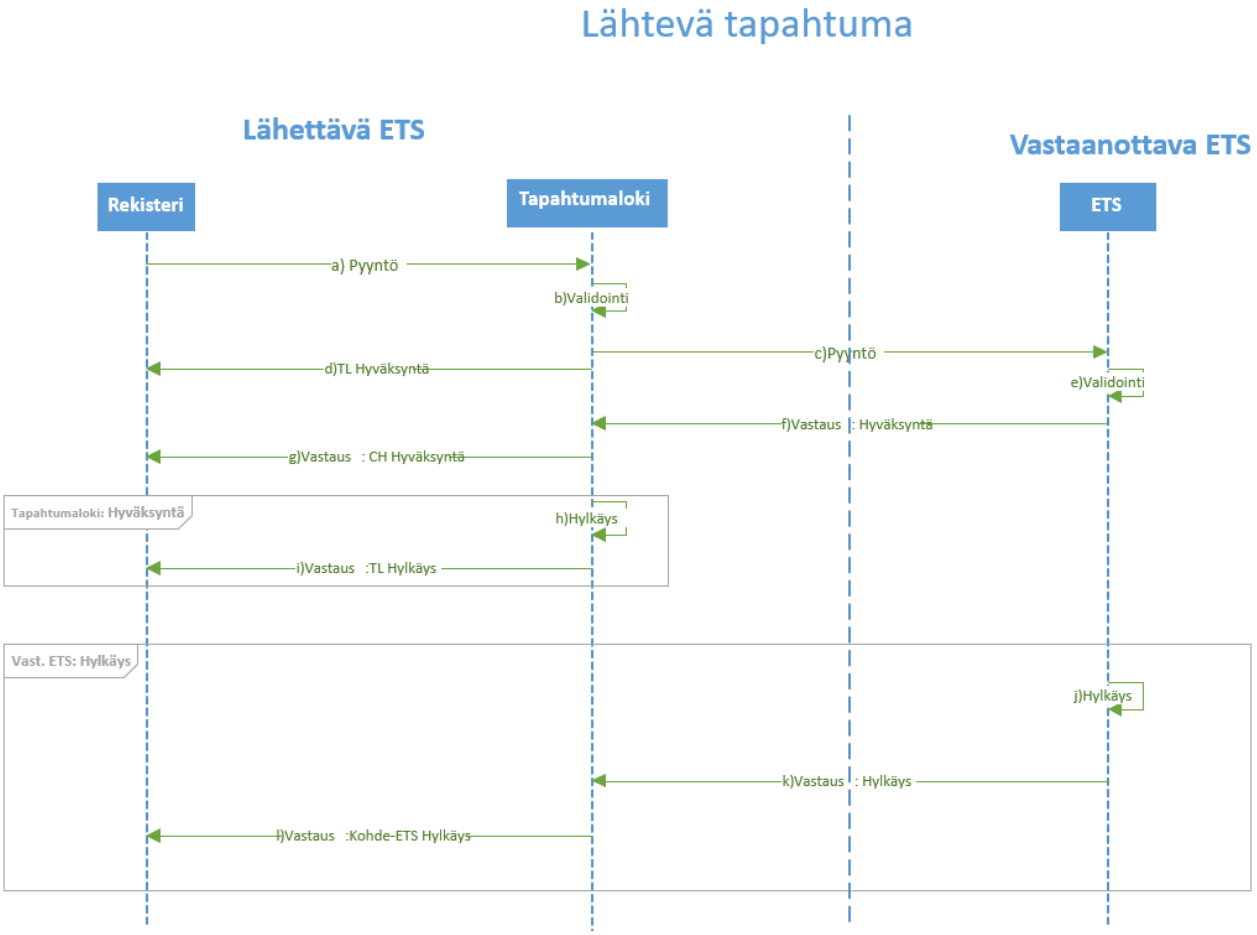
Muutoksia näiden tapahtumien ajoituksessa ja/tai tiheydessä käsitellään noudattaen

toiminnallisia menettelyjä, jotka on vahvistettu COP:n palvelupyyntöprosessissa.

3.1.4. Tapahtumaviestivirrat

Lähtevät tapahtumat

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



Päävirrassa näkyvät seuraavat vaiheet (kuten 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” (Tapahtumaloki hylkäys) (kuten edellä olevassa piirroksessa, alkaen a) päävirrasta):

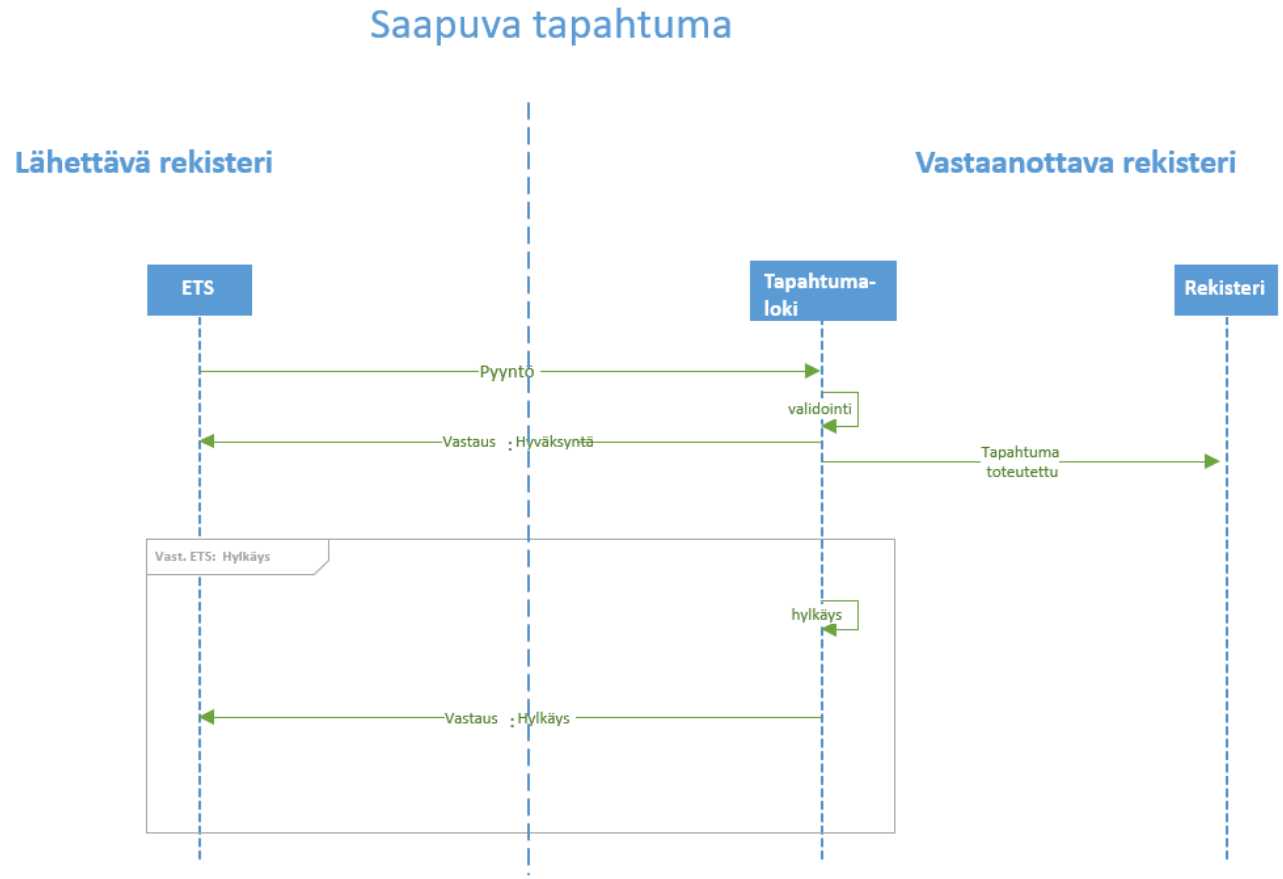
(a) Alkuperäjärjestelmässä tapahtumapyyntö lähetetään rekisteristä tapahtumalokiin heti, kun kaikki toiminnalliset viiveet ovat ohi (soveltuvin osin 24 tunnin viive).

(b) Tapahtumaloki ei validoi pyyntöä.
(c) Hylkäämisviesti lähetetään alkuperäiseen rekisteriin.

Vaihtoehtoinen virta ”ETS Rejection” (ETS hylkäys) (kuten edellä olevassa piirroksessa, alkaen d) päävirrasta):

(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.
(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” (tapahtuma toteutettu) vastaanottavan ETS:n rekisteriin.

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

Protokolla

Tapahtumaviestisyklissä on vain kaksi viestiä:

- Lähettävä ETS → Vastaanottava ETS Tapahtumapyyntö.
- Vastaanottava ETS → Lähettävä ETS Vastaus: Joko hyväksytty (”Accepted”) tai hylätty (”Rejected”) (mukaan lukien hylkäämisen syy).
  - Hyväksytty: Tapahtuma on toteutettu onnistuneesti.
  - Hylätty: Tapahtuma on keskeytetty.

Tapahtumatila

- Lähettävässä ETS:ssä tapahtumatilaksi asetetaan ”proposed” (pyydetty), kun pyyntö lähetetään.
- Vastaanottavassa ETS:ssä tapahtumatilaksi asetetaan ”proposed” (pyydetty), kun pyyntö on vastaanotettu ja kun sitä käsitellään.
- Vastaanottavassa ETS:ssä tapahtumatilaksi asetetaan ”completed”/”terminated” (toteutettu/päätetty), kun ehdotus on käsitelty. Vastaanottava ETS lähettää tämän jälkeen vastaavan hyväksymis-/hylkäämisviestin.
- Pyynnön lähettäneessä ETS:ssä tapahtumatilaksi asetetaan ”completed”/”terminated” (toteutettu/päätetty), kun hyväksymis-/hylkäämisviesti on vastaanotettu ja käsitelty.
- Pyynnön lähettäneessä ETS:ssä tapahtumatilana pysyy ”proposed” (pyydetty) myös siinä tapauksessa, että vastausta ei saada.
- Vastaanottavassa ETS:ssä kaikki tapahtumat, jotka ovat olleet tilassa ”proposed” (pyydetty) yli 30 minuuttia, siirtyvät tapahtumatilaan ”terminated” (päätetty).

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.

(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 VPN-teknologiaa. 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.

Euroopan unioni käyttää yleensä suojattuja Euroopan laajuisia julkishallinnon telematiikkapalveluja (sTESTA) yksityisenä IP-verkkona. Tämä verkko soveltuu myös pysyvään rekisteriyhteyteen.

3.2.3. IPSecin toteutus

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.

Pysyvä rekisteriyhteys perustuu useisiin salauskerroksiin, joiden avulla osapuolet voivat turvallisesti vaihtaa tietoja. Sekä järjestelmät ja niiden tekniset ympäristöt on yhteenliitetty verkkokerroksessa VPN-tunneleiden kautta. Sovelluskerroksessa tiedostot siirretään käyttäen suojattua viestiensiirtoprotokollaa 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 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. Ajastettu täsmäytys on kuitenkin toteutettava vähintään kunkin tulkinnan jälkeen.

Kumpi tahansa osapuoli voi kuitenkin 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. 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. Varmistetaan molempien päästökauppajärjestelmien välillä.

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” (hyväksytty) tai ”Discrepancies” (poikkeamia). Pysyvässä rekisteriyhteydessä täsmäytyssanomat ovat erottamaton osa vaihdettuja viestejä, joten ne tallennetaan kohdassa ”Viestiarkisto” kuvatulla tavalla.

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.

3.5. Toiminnalliset vaatimukset

Tietojenvaihto näiden kahden järjestelmän välillä ei pysyvässä rekisteriyhteydessä ole täysin automatisoitua, joten yhteys edellyttää manuaalisia toimenpiteitä ja menettelyjä. Tässä prosessissa esitetään tätä varten useita rooleja ja välineitä.

4. SAATAVUUTTA KOSKEVAT MÄÄRÄYKSET

4.1. Tiedonsiirron saatavuuden suunnittelu

Pysyvän yhteyden 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 keskeinen näkökohta, joka on otettava huomioon 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 pysyvässä yhteydessä otetaan käyttöön vakaa VPN-verkko, 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

Pysyvässä rekisteriyhteydessä tietoja vaihdetaan osapuolten välillä ennalta määrättyinä ajankohtina. 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 aika-ikkunat kunkin vaiheen suorittamista varten;
- pysyvän rekisteriyhteyden 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 pysyvän rekisteriyhteyden 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 pysyvän rekisteriyhteyden 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 rekisterinvalvoja 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 testit saatetaan päätökseen yhteistyössä toisen pään kanssa.

Kun yksittäiset elementit ovat toimintakykyisiä, testataan rekisterien väliset tiedonsiirtokanavat. Tätä varten kumpikin osapuoli tarkistaa, että internetyhteys toimii, VPN-tunnelit 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 rekisterinvalvojat suorittavat ja/tai käynnistävät nämä testit kummassakin päässä osioissa ”Tietoturvatestausta koskevat ohjeet” ja ”Riskinarviointia koskevat määräykset” täsmennetyillä tavoilla.

Vasta sen jälkeen, kun kukin neljästä vaiheesta/lohkosta on toteutettu ennakkoon oletetuin tuloksin, pysyvän 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: Pysyvän rekisteriyhteyden 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 ohjelmistoversioita.
- 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 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-kokoonpanon osalta kolmen ympäristön välisen viestinnän on oltava täysin riippumatonta, mikä varmistetaan käyttämällä STESTA-palveluja.

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, mutta sitä ei 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 ”Hyväksyntä-/Testausympäristöt”). Tähän periaatteeseen voidaan tehdä poikkeuksia molempien osapuolten suostumuksella.

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

Testausinfrastruktuuri on erotettava sekä verkko- että infrastruktuurikerroksessa tuotantoympäristöstä, ja 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, molempien osapuolten on välittömästi ilmoitettava asiasta toisilleen 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 uudelleenaktivoinnista tehdään COP:ssä täsmennetyn mukaisesti, ei kuitenkaan ennen kuin tietoturvatestausta koskevat menettelyt, jotka täsmennetään kohdissa ”Tietoturvatestausta koskevat ohjeet” ja ”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 osassa.

Tietoturvaloukkaukseen suoraan liittyviä tietoja pidetään arkaluonteisina, ne merkitään kuuluvaksi "SPECIAL HANDLING: *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 samalla periaatteella, joka määritellään edellisessä jaksossa, 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 "SPECIAL HANDLING: ETS Critical" käsittelyohjeiden mukaisesti.