2025/908

23.5.2025.

AR NOLĪGUMU STARP EIROPAS SAVIENĪBU UN ŠVEICES KONFEDERĀCIJU PAR SILTUMNĪCEFEKTA GĀZU EMISIJAS KVOTU TIRDZNIECĪBAS SISTĒMU SASAISTI IZVEIDOTĀS APVIENOTĀS KOMITEJAS LĒMUMS Nr. 1/2024

(2024. gada 4. decembris)

attiecībā uz Nolīguma II pielikuma un kopējo darbības procedūru un sasaistes tehnisko standartu grozīšanu [2025/908]

APVIENOTĀ KOMITEJA,

ņemot vērā Nolīgumu starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti ([1]) ("Nolīgums") un jo īpaši tā 9. pantu un 13. panta 2. punktu,

tā kā:

(1) Apvienotās komitejas Lēmums Nr. 2/2019 ([2]) paredzēja pagaidu risinājumu, ar kura palīdzību tika operacionalizēta ES ETS un Šveices ETS sasaiste.

(2) Trešajā sanāksmē Apvienotā komiteja vienojās, ka ir jāanalizē Savienības reģistra un Šveices reģistra pastāvīgas sasaistes izmakslietderība.

(3) Piektajā sanāksmē Apvienotā komiteja vienojās par ziņojumu, kuru iesniedza ar Apvienotās komitejas Lēmumiem Nr. 1/2020 ([3]) un Nr. 2/2020 ([4]) izveidotā darba grupa. Minētajā paziņojumā darba grupa bija analizējusi un ieteikusi pieeju, kā īstenot Savienības reģistra un Šveices reģistra pastāvīgo sasaisti.

(4) Lai atspoguļotu Savienības reģistra un Šveices reģistra pastāvīgās sasaistes tehniskās prasības, kā arī racionalizētu Nolīguma II pielikuma noteikumus, ņemot vērā tehnoloģiju attīstību, Nolīguma II pielikums būtu jāgroza.

(5) Lai nodrošinātu kopējo darbības procedūru un sasaistes tehnisko standartu konsekvenci ar Nolīguma II pielikumu, arī šie dokumenti būtu jāgroza,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

1. Nolīguma II pielikumu aizstāj tekstu šā lēmuma I pielikumā.

2. Nolīguma 3. panta 6. punktā minētās kopējās darbības procedūras ir izklāstītas šā lēmuma II pielikumā. Tās aizstāj Lēmuma Nr. 1/2020 pielikumā izklāstītās kopējās darbības procedūras.

([1]) OV L 322, 7.12.2017., 3. lpp.

([2]) Ar Nolīgumu starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti izveidotās Apvienotās komitejas Lēmums Nr. 2/2019 (2019. gada 5. decembris), ar ko groza Nolīguma starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti I un II pielikumu [2020/1359] (OV L 314, 29.9.2020., 68. lpp.).

([3]) Ar Nolīgumu starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti izveidotās Apvienotās komitejas Lēmums Nr. 1/2020 (2020. gada 5. novembris) par kopējo darbības procedūru pieņemšanu [2021/1033] (OV L 226, 25.6.2021., 2. lpp.).

([4]) Ar Nolīgumu starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti izveidotās Apvienotās komitejas Lēmums Nr. 2/2020 (2020. gada 5. novembris) par Nolīguma I un II pielikuma grozīšanu un sasaistes tehnisko standartu (STS) pieņemšanu [2021/1034] (OV L 226, 25.6.2021., 16. lpp.).

3. Nolīguma 3. panta 7. punktā minētie sasaistes tehniskie standarti ir izklāstīti šā lēmuma III pielikumā. Tie aizstāj Lēmuma Nr. 2/2020 pielikumā izklāstītos sasaistes tehniskos standartus.

2. pants

Šis lēmums stājas spēkā tā pieņemšanas dienā.

Briselē, 2024. gada 4. decembrī

Apvienotās komitejas vārdā

sekretārs no Eiropas Savienības puses	*priekšsēdētāja*	*sekretārs no Šveices puses*
Ruben VERMEEREN	Beatriz YORDI	Thomas MEIER

I PIELIKUMS

"II PIELIKUMS

SASAISTES TEHNISKIE STANDARTI

Lai ES ETS un Šveices ETS sasaiste varētu darboties, 2020. gadā tika ieviests pagaidu risinājums. No 2023. gada abu emisijas kvotu tirdzniecības sistēmu reģistru sasaiste pakāpeniski tiks pārveidota par pastāvīgu reģistru sasaisti, un to paredzēts īstenot ne vēlāk kā 2024. gadā; tā nodrošinās, ka sasaistītie tirgi funkcionē attiecībā uz ieguvumiem no tirgus likviditātes, un dos iespēju izpildīt darījumus starp abām sasaistītajām sistēmām veidā, kas ir līdzvērtīgs vienam tirgum, kuru veido divas sistēmas, un kas tirgus dalībniekiem nodrošina iespēju rīkoties tā, it kā tie būtu vienā tirgū, uz kuru attiecas tikai atsevišķi Pušu regulatīvie noteikumi.

Sasaistes tehniskajos standartos (STS) ir apskatīti šādi elementi:

— komunikācijas līnijas arhitektūra,

— komunikācija starp *SSTL* un *EUTL*,

— datu pārsūtīšanas drošība,

— funkciju saraksts (darījumi, saskaņošana),

— transporta slāņa definīcija,

— datu reģistrēšanas prasības,

— darba kārtība (zvanu centrs, tehniskais atbalsts),

— komunikācijas aktivācijas plāns un testēšanas procedūra,

— drošības testēšanas procedūra.

STS norāda, ka administratoriem jāveic visi saprātīgie pasākumi, lai nodrošinātu, ka *SSTL*, *EUTL* un to sasaiste darbojas 24 stundas diennaktī un 7 dienas nedēļā un ka jebkādi traucējumi *SSTL*, *EUTL* un to sasaistē ir samazināti līdz minimumam.

STS nosaka papildu drošības prasības Šveices reģistram, *SSTL*, Savienības reģistram un *EUTL*, un tās tiek dokumentētas "drošības vadības plānā". Konkrētāk, STS nosaka, ka:

— ja ir aizdomas, ka Šveices reģistra, *SSTL*, Savienības reģistra vai *EUTL* drošība ir apdraudēta, abas Puses nekavējoties viena otru par to informē un aptur sasaisti starp *SSTL* un *EUTL*,

— ja noticis drošības pārkāpums, Puses apņemas nekavējoties savā starpā dalīties informācijā. Šveices reģistra administrators un Savienības centrālais administrators 24 stundu laikā pēc tam, kad drošības incidents atzīts par drošības pārkāpumu, savstarpēji apmainās ar ziņojumu ar incidenta aprakstu (datums, cēlonis, ietekme, novēršana), ciktāl ir pieejama tehniskā informācija.

STS izklāstītā drošības testēšanas procedūra tiek izpildīta gan pirms *SSTL* un *EUTL* komunikācijas līnijas izveidošanas, gan ikreiz, kad ir nepieciešama jauna *SSTL* vai *EUTL* versija vai laidums.

STS papildus ražošanas videi paredz divas testēšanas vides: izstrādāšanas vidi un akceptēšanas vidi.

Puses ar Šveices reģistra administratora un Savienības centrālā administratora starpniecību sniedz pierādījumus, ka iepriekšējo divpadsmit mēnešu laikā ir veikts to sistēmu neatkarīgs drošības novērtējums saskaņā ar STS noteiktajām drošības prasībām. Drošības testēšanu un jo īpaši ielaušanās testēšanu veic visiem jauniem, nozīmīgiem programmatūras laidumiem saskaņā ar STS noteiktajām prasībām. Ielaušanās testēšanu neveic ne programmatūras izstrādātājs, ne programmatūras izstrādātāja apakšuzņēmējs."

II PIELIKUMS

KOPĒJĀS DARBĪBAS PROCEDŪRAS (KPD) SASKAŅĀ AR 3. PANTA 6. PUNKTU NOLĪGUMĀ STARP EIROPAS SAVIENĪBU UN ŠVEICES KONFEDERĀCIJU PAR SILTUMNĪCEFEKTA GĀZU EMISIJAS KVOTU TIRDZNIECĪBAS SISTĒMU SASAISTI

Pastāvīgas reģistru sasaistes procedūras

Satura rādītājs

1. GLOSĀRIJS 7
2. IEVADS 7
2.1. Tvērums 8
2.2. Adresāti 8
3. PIEEJA UN STANDARTI 8
4. INCIDENTU PĀRVALDĪBA 9
4.1. Incidentu konstatēšana un reģistrēšana 9
4.2. Klasificēšana un sākotnējais atbalsts 9
4.3. Izmeklēšana un diagnostika 10
4.4. Atrisināšana un atkopšana 10
4.5. Incidenta slēgšana 10
5. PROBLĒMU PĀRVALDĪBA 11
5.1. Problēmas identificēšana un reģistrēšana 11
5.2. Problēmu prioritizēšana 11
5.3. Problēmas izmeklēšana un diagnostika 11
5.4. Atrisinājums 11
5.5. Problēmas slēgšana 11
6. PIEPRASĪJUMA IZPILDE 11
6.1. Pieprasījuma iniciēšana 11
6.2. Pieprasījuma reģistrēšana un analīze 12
6.3. Pieprasījuma apstiprināšana 12
6.4. Pieprasījuma izpilde 12
6.5. Pieprasījuma eskalēšana 12
6.6. Pieprasījuma izpildes izskatīšana 12
6.7. Pieprasījuma slēgšana 12
7. IZMAIŅU PĀRVALDĪBA 12
7.1. Izmaiņas pieprasījums 13
7.2. Izmaiņas izvērtēšana un plānošana 13
7.3. Izmaiņas apstiprināšana 13
7.4. Izmaiņas īstenošana 13
8. LAIDUMU VADĪBA 13
8.1. Laiduma plānošana 14
8.2. Laiduma paketes kompilēšana un testēšana 14
8.3. Ieviešanas sagatavošana 14
8.4. Laiduma atrite 15

8.5. Laiduma izskatīšana un noslēgšana 15
9. DROŠĪBAS INCIDENTU PĀRVALDĪBA 15
9.1. Informācijas drošības incidentu kategorizācija 15
9.2. Rīkošanās informācijas drošības incidentu gadījumā 15
9.3. Drošības incidenta identificēšana 16
9.4. Drošības incidenta analīze 16
9.5. Drošības incidentu smaguma novērtējums, eskalēšana un ziņošana 16
9.6. Ziņošana par drošības incidentu 16
9.7. Monitorings, kapacitātes veidošana un pastāvīgi uzlabojumi 16
10. INFORMĀCIJAS DROŠĪBAS PĀRVALDĪBA 17
10.1. Sensitīvas informācijas identificēšana 17
10.2. Informācijas aktīvu sensitivitātes pakāpes 17
10.3. Informācijas aktīvu īpašnieka nozīmēšana 17
10.4. Sensitīvas informācijas reģistrēšana 17
10.5. Rīkošanās ar sensitīvu informāciju 18
10.6. Piekļuves pārvaldība 18
10.7. Sertifikātu/atslēgu pārvaldība 18

1. **GLOSĀRIJS**

1.1. tabula.

Akronīmi un definīcijas

Akronīms/termins	Definīcija
Sertificētājs (*CA*)	Iestāde, kas izdod digitālos sertifikātus
CH	Šveices Konfederācija
ETS	Emisijas kvotu tirdzniecības sistēma
ES	Eiropas Savienība
IMT	Incidentu pārvaldības vienība
Informācijas aktīvs	Uzņēmumam vai organizācijai vērtīga informācija
IT	Informācijas tehnoloģijas
ITIL	Informācijas tehnoloģiju infrastruktūras bibliotēka
ITSM	IT pakalpojumu pārvaldība
STS	Sasaistes tehniskie standarti
Reģistrs	Uzskaites sistēma, kurā uzskaita ETS ietvaros iedalītās kvotas un kura ļauj izsekot elektroniskajos kontos turēto kvotu īpašumtiesībām
RFC	Izmaiņas pieprasījums
SIL	Sensitīvas informācijas saraksts
SR	Pakalpojuma pieprasījums
Wiki	Tīmekļvietne, kas dod iespēju lietotājiem dalīties informācijā un zināšanās, saturu papildinot vai pielāgojot tieši tīmekļa pārlūkprogrammā

2. **IEVADS**

2017. gada 23. novembrī noslēgtais Nolīgums starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti ("Nolīgums") paredz savstarpēji atzīt emisijas kvotas, ko var izmantot, lai panāktu atbilstību Eiropas Savienības emisijas kvotu tirdzniecības sistēmā (ES ETS) vai Šveices emisijas kvotu tirdzniecības sistēmā (Šveices ETS). Lai ES ETS un Šveices ETS sasaiste varētu darboties, starp Savienības reģistra Eiropas Savienības darījumu žurnālu (*EUTL*) un Šveices reģistra Šveices papildu darījumu žurnālu (*SSTL*) tiks izveidota tieša sasaiste, kas dos iespēju katras ETS ietvaros izdotās kvotas pārskaitīt no viena reģistra uz otru (Nolīguma 3. panta 2. punkts). Lai ES ETS un Šveices ETS sasaiste varētu darboties 2020. gadā tika ieviests pagaidu risinājums. No 2023. gada abu emisijas kvotu tirdzniecības sistēmu reģistru sasaiste pakāpeniski tiks pārveidota par pastāvīgu reģistru sasaisti, un to paredzēts īstenot ne vēlāk kā 2024. gadā; tā nodrošinās, ka sasaistītie tirgi funkcionē attiecībā uz ieguvumiem no tirgus likviditātes, un dos iespēju izpildīt darījumus starp abām sasaistītajām sistēmām veidā, kas ir līdzvērtīgs vienam tirgum, kuru veido divas sistēmas, un kas tirgus dalībniekiem nodrošina iespēju rīkoties tā, it kā tie būtu vienā tirgū, uz kuru attiecas tikai atsevišķi Pušu regulatīvie noteikumi (Nolīguma II pielikums).

Saskaņā ar Nolīguma 3. panta 6. punktu Šveices reģistra administrators un Savienības centrālais administrators nosaka kopējās darbības procedūras (KDP), kas saistītas ar tehniskiem vai citiem jautājumiem un ir vajadzīgas, lai nodrošinātu sasaistes funkcionēšanu, tostarp ņemot vērā iekšējos tiesību aktos izklāstītās prioritātes. Administratoru izstrādātās KDP stājas spēkā, kad tās ir pieņemtas ar Apvienotās komitejas lēmumu.

Apvienotā komiteja KDP pieņēma ar Lēmumu Nr. 1/2020. Šajā dokumentā izklāstītās atjauninātās KDP Apvienotā komiteja pieņems ar Lēmumu Nr. 1/2024. Saskaņā ar šo lēmumu un Apvienotās komitejas lūgumiem Šveices reģistra administrators un Savienības centrālais administrators ir izstrādājuši sīkākas tehniskās vadlīnijas, kas nepieciešamas, lai nodrošinātu sasaistes funkcionēšanu, tās pastāvīgu pielāgošanu tehnikas attīstībai un jaunām prasībām, kas saistītas ar sasaistes drošumu un drošību, un tās rezultatīvu un efektīvu darbību, un atjauninās tās.

2.1. **Tvērums**

Šis dokuments atspoguļo Nolīguma pušu kopīgo izpratni par ES ETS un Šveices ETS reģistru sasaistes procedurālā pamata izveidi. Tajā izklāstītas vispārējās procedurālās prasības attiecībā uz sasaistes operācijām, tomēr būs vajadzīgas arī sīkākas tehniskas vadlīnijas, lai sasaiste varētu darboties.

Lai tā varētu pienācīgi funkcionēt, būs jānosaka sasaistes darbības tehniskās specifikācijas. Saskaņā ar Nolīguma 3. panta 7. punktu šie jautājumi tiks iztirzāti sasaistes tehnisko standartu (STS) dokumentā, ko Apvienotā komiteja pieņems atsevišķi ar attiecīgu lēmumu.

KDP mērķis ir nodrošināt, ka IT pakalpojumi, kas saistīti ar ES ETS un Šveices ETS reģistru sasaistes darbību, tiek sniegti rezultatīvi un efektīvi, proti, ka tiek izpildīti pakalpojuma pieprasījumi, novērstas pakalpojumu atteices, atrisinātas problēmas un ka rutīnas operacionālie uzdevumi tiek izpildīti saskaņā ar starptautiskajiem IT pakalpojumu pārvaldības standartiem.

Ierosinātajam pagaidu risinājumam būs vajadzīgas tikai šādas KDP, kas ir daļa no šā dokumenta:

— incidentu pārvaldība,

— problēmu pārvaldība,

— pieprasījumu izpilde,

— izmaiņu pārvaldība,

— laidumu vadība,

— drošības incidentu pārvaldība,

— informācijas drošības pārvaldība.

2.2. **Adresāti**

KDP mērķauditorija ir ES un Šveices reģistru atbalsta vienības.

3. **PIEEJA UN STANDARTI**

Uz visām KDP attiecas šāds princips:

— ES un CH vienojas KDP definēt, pamatojoties uz *ITIL* (Informācijas tehnoloģiju infrastruktūras bibliotēka, 4. versija). Šajā standartā paredzēto praksi izmanto un pielāgo specifiskajām vajadzībām, kas saistītas ar pastāvīgu reģistru sasaisti;

— saziņa un koordinācija, kas nepieciešama, lai KDP ieviestu abas puses, notiek ar CH un ES reģistru apkalpošanas dienestu starpniecību. Uzdevumus allaž piešķir vienas puses ietvaros;

— ja rodas domstarpības par KDP izmantošanu, tās analizē un atrisina abi apkalpošanas dienesti savā starpā. Ja vienošanos panākt neizdodas, kopīga risinājuma meklēšanu nodod nākamajam līmenim;

Eskalācijas līmeņi	ES	CH
1. līmenis	ES apkalpošanas dienests	CH apkalpošanas dienests
2. līmenis	ES operāciju vadītājs	CH reģistra lietojumu vadītājs
3. līmenis	Apvienotā komiteja (kas šo atbildību var deleģēt saskaņā ar nolīguma 12. panta 5. punktu)	
4. līmenis	Apvienotā komiteja, ja 3. līmenī atbildība tikusi deleģēta	

— katra puse var noteikt savas reģistra sistēmas darbības procedūras, ņemot vērā ar šīm KDP saistītās prasības un saskarnes;

— KDP atbalstam, jo īpašu incidentu pārvaldības, problēmu pārvaldības un pieprasījumu izpildes aspektā, un saziņai starp abām pusēm izmanto IT pakalpojumu pārvaldības (*ITSM*) rīku;

— ir atļauta informācijas apmaiņa pa e-pastu;

— abas puses nodrošina, ka tiek izpildītas informācijas drošības prasības saskaņā ar rīkošanās instrukcijām.

4. **INCIDENTU PĀRVALDĪBA**

Incidentu pārvaldības procesa mērķis ir panākt, ka IT pakalpojumi pēc incidenta iespējami ātri un ar minimāliem darbības traucējumiem atsāk darboties normālā pakalpojumu sniegšanas režīmā.

Incidentu pārvaldības gaitā incidenti tiek fiksēti ziņošanas vajadzībām, un incidentu pārvaldību integrē ar pārējiem procesiem, lai sekmētu pastāvīgus uzlabojumus.

Vispārīgā skatījumā incidentu pārvaldība sastāv no šādām darbībām:

— incidentu konstatēšana un reģistrēšana,

— klasificēšana un sākotnējais atbalsts,

— izmeklēšana un diagnostika,

— atrisināšana un atkopšana,

— incidenta slēgšana.

Visā incidenta ciklā incidentu pārvaldības procesam ir pastāvīgi jānodrošina īpašumtiesību apstrāde, monitorings, izsekošana un saziņa.

4.1. **Incidentu konstatēšana un reģistrēšana**

Incidentu var konstatēt atbalsta grupa, automatizēti monitoringa rīki vai tehniskais personāls, kas nodarbojas ar rutīnas pārraudzību.

Kad incidents ir konstatēts, tas ir jāreģistrē un tam jāpiešķir unikāls identifikators, lai būtu iespējama pienācīga incidenta izsekošana un monitorings. Incidenta unikālais identifikators ir identifikators, ko kopējā pretenziju sistēmā piešķir tās puses (ES vai CH) apkalpošanas dienests, kas signalizējusi par incidentu, un tas ir jāizmanto jebkādā saziņā par šo incidentu.

Visiem incidentiem kontaktpunkts ir tās puses apkalpošanas dienests, kas pretenziju reģistrējusi.

4.2. **Klasificēšana un sākotnējais atbalsts**

Incidentu klasificēšanas mērķis ir izprast un identificēt, kādas sistēmas un/vai pakalpojumus incidents skāris un kādā mērā. Lai klasifikācija būtu lietderīga un paātrinātu incidenta atrisināšanu, tai jau ar pirmo mēģinājumu incidents jānovirza uz pareizo resursu.

Klasificēšanas posmā incidents jākategorizē un jāprioritizē atkarībā no ietekmes un steidzamības, lai to varētu risināt tā prioritātei atbilstošā termiņā.

Ja incidents var potenciāli ietekmēt sensitīvu datu konfidencialitāti vai integritāti un/vai ietekmēt sistēmas pieejamību, incidents jāklasificē arī kā drošības incidents un tā pārvaldībai jānorit saskaņā ar procesu, kas definēts šā dokumenta nodaļā "Drošības incidentu pārvaldība".

Ja iespējams, sākotnējo diagnostiku veic apkalpošanas dienests, kas reģistrējis pretenziju. Lai to izdarītu, apkalpošanas dienests vispirms noskaidros, vai incidents nav jau zināma kļūda. Tādā gadījumā risināšanas gaita vai aprisinājums jau ir zināms un dokumentēts.

Ja apkalpošanas dienests incidentu ir sekmīgi atrisinājis, tas šajā brīdī faktiski incidentu slēdz, jo ir izpildīts incidentu pārvaldības primārais uzdevums (proti, pakalpojuma nodrošināšana galalietotājam ir ātri atjaunota). Pretējā gadījumā apkalpošanas dienests incidentu eskalē līdz piemērotai risinātāju grupai tālākai izmeklēšanai un diagnostikai.

4.3. **Izmeklēšana un diagnostika**

Incidentu izmeklēšanu un diagnostiku izmanto tad, kad incidentu nevar atrisināt apkalpošanas dienests sākotnējā diagnosticēšanā un tas tiek pienācīgi eskalēts. Incidentu eskalācija ir izmeklēšanas un diagnostikas procesa pilnvērtīga daļa.

Ierasta prakse izmeklēšanas un diagnostikas posmā ir mēģinājums reproducēt incidentu kontrolētos apstākļos. Incidenta izmeklēšanas un diagnostikas gaitā ir ļoti svarīgi izprast to notikumu secību, kas pie incidenta noveduši.

Eskalācija nozīmē atzīt, ka incidentu nevar atrisināt pašreizējā atbalsta līmenī un ka tas ir jānodod augstāka līmeņa atbalsta grupai vai otrai pusei. Eskalācija var būt divējāda: horizontāla (funkcionāla) vai vertikāla (hierarhiska).

Eskalēt incidentu līdz piemērotam resursam un sekot līdzi incidenta statusam un piešķiršanai ir incidentu reģistrējušā un ierosinājušā apkalpošanas dienesta pienākums.

Pienākums nodrošināt, ka prasītās darbības tiek veiktas savlaicīgi, un nodrošināt atgriezenisko saisti savam apkalpošanas dienestam, ir tās puses uzdevums, kurai incidents piešķirts.

4.4. **Atrisināšana un atkopšana**

Incidentu atrisināšana un atkopšana notiek, kad incidents ir pilnībā izprasts. Incidenta risinājuma atrašana nozīmē, ka ir uziets veids, kā problēmu novērst. Incidenta risinājuma piemērošana ir atkopšanas posms.

Kad attiecīgie resursi ir pakalpojuma atteici atrisinājuši, incidentu novirza atpakaļ attiecīgajam apkalpošanas dienestam, kurš incidentu reģistrējis, un šis apkalpošanas dienests vēršas pie incidenta iniciatora, lai pārliecinātos, ka kļūda ir novērsta un ka incidentu var slēgt. Incidenta apstrādes gaitā izdarītie konstatējumi ir jāfiksē, jo tie varētu noderēt turpmāk.

Atkopšanu var veikt IT atbalsta darbinieki vai arī galalietotājs, kam dod norādījumus, kā to izdarīt.

4.5. **Incidenta slēgšana**

Slēgšana ir incidentu pārvaldības pēdējais posms un notiek neilgi pēc incidenta atrisināšanas.

Slēgšanas posmā ir jāveic virkne darbību, no kurām īpaši izceļamas šādas:

— verificēt incidentam sākotnēji piešķirto kategoriju,

— pienācīgi fiksēt visu informāciju par incidentu,

— pienācīgi dokumentēt incidentu un atjaunināt zināšanu bāzi,

— pienācīgi sazināties ar visām ieinteresētajām personām, ko tieši vai netieši skāris incidents.

Incidentu formāli slēdz tad, kad apkalpošanas dienests ir pabeidzis incidenta slēgšanas posmu un par to paziņojis otrai pusei.

Kad incidents ir slēgts, to vairs neatver. Ja incidents pēc neilga laika atkārtojas, reģistrē jaunu incidentu, nevis vēlreiz atver sākotnējo incidentu.

Ja incidentam seko līdzi gan ES, gan CH apkalpošanas dienesti, incidenta galīgā slēgšana ir tā apkalpošanas dienesta pienākums, kas pretenziju reģistrējis.

5. **PROBLĒMU PĀRVALDĪBA**

Šī procedūra ir jāievēro ikreiz, kad tiek identificēta problēma, kas savukārt ierosina problēmu pārvaldības procesu. Problēmu pārvaldības galvenais uzdevums ir uzlabot kvalitāti un samazināt incidentu skaitu. Problēma var būt viena vai vairāku incidentu cēlonis. Kad tiek ziņots par incidentu, incidentu pārvaldības mērķis ir pakalpojumu pēc iespējas ātrāk atjaunot, izmantojot arī aprisinājumus. Kad problēma reģistrēta, mērķis ir izpētīt problēmas pamatcēloni, lai noskaidrotu, kādas izmaiņas vajadzīgas, lai nodrošinātu, ka problēma un ar to saistītie incidenti vairs nenotiek.

5.1. **Problēmas identificēšana un reģistrēšana**

Atkarībā no tā, kura puse ierosinājusi pretenziju, kontaktpunkts ar problēmu saistītajos jautājumos būs ES vai CH apkalpošanas dienests.

Problēmas unikālais identifikators ir identifikators, ko piešķir IT pakalpojumu pārvaldība (*ITSM*). To izmanto jebkādā saziņā par šo problēmu.

Problēmu var ierosināt incidents, vai arī to var ierosināt pēc pašu iniciatīvas, lai novērstu jebkurā laikā atklātas nepilnības.

5.2. **Problēmu prioritizēšana**

Lai problēmām varētu vieglāk izsekot, tās var iedalīt kategorijās pēc to smaguma un prioritātes tādā pašā veidā kā incidentus, ņemot vērā saistīto incidentu ietekmi un biežumu.

5.3. **Problēmas izmeklēšana un diagnostika**

Katra puse var izvirzīt problēmu, un šīs puses apkalpošanas dienests būs atbildīgs par problēmas reģistrēšanu, tās novirzīšanu piemērotam resursam un sekošanu problēmas statusam kopumā.

Risinātāju grupa, kam problēma eskalēta, ir atbildīga par problēmas savlaicīgu risināšanu un saziņu ar apkalpošanas dienestu.

Pēc pieprasījuma – nodrošināt, ka piešķirtās darbības tiek veiktas, un nodrošināt atgriezenisko saiti savam apkalpošanas dienestam ir abu pušu uzdevums.

5.4. **Atrisinājums**

Par problēmas atrisināšanu ir atbildīga risinātāju grupa, kam problēma piešķirta, un tā ir atbildīga arī par to, ka grupas puses apkalpošanas dienestam tiek sniegta relevantā informācija.

Problēmas apstrādes gaitā izdarītie konstatējumi ir jāfiksē, jo tie varētu noderēt turpmāk.

5.5. **Problēmas slēgšana**

Problēma tiek formāli slēgta tad, kad tā ir novērsta, pateicoties ieviestām izmaiņām. Problēmas slēgšanas posmu realizē tas apkalpošanas dienests, kas problēmu reģistrēja un informēja otras puses apkalpošanas dienestu.

6. **PIEPRASĪJUMA IZPILDE**

Pieprasījuma izpildes procesa ietvaros no sākuma līdz beigām tiek pārvaldīti pieprasījumi pēc jauna vai esoša pakalpojuma, proti, no brīža, kad pieprasījums tiek reģistrēts un apstiprināts, līdz brīdim, kad tas tiek slēgts. Pakalpojuma pieprasījumi parasti ir nelieli, iepriekš definēti, atkārtojami, bieži, iepriekš apstiprināti un procedurāli pieprasījumi.

Galvenā darbību virkne ir šāda.

6.1. **Pieprasījuma iniciēšana**

Ar pakalpojuma pieprasījumu saistīto informāciju ES vai CH apkalpošanas dienestam iesniedz pa e-pastu, telefoniski, izmantojot IT pakalpojumu pārvaldības (*ITSM*) rīku vai citu norunātu saziņas kanālu.

6.2. **Pieprasījuma reģistrēšana un analīze**

Attiecībā uz visiem pakalpojuma pieprasījumiem kontaktpunkts ir ES vai CH apkalpošanas dienests atkarībā no tā, kura puse izvirzījusi pakalpojuma pieprasījumu. Šis apkalpošanas dienests ir atbildīgs par pakalpojuma pieprasījuma reģistrēšanu un rūpīgu analīzi.

6.3. **Pieprasījuma apstiprināšana**

Pakalpojuma pieprasījumu izvirzījušās puses apkalpošanas dienesta darbinieks pārbauda, vai ir vajadzīgs kāds apstiprinājums no otras puses, un, ja jā, rīkojas, lai to saņemtu. Ja pakalpojuma pieprasījums netiek apstiprināts, apkalpošanas dienests atjaunina un noslēdz pretenziju.

6.4. **Pieprasījuma izpilde**

Šajā posmā tiek rezultatīvi un efektīvi apstrādāti pakalpojuma pieprasījumi. Jānošķir šādi gadījumi:

— pakalpojuma pieprasījuma izpilde skar tikai vienu pusi. Tādā gadījumā šī puse izdod darba rīkojumus un koordinē izpildi,

— pakalpojuma pieprasījuma realizācija skar gan ES, gan CH. Tādā gadījumā apkalpošanas dienesti izdod darba rīkojumus savā atbildības jomā. Pakalpojuma pieprasījuma izpildes norisi savstarpēji koordinē abi apkalpošanas dienesti. Vispārējā atbildība gulstas uz to apkalpošanas dienestu, kas pakalpojuma pieprasījumu saņēmis un iniciējis.

Kad pakalpojuma pieprasījums ir atrisināts, tam jāpiešķir statuss “atrisināts”.

6.5. **Pieprasījuma eskalēšana**

Vēl neizpildītu pakalpojuma pieprasījumu apkalpošanas dienests vajadzības gadījumā var eskalēt un novirzīt attiecīgajam resursam (trešām personām).

Eskalācijas gaitā pieprasījumus novirza attiecīgajām trešām personām, t. i., ES apkalpošanas dienests pieprasījumu CH trešai pusei var novirzīt tikai ar CH apkalpošanas dienesta starpniecību un otrādi.

Trešā puse, kurai pakalpojuma pieprasījums novirzīts, ir atbildīga par pakalpojuma pieprasījuma savlaicīgu risināšanu un saziņu ar to apkalpošanas dienestu, kas pakalpojuma pieprasījumu eskalējis.

Pakalpojuma pieprasījumu reģistrējušā apkalpošanas dienesta pienākums ir kopumā sekot līdzi pakalpojuma pieprasījuma statusam un piešķiršanai.

6.6. **Pieprasījuma izpildes izskatīšana**

Pirms pakalpojuma pieprasījuma noslēgšanas atbildīgais apkalpošanas dienests pakalpojuma pieprasījuma protokolu nodod galīgajai kvalitātes kontrolei. Mērķis ir pārliecināties, ka pakalpojuma pieprasījums ir patiešām apstrādāts un ka pietiekami detalizēti ir sniegta visa informācija, kas nepieciešama, lai aprakstītu pieprasījuma ciklu. Turklāt pieprasījuma apstrādes gaitā izdarītie konstatējumi ir jāfiksē, jo tie varētu noderēt turpmāk.

6.7. **Pieprasījuma slēgšana**

Ja puses, kam pieprasījums piešķirts, vienojas, ka pakalpojuma pieprasījums ir izpildīts, un prasītājs uzskata, ka lieta ir atrisināta, nākamais pieprasījumam piešķiramais statuss ir “slēgts”.

Pakalpojuma pieprasījumu formāli slēdz pēc tam, kad pakalpojuma pieprasījumu reģistrējušais apkalpošanas dienests ir izpildījis pieprasījuma slēgšanas posmu un informējis otras puses apkalpošanas dienestu.

7. **IZMAIŅU PĀRVALDĪBA**

Mērķis ir nodrošināt, ka tiek izmantotas standartizētas metodes un procedūras, kā efektīvi un nekavējoties pārņemt kontroli pār visām izmaiņām, kas skar IT infrastruktūru, lai līdz minimumam samazinātu jebkādu saistīto incidentu skaitu un ietekmi uz pakalpojumiem. Izmaiņas IT infrastruktūrā var rasties reaktīvi – kā atbildes reakcija uz problēmām vai ārēji uzliktām prasībām, piemēram, normatīvo aktu grozījumiem – vai proaktīvi – lai uzlabotu efektivitāti un rezultativitāti vai atspoguļotu komerciālas iniciatīvas.

Izmaiņu pārvaldības process ietver dažādus posmus, kuru gaitā tiek fiksēta visa informācija par izmaiņas pieprasījumu, lai nākotnē būtu iespējams tam izsekot. Šie procesi nodrošina, ka izmaiņa pirms ieviešanas tiek validēta un testēta. Sekmīgu ieviešanu nodrošina laidumu vadības process.

7.1. **Izmaiņas pieprasījums**

Izmaiņas pieprasījumu (*RFC*) iesniedz izmaiņu pārvaldības vienībai validēšanai un apstiprināšanai. Attiecībā uz visiem izmaiņas pieprasījumiem kontaktpunkts ir ES vai CH apkalpošanas dienests atkarībā no tā, kura puse izvirzījusi izmaiņas pieprasījumu. Šis apkalpošanas dienests ir atbildīgs par izmaiņu pieprasījuma reģistrēšanu un rūpīgu analīzi.

Izmaiņas pieprasījumu iemesls var būt:

— incidents, kas izraisa izmaiņu,

— esoša problēma, kuras rezultātā rodas izmaiņa,

— galalietotāja pieprasījums pēc jaunas izmaiņas,

— izmaiņa, kas rodas notiekošas uzturēšanas rezultātā,

— leģislatīva izmaiņa.

7.2. **Izmaiņas izvērtēšana un plānošana**

Šajā posmā notiek izmaiņas novērtēšana un darbību plānošana. Tas ietver prioritizēšanu un darbību plānošanu nolūkā līdz minimumam samazināt risku un ietekmi.

Ja *RFC* realizācija skar gan ES, gan CH, puse, kas reģistrējusi *RFC*, izmaiņas izvērtēšanu un plānošanu verificē ar otru pusi.

7.3. **Izmaiņas apstiprināšana**

Visi reģistrētie izmaiņas pieprasījumi ir jāapstiprina attiecīgajā eskalācijas līmenī.

7.4. **Izmaiņas īstenošana**

Izmaiņas īstenošana notiek laidumu vadības procesā. Abu pušu laidumu vadības vienības ievēro pašas savas procedūras, kas ietver gan plānošanu, gan testēšanu. Izmaiņas izskatīšana notiek, kad īstenošana ir pabeigta. Lai nodrošinātu, ka viss ir paveikts saskaņā ar plānu, esošo izmaiņu pārvaldības procesu pastāvīgi izskata un vajadzības gadījumā atjaunina.

8. **LAIDUMU VADĪBA**

Laidums jeb izlaišana nozīmē vienu vai vairākas izmaiņas IT pakalpojumā, kas ir apkopotas laiduma plānā un kas ir jāautorizē, jāsagatavo, jākompilē, jātestē un jāievieš vienlaikus. Laidums var būt kļūdas izlabošana, aparatūras vai citu komponentu maiņa, izmaiņas programmatūrā, lietojumprogrammu versiju atjauninājumi, izmaiņas dokumentācijā un/vai procesos. Katra laiduma saturu pārvalda, testē un ievieš kā vienvienīgu vienumu.

Laidumu vadības mērķis ir plānot, kompilēt, testēt, validēt un nodrošināt spēju sniegt plānotos pakalpojumus tā, lai tie atbilstu ieinteresēto personu prasībām un sasniegtu iecerētos mērķus. Visu pakalpojumā ieviesto izmaiņu akceptēšanas kritēriji tiks definēti un dokumentēti projektēšanas koordinācijas laikā un nodoti laidumu vadības vienībām.

Laidums parasti sastāv no vairākiem problēmu labojumiem un pakalpojuma uzlabojumiem. Tas satur nepieciešamo jauno vai izmainīto programmatūru un jebkādu jaunu vai izmainītu aparatūru, kas nepieciešama apstiprināto izmaiņu ieviešanai.

8.1. **Laiduma plānošana**

Pirmajā procesa posmā autorizētās izmaiņas tiek sakopotas laiduma paketēs, kā arī tiek definēts laidumu tvērums un saturs. Balstoties uz šo informāciju, laiduma plānošanas apakšprocesa ietvaros tiek sagatavots laiduma kompilēšanas, testēšanas un ieviešanas grafiks.

Plānošanas gaitā definē šādus elementus:

— laiduma tvērums un saturs,

— laiduma riska novērtējums un riska profils,

— laiduma skartie klienti/lietotāji,

— par laidumu atbildīgā vienība,

— nodošanas un ieviešanas stratēģija,

— izlaišanai un ieviešanai vajadzīgie resursi.

Puses viena otru informē par saviem laidumu plānošanas un uzturēšanas logiem. Ja laidums ietekmē gan ES, gan CH, tās koordinē plānošanu un definē kopīgu uzturēšanas logu.

8.2. **Laiduma paketes kompilēšana un testēšana**

Laidumu vadības procesa kompilēšanas un testēšanas posmā tiek noteikta pieeja, kā realizēt laidumu vai laiduma paketi un kā saglabāt kontroli pār vidi pirms ražošanas maiņas, un kā testēt visas izmaiņas visās laiduma vidēs.

Ja laidums ietekmē gan ES, gan CH, tās koordinē nodošanas plānus un testus. Tas ietver šādus aspektus:

— kā un kad tiks nodoti laiduma vienumi un pakalpojuma komponenti,

— kādi ir tipiskie izpildes laiki, kas notiek kavēšanās gadījumā,

— kā izsekot nodošanas progresam un saņemt apstiprinājumu,

— kādu metriku izmantot laiduma ieviešanas monitoringā un sekmīguma novērtēšanā,

— kādi ir izplatītākie testpiemēri, ko izmanto relevantajai funkcionalitātei un izmaiņām.

Šī apakšprocesa noslēgumā visi vajadzīgie laiduma komponenti ir gatavi faktiskajam ieviešanas posmam.

8.3. **Ieviešanas sagatavošana**

Sagatavošanas apakšprocess nodrošina, ka tiek pareizi definēti komunikācijas plāni un ka ir sagatavoti paziņojumi, kas izsūtāmi visām skartajām ieinteresētajām personām un galalietotājiem, un ka laidums tiek integrēts izmaiņu pārvaldības procesā, lai nodrošinātu, ka visas izmaiņas tiek izdarītas kontrolēti un ir apstiprinātas attiecīgajos forumos.

Ja laidums skar gan ES, gan CH, tās koordinē šādas darbības:

— izmaiņas pieprasījuma protokola sagatavošana nolūkā ieplānot un sagatavot ieviešanu ražošanas vidē,

— īstenošanas plāna sagatavošana,

— atrites pieeja, lai gadījumā, ja ieviešana ir kļūmīga, var atjaunot iepriekšējo stāvokli,

— paziņojumu izsūtīšana visām attiecīgajām pusēm,

— laiduma īstenošanai vajadzīgā apstiprinājuma pieprasīšana attiecīgajā eskalācijas līmenī.

8.4. **Laiduma atrite**

Ja ieviešana ir kļūmīga vai testēšanā ir noskaidrojies, ka ieviešana nav bijusi sekmīga vai nav atbildusi norunātajiem akceptēšanas/kvalitātes kritērijiem, abu pušu laiduma vadības vienībām ir jānodrošina atrite iepriekšējā stāvoklī. Par to jāinformē visas attiecīgās ieinteresētās personas, toskait skartie/aptvertie galalietotāji. Kamēr nav saņemts apstiprinājums, procesu var atsākt jebkurā no iepriekšējiem posmiem.

8.5. **Laiduma izskatīšana un noslēgšana**

Izskatot, kā izdevusies ieviešana, veic šādas darbības:

— noskaidro un nodod tālāk informāciju par klientu un lietotāju apmierinātību un pakalpojuma kvalitāti pēc ieviešanas (ievāc atsauksmes un apdomā, kā pastāvīgi uzlabot pakalpojumu),

— izskata visus neizpildītos kvalitātes kritērijus,

— pārbauda, vai ir pabeigtas visas darbības, nepieciešamie labojumi un izmaiņas,

— pārliecinās, ka ieviešanas beigās nav radušās problēmas ar spējām, resursiem, kapacitāti vai veiktspēju,

— pārbauda, vai visas problēmas, zināmās kļūdas un aprisinājumi ir dokumentēti un ka tos ir akceptējuši klienti, galalietotāji, operacionālā atbalsta sniedzēji un citas skartās puses,

— seko līdzi ieviešanas radītiem incidentiem un problēmām (savlaicīgi sniedz atbalstu operacionālajām vienībām gadījumos, kad laiduma dēļ ir palielinājies darba apjoms),

— atjaunina atbalsta dokumentāciju (t. i., tehniskās informācijas dokumentus),

— formāli nodod laiduma ieviešanu pakalpojumu operācijām,

— dokumentē gūto pieredzi,

— ievāc laiduma kopsavilkuma dokumentu no īstenošanas vienībām,

— formāli noslēdz laidumu pēc tam, kad ir verificēts izmaiņas pieprasījuma protokols.

9. **DROŠĪBAS INCIDENTU PĀRVALDĪBA**

Drošības incidentu pārvaldība ir process, kas nodarbojas ar drošības incidentiem nolūkā nodrošināt, ka ir iespējams par incidentiem paziņot potenciāli skartajām ieinteresētajām personām; incidentus izvērtēt un prioritizēt; uz incidentiem reaģēt tā, lai novērstu sensitīvu informācijas aktīvu konfidencialitātes, pieejamības vai integritātes jebkādu faktisku, aizdomīgu vai potenciālu pārkāpumu.

9.1. **Informācijas drošības incidentu kategorizācija**

Visus incidentus, kas ietekmē Savienības reģistra un Šveices reģistra sasaisti, analizē, lai noskaidrotu, vai ir noticis jebkādas sensitīvas informācijas sarakstā (*SIL*) iekļautās informācijas konfidencialitātes, integritātes vai pieejamības iespējams pārkāpums.

Tādā gadījumā incidentu raksturo kā informācijas drošības incidentu, nekavējoties reģistrē IT pakalpojumu pārvaldības rīkā un kā tādu arī pārvalda.

9.2. **Rīkošanās informācijas drošības incidentu gadījumā**

Drošības incidenti ir 3. eskalācijas līmeņa pārziņā, un ar šo incidentu atrisināšanu nodarbojas īpaša incidentu pārvaldības vienība (*IMT*).

IMT pienākumi ir:

— veikt pirmo analīzi, kategorizēt un novērtēt incidenta smagumu,

— koordinēt darbības starp visām ieinteresētajām personām, tostarp pilnībā dokumentēt incidenta analīzi, incidenta novēršanai pieņemtos lēmumus un konstatētās iespējamās vājās vietas,

— atkarībā no drošības incidenta smaguma incidentu laikus eskalēt līdz pienācīgam līmenim informēšanai un/vai lēmuma pieņemšanai.

Informācijas drošības pārvaldības procesā visa informācija par incidentiem tiek klasificēta visaugstākajā informācijas sensitivitātes līmenī, un jebkurā gadījumā zemākais līmenis ir "SENSITIVE: *ETS*".

Kamēr notiek izmeklēšana un/vai pastāv nepilnība, ko varētu ļaunprātīgi izmantot un kas vēl nav izlabota, informāciju klasificē ar grifu "SPECIAL HANDLING: *ETS Critical*".

9.3. **Drošības incidenta identificēšana**

Atkarībā no drošības notikuma veida informācijas drošības speciālists nosaka, kādas organizācijas jāiesaista *IMT*.

9.4. **Drošības incidenta analīze**

IMT incidenta izskatīšanā sadarbojas ar visām iesaistītajām organizācijām un attiecīgajiem to vienību dalībniekiem. Analīzes gaitā noskaidro aktīva konfidencialitātes, integritātes vai pieejamības zuduma apmēru un novērtē, kā tas ietekmēs visas skartās organizācijas. Pēc tam tiek definētas sākotnējās un pēcākās darbības, kā atrisināt incidentu un pārvaldīt tā ietekmi, tostarp šo darbību ietekmi uz resursiem.

9.5. **Drošības incidentu smaguma novērtējums, eskalēšana un ziņošana**

Pēc incidenta klasificēšanas par drošības incidentu *IMT* novērtē jebkura jauna drošības incidenta smagumu un nekavējoties sāk rīkoties atkarībā no smaguma pakāpes.

9.6. **Ziņošana par drošības incidentu**

Ziņojumā par reaģēšanu uz informācijas drošības incidentu *IMT* norāda, ar kādiem rezultātiem incidents ir iegrožots un pakalpojums ir atjaunots. Ziņojumu nosūta 3. eskalācijas līmenim, izmantojot drošu e-pastu vai citus savstarpēji akceptētus drošas saziņas līdzekļus.

Atbildīgā puse pārskata iegrožošanas un pakalpojuma atjaunošanas rezultātus un,

— ja reģistrs iepriekš ticis atslēgts, to atkal pieslēdz,

— informāciju par incidentu sniedz reģistru vienībām,

— incidentu slēdz.

Ziņojumā par informācijas drošības incidentu *IMT* būtu drošā veidā jāiekļauj relevantās ziņas, lai varētu garantēt, ka incidenti tiek reģistrēti un par tiem tiek paziņots saskanīgā veidā, un lai būtu iespējams nekavējoties un pienācīgi rīkoties, lai incidentu iegrožotu. Galīgo ziņojumu par informācijas drošības incidentu *IMT* iesniedz pienācīgā laikā.

9.7. **Monitorings, kapacitātes veidošana un pastāvīgi uzlabojumi**

IMT par visiem drošības incidentiem sniegs ziņojumus 3. eskalācijas līmenim. Šajā eskalācijas līmenī ziņojumi tiks izmantoti, lai apzinātu

— drošības kontroļu un/vai operāciju vājās vietas, kas jāstiprina,

— iespējamās vajadzības šo procedūru pilnveidot, lai reaģēšanu uz incidentiem padarītu rezultatīvāku,

— apmācības un kapacitātes veidošanas iespējas, lai pastiprinātu reģistru sistēmu noturību informācijas drošības aspektā, mazinātu turpmāku incidentu risku un minimalizētu to ietekmi.

10. **INFORMĀCIJAS DROŠĪBAS PĀRVALDĪBA**

Informācijas drošības pārvaldības mērķis ir nodrošināt organizācijas klasificētās informācijas, datu un IT pakalpojumu konfidencialitāti, integritāti un pieejamību. Līdztekus tehniskajiem komponentiem, t. sk. projektēšanai un testēšanai (sk. STS), pastāvīgās reģistru sasaistes drošības prasību izpildei ir vajadzīgas šādas kopējas darbības procedūras.

10.1. **Sensitīvas informācijas identificēšana**

Konkrēta informācijas elementa sensitivitāti novērtē, nosakot, kādā mērā ar šo informāciju saistīts drošības pārkāpums ietekmētu darbību (piem., finansiālie zaudējumi, tēla pasliktināšanās, normatīvo aktu pārkāpums).

Sensitīvās informācijas aktīvus identificē, balstoties uz to ietekmi uz sasaisti.

Šīs informācijas sensitivitātes pakāpi novērtē saskaņā ar sensitivitātes skalu, kas piemērojama šai sasaistei un kas sīki izklāstīta šā dokumenta sadaļā "Rīkošanās informācijas drošības incidentu gadījumā".

10.2. **Informācijas aktīvu sensitivitātes pakāpes**

Identificējot informācijas aktīvus, tos klasificē pēc šādiem noteikumiem:

— ja identificēta vismaz viena AUGSTA konfidencialitātes, integritātes vai pieejamības pakāpe, aktīvs klasificējams kā "SPECIAL HANDLING: *ETS Critical*" aktīvs,

— ja identificēta vismaz viena VIDĒJA konfidencialitātes, integritātes vai pieejamības pakāpe, aktīvs klasificējams kā "SENSITIVE: *ETS*" aktīvs,

— ja identificēta tikai ZEMA konfidencialitātes, integritātes vai pieejamības pakāpe, aktīvs ES klasificējams ar grifu "SENSITIVE: *ETS Joint Procurement*" vai Šveicē – ar grifu "LIMITED: *ETS*".

10.3. **Informācijas aktīvu īpašnieka nozīmēšana**

Visiem informācijas aktīviem nozīmē īpašnieku. ETS informācijas aktīvi, kas ir daļa no *EUTL* un *SSTL* sasaistes vai ir ar to saistīti, ir jāiekļauj kopējo aktīvu inventarizācijas sarakstā, ko uztur abas puses. ETS informācijas aktīvi, kas nav daļa no *EUTL* un *SSTL* sasaistes, ir jāiekļauj aktīvu inventarizācijas sarakstā, ko uztur attiecīgā puse.

Par to, kas ir īpašnieks katram informācijas aktīvam, kurš ir daļa no *EUTL* vai *SSTL* sasaistes vai ir ar to saistīts, puses vienojas savā starpā. Par informācijas aktīva sensitivitātes novērtēšanu atbild tā īpašnieks.

Īpašniekam jābūt senioritātes līmenim, kas atbilst piešķirto aktīvu vērtībai. Par īpašnieka atbildību par aktīvu(-iem) un pienākumu uzturēt vajadzīgo konfidencialitātes, integritātes un pieejamības līmeni būtu jāvienojas un šie aspekti jāformalizē.

10.4. **Sensitīvas informācijas reģistrēšana**

Visu sensitīvo informāciju iekļauj sensitīvās informācijas sarakstā (*SIL*).

SIL ņem vērā un reģistrē gadījumus, kad sensitīvas informācijas sakopojumam (piemēram, informācijas kopumam, kas glabājas sistēmas datubāzē) var būt lielāka ietekme nekā vienvienīgam informācijas elementam.

SIL nav statisks. Ar aktīviem saistītie draudi, ievainojamības, drošības incidentu iespējamība vai sekas var mainīties negaidīti; tāpat reģistru sistēmas darbībā var tikt ieviesti jauni aktīvi.

Tāpēc *SIL* regulāri pārskata, un jebkādu jaunu informāciju, kas identificēta kā sensitīva, nekavējoties reģistrē *SIL*.

Katrā *SIL* ierakstā norāda vismaz šādas ziņas:

— informācijas apraksts,

— informācijas īpašnieks,

— sensitivitātes pakāpe,

— norāde, vai informācija satur persondatus,

— papildu ziņas, ja vajadzīgs.

10.5. **Rīkošanās ar sensitīvu informāciju**

Ja sensitīvu informāciju apstrādā ārpus Savienības reģistra un Šveices reģistra sasaistes, ar to rīkojas saskaņā ar rīkošanās instrukcijām.

Ja sensitīvu informāciju apstrādā Savienības reģistra un Šveices reģistra sasaistes ietvaros, ar to rīkojas saskaņā ar pušu drošības prasībām.

10.6. **Piekļuves pārvaldība**

Piekļuves pārvaldības uzdevums ir autorizētiem lietotājiem piešķirt tiesības izmantot pakalpojumu un tajā pašā laikā novērst neautorizētu lietotāju piekļuvi. Piekļuves pārvaldību reizēm dēvē par "Tiesību pārvaldību" vai "Identitātes pārvaldību".

Kas attiecas uz pastāvīgu reģistru sasaisti un tās darbību, abām pusēm ir vajadzīga piekļuve šādiem komponentiem:

— *Wiki* – kopdarbības vide, kurā apmainās ar kopējo informāciju, piemēram, plānojot laidumus,

— IT pakalpojumu pārvaldības (*ITSM*) rīks, ko izmanto incidentu un problēmu pārvaldībā (sk. 3. nodaļu "Pieeja un standarti"),

— ziņojumapmaiņas sistēma – katra puse nodrošina drošu ziņojumapmaiņas sistēmu, kas domāta, lai nosūtītu darījumu datus saturošus ziņojumus.

Šveices reģistra administrators un Savienības centrālais administrators nodrošina, ka piekļuve ir aktualizēta, un attiecībā uz piekļuves pārvaldības darbībām darbojas kā pušu kontaktpunkti. Piekļuves pieprasījumus apstrādā saskaņā ar pieprasījuma izpildes procedūrām.

10.7. **Sertifikātu/atslēgu pārvaldība**

Katra puse ir atbildīga par savu sertifikātu/atslēgu pārvaldību (sertifikātu/atslēgu ģenerēšanu, reģistrēšanu, glabāšanu, instalēšanu, izmantošanu, atjaunošanu, atsaukšanu, dublēšanu un atkopšanu). Kā izklāstīts sasaistes tehniskajos standartos (STS), izmantojami ir tikai digitālie sertifikāti, ko izdevis sertificētājs (*CA*), kuram uzticas abas puses. Rīkojoties ar sertifikātiem/atslēgām un tos glabājot, ir jāievēro rīkošanās instrukcijās izklāstītie noteikumi.

Sertifikātu un atslēgu atsaukšanu un/vai atjaunošanu abas puses koordinē savā starpā. Tas notiek saskaņā ar pieprasījuma izpildes procedūrām.

Šveices reģistra administrators un Savienības centrālais administrators ar sertifikātiem/atslēgām apmainās, izmantojot drošus saziņas līdzekļus saskaņā ar rīkošanās instrukcijās izklāstītajiem noteikumiem.

Sertifikātu/atslēgu verifikācija jebkādā veidā starp pusēm notiek ārpus joslas.

III PIELIKUMS

SASAISTES TEHNISKIE STANDARTI (STS) SASKAŅĀ AR 3. PANTA 7. PUNKTU NOLĪGUMĀ STARP EIROPAS SAVIENĪBU UN ŠVEICES KONFEDERĀCIJU PAR SILTUMNĪCEFEKTA GĀZU EMISIJAS KVOTU TIRDZNIECĪBAS SISTĒMU SASAISTI

Pastāvīgas reģistru sasaistes standarts

Satura rādītājs

1. GLOSĀRIJS 21
2. IEVADS 22
2.1. Tvērums 22
2.2. Adresāti 23
3. VISPĀRĪGI NOTEIKUMI 23
3.1. Komunikācijas līnijas arhitektūra 23
3.1.1. Ziņojumapmaiņa 23
3.1.2. XML ziņojums – augsta līmeņa apraksts 23
3.1.3. Uzņemšanas logi 24
3.1.4. Darījuma ziņojumu plūsmas 24
3.2. Datu pārsūtīšanas drošība 26
3.2.1. Ugunsmūris un tīklu starpsavienojums 26
3.2.2. Virtuāls privātais tīkls (VPN) 26
3.2.3. IPsec ieviešana 27
3.2.4. Drošas ziņojumu apmaiņas pārsūtīšanas protokols 27
3.2.5. XML satura šifrēšana un paraksts 27
3.2.6. Šifrēšanas atslēgas 27
3.3. Sasaistes funkciju saraksts 27
3.3.1. Darbības darījumi 28
3.3.2. Saskaņošanas protokols 28
3.3.3. Testa ziņojums 28
3.4. Datu reģistrēšanas prasības 29
3.5. Operacionālās prasības 29
4. PIEEJAMĪBAS NOTEIKUMI 30
4.1. Komunikācijas pieejamības nodrošināšana 30
4.2. Inicializēšanas, komunikācijas reaktivizēšanas un testēšanas plāns 30
4.2.1. Iekšējie IKT infrastruktūras testi 31
4.2.2. Komunikācijas testi 31
4.2.3. Pilnas sistēmas (“no gala līdz galam”) testi 31
4.2.4. Drošības testi 31
4.3. Akceptēšanas vide / testēšanas vide 32
5. KONFIDENCIALITĀTES UN INTEGRITĀTES NOTEIKUMI 32
5.1 Drošības testēšanas infrastruktūra 32
5.2 Sasaistes apturēšanas un reaktivizēšanas noteikumi 32
5.3 Noteikumi par drošības pārkāpumiem 33

5.4 Drošības testēšanas vadlīnijas 33
5.4.1 Programmatūra 33
5.4.2 Infrastruktūra 34
5.5 Riska novērtēšanas noteikumi 34

1. **GLOSĀRIJS**

1.1. tabula.

Tematiskie akronīmi un definīcijas

Akronīms/termins	Definīcija
Kvota	Tiesības noteiktā periodā emitēt vienu tonnu oglekļa dioksīda ekvivalenta; kvota derīga tikai vienas vai otras puses ETS prasību izpildei
CH	Šveices Konfederācija
CHU	Stacionāro iekārtu kvota, saukta arī par *CHU2* (atsaucoties uz Kioto protokola 2. saistību periodu), ko piešķīrusi CH
CHUA	Šveices aviācijas kvota
KDP	Kopējās darbības procedūras Kopīgi izstrādātas procedūras, kas vajadzīgas, lai ES ETS un Šveices ETS sasaiste varētu darboties
EKTR	Emisijas kvotu tirdzniecības reģistrs
ETS	Emisijas kvotu tirdzniecības sistēma
ES	Eiropas Savienība
EUA	ES vispārīgā kvota
EUAA	ES aviācijas kvota
ESKR	Eiropas Savienības konsolidētais reģistrs
EUTL	Eiropas Savienības darījumu žurnāls
Reģistrs	Uzskaites sistēma, kurā uzskaita ETS ietvaros iedalītās kvotas un kura ļauj izsekot elektroniskajos kontos turēto kvotu īpašumtiesībām
SSTL	Šveices papildu darījumu žurnāls
Darījums	Reģistra process, kurā kvota tiek no viena konta pārskaitīta uz citu kontu
Darījumu žurnāla sistēma	Darījumu žurnālā ir ieraksts par katru ierosināto darījumu, ko viens reģistrs nosūta otram reģistram

1.2. tabula.

Tehniskie akronīmi un definīcijas

Akronīms	Definīcija
Asimetriskā kriptogrāfija	Datu šifrēšanai un atšifrēšanai izmanto publiskās un privātās atslēgas
Sertificētājs (*CA*)	Iestāde, kas izdod digitālos sertifikātus
Šifrēšanas atslēga	Informācijas bloks, kas nosaka šifrēšanas algoritma funkcionālo izlaidi
Atšifrēšana	Šifrēšanai pretējs process
Digitālais paraksts	Matemātiska metode, ko izmanto, lai validētu ziņojuma, programmatūras vai digitāla dokumenta autentiskumu un integritāti
Šifrēšana	Informācijas vai datu pārvēršana kodā, jo īpaši nolūkā novērst neatļautu piekļuvi
Datnes uzņemšana	Datnes nolasīšanas process

Akronīms	Definīcija
Ugunsmūris	Tīkla drošības ierīce vai programmatūra, kas, balstoties uz iepriekš noteiktiem noteikumiem, monitorē un kontrolē ienākošo un izejošo tīkla datplūsmu
Periodisko kontrolziņojumu monitorēšana	Aparatūra vai programmatūra ģenerē un monitorē periodisku signālu normālas darbības apliecināšanai vai citu datorsistēmas daļu sinhronizēšanai
IPS_{EC}	IP drošība (angliski: *IP SECurity*). Tīkla protokolu komplekts, kas autentificē un šifrē datu paketes, lai nodrošinātu drošu šifrētu komunikāciju starp diviem datoriem interneta protokola tīklā
Ielaušanās testēšana	Datorsistēmas, tīkla vai tīmekļa lietotnes testēšana nolūkā atklāt ievainojamības, ko varētu izmantot uzbrucējs
Saskaņošanas process	Process, kurā nodrošina, ka divi ierakstu kopumi savstarpēji atbilst
VPN	Virtuāls privāts tīkls
XML	Paplašināmās iezīmēšanas valoda. Tas izstrādātājiem dod iespēju izveidot savus īpašus tagus, kas ļauj definēt, pārsūtīt, validēt un interpretēt datus starp lietotnēm un starp organizācijām

2. **IEVADS**

2017. gada 23. novembrī noslēgtais Nolīgums starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti ("Nolīgums") paredz savstarpēji atzīt emisijas kvotas, ko var izmantot, lai panāktu atbilstību Eiropas Savienības emisijas kvotu tirdzniecības sistēmā (ES ETS) vai Šveices emisijas kvotu tirdzniecības sistēmā (Šveices ETS). Lai ES ETS un Šveices ETS sasaiste varētu darboties, starp Savienības reģistra Eiropas Savienības darījumu žurnālu (*EUTL*) un Šveices reģistra Šveices papildu darījumu žurnālu (*SSTL*) izveidos tiešu sasaisti, kas dos iespēju katras ETS ietvaros izdotās kvotas pārskaitīt no viena reģistra uz otru (Nolīguma 3. panta 2. punkts). Lai ES ETS un Šveices ETS sasaiste varētu darboties 2020. gadā tika ieviests pagaidu risinājums. No 2023. gada abu emisijas kvotu tirdzniecības sistēmu reģistru sasaiste pakāpeniski tiks pārveidota par pastāvīgu reģistru sasaisti, un to paredzēts īstenot ne vēlāk kā 2024. gadā; tā nodrošinās, ka sasaistītie tirgi funkcionē attiecībā uz ieguvumiem no tirgus likviditātes, un dos iespēju izpildīt darījumus starp abām sasaistītajām sistēmām veidā, kas ir līdzvērtīgs vienam tirgum, kuru veido divas sistēmas, un kas tirgus dalībniekiem nodrošina iespēju rīkoties tā, it kā tie būtu vienā tirgū, ievērojot tikai atsevišķus Pušu regulatīvos noteikumus (Nolīguma II pielikums).

Saskaņā ar Nolīguma 3. panta 7. punktu Šveices reģistra administrators un Savienības centrālais administrators, balstoties uz Nolīguma II pielikumā izklāstītajiem principiem, izstrādā sasaistes tehniskos standartus (STS), kas sīki apraksta prasības stabila un droša savienojuma izveidei starp *SSTL* un *EUTL*. Administratoru izstrādātie STS stājas spēkā, kad tie ir pieņemti ar Apvienotās komitejas lēmumu.

Apvienotā komiteja STS pieņēma ar Lēmumu Nr. 2/2020. Šajā dokumentā izklāstītos atjauninātos STS Apvienotā komiteja pieņems ar Lēmumu Nr. 1/2024. Saskaņā ar šo lēmumu un Apvienotās komitejas lūgumiem Šveices reģistra administrators un Savienības centrālais administrators ir izstrādājuši sīkākas tehniskās vadlīnijas, kas nepieciešamas, lai nodrošinātu sasaistes funkcionēšanu, tās pastāvīgu pielāgošanu tehnikas attīstībai un jaunām prasībām, kas saistītas ar sasaistes drošumu un drošību, un tās rezultatīvu un efektīvu darbību, un atjauninās tās.

2.1. **Tvērums**

Šis dokuments atspoguļo Nolīguma pušu kopīgo izpratni par ES ETS un Šveices ETS reģistru sasaistes tehniskā pamata izveidi. Lai gan tajā ir izklāstītas bāzlīnijas tehniskās specifikācijas, proti, bāzlīnijas arhitektūras, pakalpojumu un drošības prasības, šīs sasaistes operacionalizēšanai būs vajadzīgi vēl sīkāki norādījumi.

Lai tā varētu pienācīgi funkcionēt un to lielākā mērā operacionalizētu, būs jānosaka dažādi procesi un procedūras. Saskaņā ar Nolīguma 3. panta 6. punktu šie jautājumi tiks iztirzāti kopējo darbības procedūru (KDP) dokumentā, ko Apvienotā komiteja pieņems atsevišķi ar attiecīgu lēmumu.

2.2. **Adresāti**

Šis dokuments ir adresēts Šveices reģistra administratoram un Savienības centrālajam administratoram.

3. **VISPĀRĪGI NOTEIKUMI**

3.1. **Komunikācijas līnijas arhitektūra**

Šīs iedaļas mērķis ir sniegt aprakstu par vispārējo arhitektūru ES ETS un Šveices ETS sasaistes operacionalizēšanai un dažādajiem tajā iesaistītajiem komponentiem.

Tā kā būtiska reģistru sasaistes arhitektūras definēšanas daļa ir drošība, ir veikti visi pasākumi stabilas arhitektūras izveidei. Pastāvīgā reģistru sasaiste droša gaisa spraugas savienojuma īstenošanai izmanto datņu apmaiņas mehānismu.

Tehniskajā risinājumā izmanto šādus elementus:

— drošas ziņojumu apmaiņas pārsūtīšanas protokols;

— *XML* ziņojumi;

— uz *XML* balstīts digitālais paraksts un šifrēšana;

— *VPN*.

3.1.1. *Ziņojumapmaiņa*

Komunikācija starp Savienības reģistru un Šveices reģistru balstās uz ziņojumu apmaiņas mehānismu, kurā izmanto drošus kanālus. Katrai sistēmai ir savs saņemto ziņojumu repozitorijs.

Abas puses saņemtos ziņojumus reģistrē kopā ar apstrādes datiem.

Par kļūdām vai neparedzētu statusu nosūtāmi brīdinājuma ziņojumi, un šādā gadījumā vajadzētu sazināties atbalsta komandu personālam.

Kļūdu un neparedzētu notikumu gadījumā ievēro KDP incidentu pārvaldības procesā noteiktās darbības procedūras.

3.1.2. *XML ziņojums – augsta līmeņa apraksts*

XML ziņojums ietver vienu no šiem elementiem:

— viens vai vairāki darījuma pieprasījumi un/vai viena vai vairākas darījuma atbildes,

— viena operācija/atbilde, kas saistīta ar saskaņošanu,

— viens testa ziņojums.

Katrā ziņojumā ir galvene, kurā norādīta(-s)

— izcelsmes ETS,

— kārtas numurs.

3.1.3. *Uzņemšanas logi*

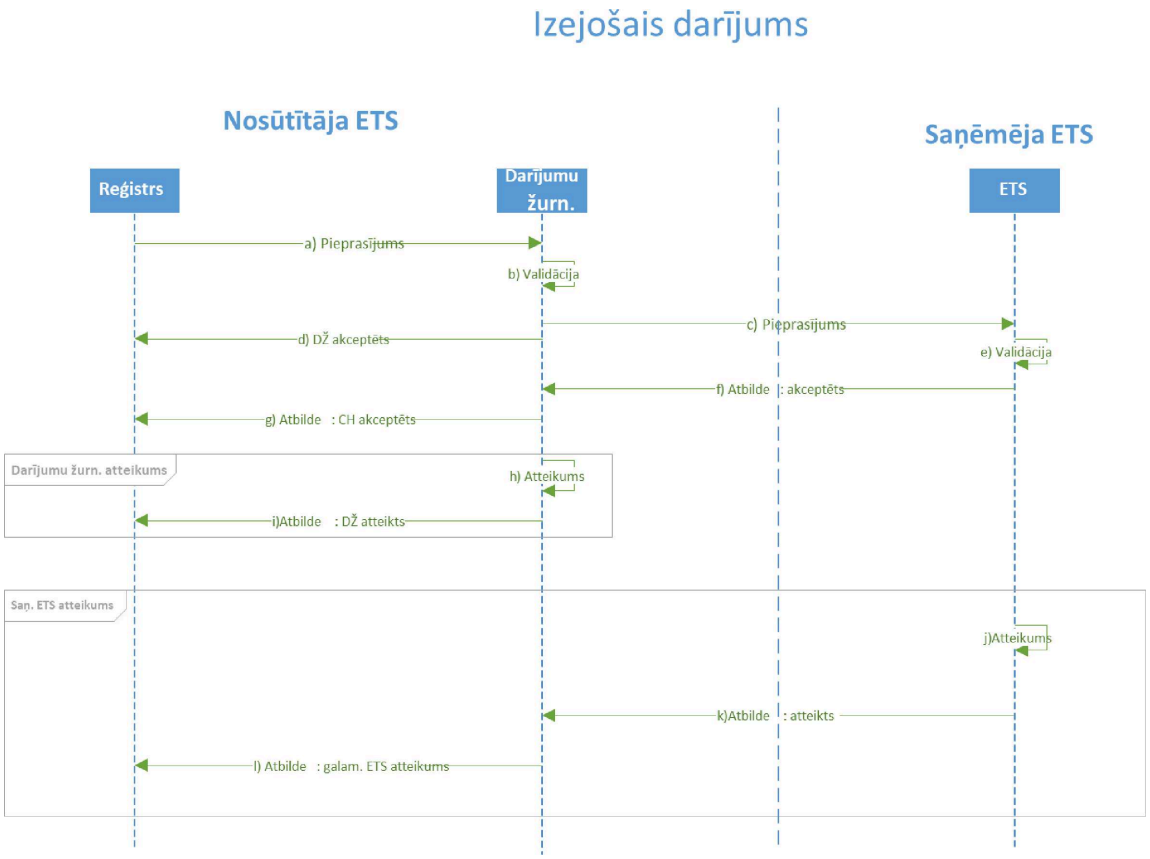
Pastāvīgā reģistru sasaiste ir balstīta uz iepriekš noteiktiem uzņemšanas logiem, kam seko nosauktu notikumu kopums. Darījumu pieprasījumi, kas saņemti, izmantojot sasaisti, tiks uzņemti tikai iepriekš noteiktos intervālos. Uzņemšanas logi ietver izejošo un ienākošo darījumu tehnisko validāciju. Turklāt saskaņošanu var veikt katru dienu, un to var palaist manuāli.

Attiecībā uz jebkuru šo notikumu biežuma un/vai laika maiņu tiks ievērotas darbības procedūras, kas noteiktas KDP pieprasījuma izpildes procesā.

3.1.4. *Darījuma ziņojumu plūsmas*

Izejošie darījumi

Šajā iedaļā atspoguļota nosūtītājas ETS perspektīva. Konkrētā plūsma ir attēlota šādā secības diagrammā:



Galvenā plūsma uzrāda šādus soļus (kā attēlots iepriekš):

a) nosūtītājā ETS darījuma pieprasījums no reģistra tiek nosūtīts uz darījumu žurnālu, tiklīdz beigušās visas darbības aizkaves (attiecīgā gadījumā – 24 h aizkave);

b) darījumu žurnāls darījuma pieprasījumu validē;

c) darījuma pieprasījums tiek nosūtīts uz galamērķa ETS;

d) izcelsmes ETS reģistram tiek nosūtīta akcepta atbilde;

e) galamērķa ETS darījuma pieprasījumu validē;

f) galamērķa ETS uz nosūtītājas ETS darījumu žurnālu nosūta akcepta atbildi;

g) darījumu žurnāls akcepta atbildi nosūta reģistram.

Alternatīva plūsma “Darījuma žurnāla atteikums” (kā attēlots iepriekš, sākot no a) soļa galvenajā plūsmā):

a) izcelsmes sistēmā darījuma pieprasījums no reģistra tiek nosūtīts uz darījumu žurnālu, tiklīdz beigušās visas darbības aizkaves (attiecīgā gadījumā – 24 h aizkave);

b) darījumu žurnāls pieprasījumu nevalidē;

c) izcelsmes reģistram tiek nosūtīts atteikuma ziņojums.

Alternatīva plūsma “ETS atteikums” (kā attēlots iepriekš, sākot no d) soļa galvenajā plūsmā):

a) izcelsmes ETS darījuma pieprasījums no reģistra tiek nosūtīts uz darījumu žurnālu, tiklīdz beigušās visas darbības aizkaves (attiecīgā gadījumā – 24 h aizkave);

b) darījumu žurnāls darījuma pieprasījumu validē;

c) darījuma pieprasījums tiek nosūtīts uz galamērķa ETS;

d) izcelsmes ETS reģistram tiek nosūtīts akcepta ziņojums;

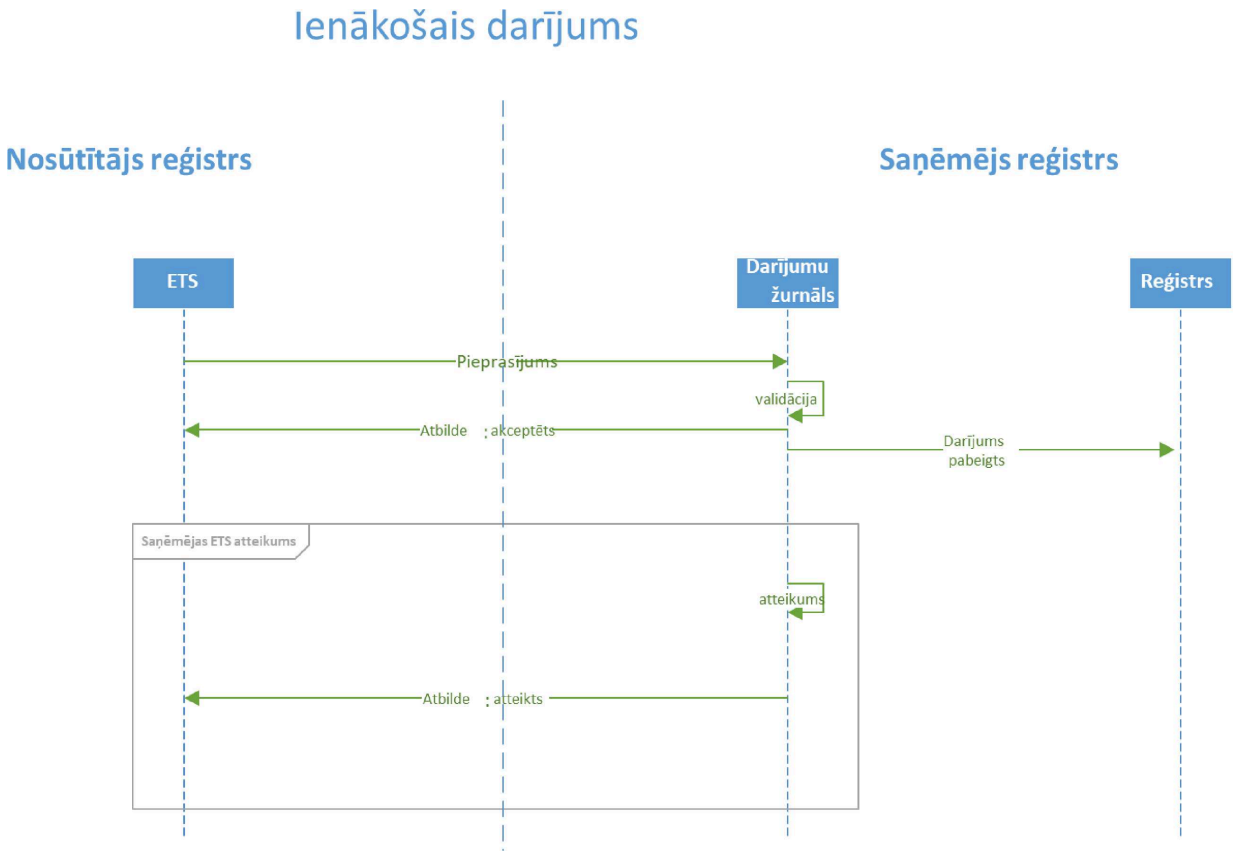
e) saņēmējas ETS darījumu žurnāls darījumu nevalidē;

f) saņēmēja ETS uz nosūtītājas ETS darījumu žurnālu nosūta atteikuma atbildi;

g) darījumu žurnāls atteikuma atbildi nosūta reģistram.

Ienākošie darījumi

Šajā iedaļā atspoguļota saņēmējas ETS perspektīva. Konkrētā plūsma ir attēlota šādā secības diagrammā.



Diagrammā redzams:

1) kad saņēmējas ETS darījumu žurnāls pieprasījumu validē, tas nosūta akcepta ziņojumu nosūtītājai ETS un ziņojumu “darījums pabeigts” saņēmējas ETS reģistram.

2) Ja ienākošais pieprasījums saņēmējas sistēmas darījumu žurnālā tiek atteikts, darījuma pieprasījums saņēmējas ETS reģistram nosūtīts netiek.

Protokols

Darījuma ziņojumu ciklā ir tikai divi ziņojumi:

— darījuma ierosinājums no nosūtītājas ETS → saņēmējai ETS,

— darījuma atbilde no saņēmējas ETS → nosūtītājai ETS – vai nu akceptēts, vai atteikts (ar atteikuma iemeslu):

  — akceptēts: darījums ir pabeigts;

  — atteikts: darījums ir izbeigts.

Darījuma statuss

— Nosūtot pieprasījumu, nosūtītājā ETS darījuma statuss tiks iestatīts uz "ierosināts".

— Saņēmējā ETS darījuma statuss tiks iestatīts uz "ierosināts", kad pieprasījums būs saņemts un kamēr tiks apstrādāts.

— Kad ierosinājums būs apstrādāts, darījuma statuss saņēmējā ETS tiks iestatīts uz "pabeigts"/"izbeigts". Tad saņēmēja ETS nosūtīs attiecīgo akcepta/atteikuma ziņojumu.

— Kad akcepts/atteikums būs saņemts un apstrādāts, darījuma statuss nosūtītājā ETS tiks iestatīts uz "pabeigts"/"izbeigts".

— Ja atbilde nebūs saņemta, darījuma statuss nosūtītājā ETS aizvien paliks "ierosināts".

— Saņēmēja ETS darījuma statuss ikvienam ierosinātam darījumam, kam statuss "ierosināts" būs ilgāk par 30 min, iestatīs darījuma statusu "izbeigts".

Ar darījumiem saistītu incidentu gadījumā tiks ievērotas darbības procedūras, kas noteiktas KDP incidentu pārvaldības procesā.

3.2. **Datu pārsūtīšanas drošība**

Sūtīšanas laikā datiem tiks piemēroti četri drošības līmeņi:

1) tīkla piekļuves kontrole: ugunsmūris un tīklu starpsavienojumu slānis;

2) transportēšanas līmeņa šifrēšana: *VPN*;

3) sesijas līmeņa šifrēšana: drošas ziņojumu apmaiņas pārsūtīšanas protokols;

4) lietotnes līmeņa šifrēšana: *XML* satura šifrēšana un paraksts.

3.2.1. *Ugunsmūris un tīklu starpsavienojums*

Sasaisti izveido tīklā, ko aizsargā aparatūras ugunsmūris. Ugunsmūri ar noteikumiem konfigurē tā, lai pieslēgties *VPN* serverim varētu tikai reģistrēti klienti.

3.2.2. *Virtuāls privātais tīkls (VPN)*

Visu komunikāciju starp pusēm aizsargā, izmantojot virtuālā privātā tīkla (*VPN*) tehnoloģiju. *VPN* tehnoloģijas nodrošina iespēju cauri tādam tīklam kā internets izveidot "tuneli" no viena punkta uz citu, tā aizsargājot visu komunikāciju. Pirms *VPN* tuneļa izveides potenciālā klienta galapunktam tiek izdots digitālais sertifikāts, kas ļauj klientam savienojuma izveides laikā uzrādīt identitātes apliecinājumu. Katra puse ir atbildīga par sertifikāta instalēšanu savā *VPN* galapunktā. Izmantojot digitālos sertifikātus, katrs gala *VPN* serveris piekļūst centrālai struktūrai, lai vienotos par autentifikācijas akreditācijas datiem. Tuneļa izveides procesā notiek vienošanās par šifrēšanu, nodrošinot, ka visa komunikācija caur tuneli ir aizsargāta.

Klienta *VPN* galapunktus konfigurē tā, lai *VPN* tuneli uzturētu pastāvīgi – tā starp pusēm jebkurā laikā ir iespējama uzticama divvirzienu un reāllaika komunikācija.

Parasti Eiropas Savienība kā privātu uz IP balstītu tīklu izmanto drošus Eiropas pakalpojumus telemātikai starp iestādēm (*STESTA*). Tāpēc šis tīkls ir piemērots arī pastāvīgai reģistru sasaistei.

3.2.3. *IPsec ieviešana*

IPSec protokola izmantošana starptīklu *VPN* infrastruktūras izveidei nodrošinās starptīklu autentifikāciju, datu integritāti un datu šifrēšanu. *IPsec VPN* konfigurācijas nodrošina pienācīgu autentifikāciju starp diviem *VPN* savienojuma galapunktiem. Puses attālināto klientu identificēs un autentificēs ar *IPSec* savienojumu, izmantojot digitālos sertifikātus, ko izsniedzis otras puses atzīts sertificētājs.

IPsec nodrošina arī visas pa *VPN* tuneli laistās komunikācijas datu integritāti. Datu pakešu jaukšana un parakstīšana notiek, izmantojot *VPN* noteikto autentifikācijas informāciju. Ar *IPSec* šifrēšanu tiek nodrošināta arī datu konfidencialitāte.

3.2.4. *Drošas ziņojumu apmaiņas pārsūtīšanas protokols*

Lai puses varētu droši apmainīties ar datiem, pastāvīga reģistru sasaiste balstās uz vairākiem šifrēšanas slāņiem. Abas sistēmas un to dažādās vides tīkla līmenī ir starpsavienotas, izmantojot *VPN* tuneļus. Lietotnes līmenī datnes tiek pārsūtītas, izmantojot drošas ziņojumu apmaiņas pārsūtīšanas protokolu sesijas līmenī.

3.2.5. *XML satura šifrēšana un paraksts*

XML datnēs parakstīšana un šifrēšana notiek divos līmeņos. Katrs darījuma pieprasījums, darījuma atbilde un saskaņošanas ziņojums tiek atsevišķi digitāli parakstīts.

Otrajā solī katrs elementa “ziņojums” apakšelements tiek atsevišķi šifrēts.

Turklāt trešajā solī, lai nodrošinātu visa ziņojuma integritāti un nenoliedzamību, tiek digitāli parakstīts pamatelementa ziņojums. Tā tiek nodrošināts augsts XML iegulto datu aizsardzības līmenis. Tehniskajā īstenošanā tiek ievēroti globālā tīmekļa konsorcija standarti.

Ziņojumu atšifrējot un verificējot, process notiek apgrieztā secībā.

3.2.6. *Šifrēšanas atslēgas*

Šifrēšanai un parakstīšanai tiks izmantota publiskās atslēgas kriptogrāfija.

Konkrēti *IPSec* gadījumā izmantojami ir tikai digitālie sertifikāti, ko izdevis sertificētājs (*CA*), kuram uzticas abas puses. Šis *CA* verificē sertifikāta turētāja identitāti un izdod sertifikātus, ko izmanto, lai pozitīvi identificētu organizāciju un pušu saziņai izveidotu drošus datu komunikācijas kanālus.

Kriptogrāfiskās atslēgas izmanto sakaru kanālu un datu datņu parakstīšanai un šifrēšanai. Puses digitāli apmainās ar publiskajiem sertifikātiem, izmantojot drošus kanālus, un tiem veic ārpusjoslas verifikāciju. Šī procedūra ir neatņemama KDP informācijas drošības pārvaldības procesa daļa.

3.3. **Sasaistes funkciju saraksts**

Sasaiste precizē pārsūtīšanas sistēmu virknei funkciju, ar kurām tiek īstenoti no Nolīguma izrietošie darbības procesi. Sasaiste turklāt ietver specifikāciju saskaņošanas procesam un testa ziņojumiem, kas ļaus veikt periodisko kontrolziņojumu monitorēšanu.

3.3.1. *Darbības darījumi*

No darbības viedokļa sasaiste paredz četru (4) veidu darījumu pieprasījumus:

— ārēja pārskaitīšana:

  — pēc ETS sasaistes stāšanās spēkā ES un CH kvotas ir savstarpēji aizstājamas un līdz ar to pilnībā pārskaitāmas no vienas puses otrai.

  — Lai ar sasaistes starpniecību varētu veikt pārskaitījumu, vienā ETS ir vajadzīgs pārskaitītāja konts un otrā – saņēmēja konts.

  — Pārskaitījumā var iekļaut šo četru (4) veidu kvotas jebkādā daudzumā:

    — Šveices vispārīgās kvotas (*CHU*),

    — Šveices aviācijas kvotas (*CHUA*),

    — ES vispārīgās kvotas (*EUA*),

    — ES aviācijas kvotas (*EUAA*);

— starptautiskā iedale:

gaisa kuģu operatori, kurus administrē viena ETS un kuriem ir saistības otrā ETS un tiesības saņemt bezmaksas kvotas no šīs otrās ETS, bezmaksas aviācijas kvotas no otrās ETS saņems ar starptautiskās iedales darījumu;

— starptautiskās iedales apvērse:

šis darījums tiks veikts tad, ja bezmaksas kvotas, ko gaisa kuģa operatora turējuma kontam iedalījusi otra ETS, būs pilnīgi jāatgriež;

— iedales apjoma pārsnieguma atgriešana:

apvērsei līdzīgs darījums, tikai iedale netiek pilnīgi apvērsta; iedalītājai ETS tiek atgrieztas tikai iedales apjoma pārsnieguma kvotas.

3.3.2. *Saskaņošanas protokols*

Saskaņošana notiks tikai pēc tam, kad būs noslēgušies ziņojumu uzņemšanas, validēšanas un apstrādes logi.

Saskaņošana ir neatņemama sasaistes drošības un konsekvences pasākumu daļa. Pirms grafika izveidošanas abas puses vienosies par precīzu saskaņošanas laiku. Ja abas puses par to vienojas, plānota saskaņošana var notikt katru dienu. Minimums ir viena plānota saskaņošana pēc katras uzņemšanas.

Katrā ziņā gan viena, gan otra puse jebkurā laikā var iniciēt manuālu saskaņošanu.

Attiecībā uz jebkuras plānotās saskaņošanas laika un/vai biežuma maiņu tiks ievērotas darbības procedūras, kas noteiktas KDP pieprasījuma izpildes procesā.

3.3.3. *Testa ziņojums*

Sakaru "no gala līdz galam" pārbaudīšanai ir paredzēts testa ziņojums. Ziņojumā būs dati, kas ziņojumu identificēs kā testu, un pēc saņemšanas otrā pusē uz to tiks nosūtīta atbilde.

3.4. **Datu reģistrēšanas prasības**

Ņemot vērā abu pušu vajadzību uzturēt precīzu un konsekventu informāciju un vajadzību pēc rīkiem, ko izmantot saskaņošanas procesā neatbilstību novēršanai, abas puses uztur četru (4) veidu datu žurnālus:

— darījumu žurnāli,

— saskaņošanas žurnāli,

— ziņojumu arhīvs,

— iekšējās revīzijas žurnāli.

Visus datus šajos žurnālos problēmu novēršanas nolūkā glabā vismaz trīs (3) mēnešus, un to tālāka saglabāšana revīzijas nolūkā ir atkarīga no katrā galā piemērojamajiem tiesību aktiem. Žurnālu datnes, kas vecākas par trim (3) mēnešiem, var arhivēt drošā vietā neatkarīgā IT sistēmā, ja vien tās var izgūt vai tām piekļūt saprātīgā termiņā.

Darījumu žurnāli

Gan *EUTL*, gan *SSTL* apakšsistēmās ir ieviesti darījumu žurnāli.

Konkrētāk, darījumu žurnālos tiks reģistrēts katrs ierosinātais darījums, kas nosūtīts uz otru ETS. Katrā ierakstā ir visi darījuma satura lauki un pēcākais darījuma iznākums (saņēmējas ETS atbilde). Darījumu žurnālos tiks reģistrēti arī ienākošie darījumi, kā arī atbilde, kas nosūtīta izcelsmes ETS.

Saskaņošanas žurnāli

Saskaņošanas žurnāls ietver ierakstu par katru saskaņošanas ziņojumu, ar kuru puses ir apmainījušās, tostarp saskaņošanas identifikatoru, laika zīmogu un saskaņošanas rezultātu – saskaņošanas statusu "atbilst" vai "neatbilstības". Pastāvīgā reģistru sasaistē saskaņošanas ziņojumi ir neatņemama ziņojumu apmaiņas daļa, un tāpēc tos glabā, kā aprakstīts sadaļā "Ziņojumu arhīvs".

Abas puses katru pieprasījumu un atbildi uz to reģistrē saskaņošanas žurnālā. Lai gan saskaņošanas žurnālā ietvertā informācija pašā saskaņošanā netiek kopīgota tieši, piekļuve šai informācijai var būt vajadzīga neatbilstību novēršanai.

Ziņojumu arhīvs

Abām pusēm ir pienākums nosūtīto un saņemto datu kopiju (*XML* datnes) arhivēt, kā arī reģistrēt, vai tie vai *XML* ziņojumi bijuši pareizā formātā.

Arhīva galvenais mērķis ir kalpot revīzijas vajadzībām, glabāt pierādījumus, kas nosūtīts otrai pusei un no tās saņemts. Šajā ziņā kopā ar datnēm jāarhivē arī saistītie sertifikāti.

Šīs datnes sniegs arī papildu informāciju problēmu novēršanai.

Iekšējās revīzijas žurnāls

Šos žurnālus katra puse definē un izmanto pati.

3.5. **Operacionālās prasības**

Pastāvīgajā reģistru sasaistē datu apmaiņa starp abām sistēmām nav pilnīgi autonoma, proti, sasaistes operacionalizēšanai ir vajadzīgi operatori un procedūras. Šajā nolūkā šajā procesā ir detalizēti aprakstītas dažādas lomas un rīki.

4. PIEEJAMĪBAS NOTEIKUMI

4.1. Komunikācijas pieejamības nodrošināšana

Pastāvīgās reģistru sasaistes arhitektūra būtībā ir IKT infrastruktūra un programmatūra, kas nodrošina komunikāciju starp Šveices ETS un ES ETS. Tāpēc, izstrādājot pastāvīgo reģistru sasaisti, ir ļoti svarīgi šai datu plūsmai nodrošināt lielu pieejamību, integritāti un konfidencialitāti. Tā kā šajā projektā būtiska nozīme ir IKT infrastruktūrai, īpaši izstrādātajai programmatūrai un procesiem, noturīgas sistēmas izveidē ir jāņem vērā visi trīs elementi.

IKT infrastruktūras noturība

Šā dokumenta vispārīgo noteikumu nodaļā ir precizēti arhitektūras pamatelementi. IKT infrastruktūras pusē ar pastāvīgo reģistru sasaisti tiek izveidots noturīgs *VPN* ar drošiem komunikācijas tuneļiem, pa kuriem var notikt droša ziņojumu apmaiņa. Citi infrastruktūras elementi tiek konfigurēti ar augstu pieejamību un/vai rezerves mehānismiem.

Īpaši izstrādātās programmatūras noturība

Īpaši izstrādātie programmatūras moduļi uzlabo noturību, proti, tie noteiktu laika periodu sakarus ar otru galu cenšas izveidot vēlreiz, ja kāda iemesla dēļ tas nav izdevies.

Pakalpojumu noturība

Pastāvīgajā reģistru sasaistē datu apmaiņa starp pusēm notiek iepriekš noteiktos intervālos. Dažiem plānotās datu apmaiņas soļiem ir vajadzīga sistēmu operatoru un/vai reģistru administratoru manuāla iejaukšanās. Ņemot vērā šo aspektu un lai palielinātu apmaiņas pieejamību un sekmīgumu,

— darbības procedūrās katra soļa veikšanai paredz laika logus,

— pastāvīgās reģistru sasaistes programmatūras moduļi nodrošina asinhronu komunikāciju,

— automātiskās saskaņošanas procesā tiks atklāts, vai vienā vai otrā galā bijušas problēmas ar datu datņu uzņemšanu,

— monitorēšanas procesi (IKT infrastruktūra un īpaši izstrādāti programmatūras moduļi) tiek ņemti vērā incidentu pārvaldības procedūrās (kas noteiktas kopējo darbības procedūru dokumentā) un ir šo procedūru ierosinātāji. Minētās procedūras, kuru mērķis ir samazināt laiku līdz normālas darbības atjaunošanai pēc incidentiem, ir vajadzīgas, lai nodrošinātu augstus pieejamības rādītājus.

4.2. Inicializēšanas, komunikācijas reaktivizēšanas un testēšanas plāns

Lai pārliecinātos, ka platforma gan IKT infrastruktūras, gan informācijas sistēmas līmenī ir gatava, visi dažādie elementi, kas saistīti ar pastāvīgās reģistru sasaistes arhitektūru, iztur vairākus individuālus un kolektīvus testus. Šie operacionālie testi ir obligāts priekšnoteikums katru reizi, kad platformas pastāvīgās reģistru sasaistes operacionālais statuss mainās no "atslēgts" uz "operacionāls".

Sasaistes operacionālā statusa aktivizācijai pēc tam ir nepieciešams sekmīgi izpildīt iepriekš noteiktu testēšanas plānu. Tādējādi tiek apstiprināts, ka, pirms starp pusēm tiek sākta darba vides darījumu nosūtīšana, katrs reģistrs vispirms ir veicis iekšējo testu kopumu, kam seko savienotības "no gala līdz galam" validācija.

Testēšanas plānā jānorāda vispārējā testēšanas stratēģija un sīka informācija par testēšanas infrastruktūru. Konkrētāk, attiecībā uz katru elementu katrā testēšanas blokā būtu jānorāda

— testēšanas kritēriji un rīki,

— testa veikšanai piešķirtās lomas,

— gaidāmie rezultāti (pozitīvie un negatīvie),

— testēšanas grafiks,

— testēšanas rezultātu reģistrēšanas prasības,

— problēmu novēršanas dokumentācija,

— eskalācijas noteikumi.

Kā procesu operacionālā statusa aktivizācijas testus varētu iedalīt četros (4) konceptuālos blokos vai posmos, kas uzskaitīti nākamajos apakšpunktos.

4.2.1. *Iekšējie IKT infrastruktūras testi*

Paredzēts, ka šos testus reģistru administratori katrā galā veic un/vai pārbauda individuāli.

Katru IKT infrastruktūras elementu katrā galā testē atsevišķi. Testā ietver pilnīgi visus infrastruktūras komponentus. Šos testus var veikt automātiski vai manuāli, bet tiem jāverificē, ka pilnīgi visi infrastruktūras elementi ir operacionāli.

4.2.2. *Komunikācijas testi*

Minētos testus ierosina katra puse atsevišķi, un testu noslēgšanai ir vajadzīga otras puses sadarbība..

Kad atsevišķie elementi ir operacionāli, ir jātestē sakaru kanāli starp abiem reģistriem. Šajā nolūkā katra puse verificē, ka darbojas piekļuve internetam, ir izveidoti *VPN* tuneļi un ir nodrošināta starptīklu IP savienotība. Tad būtu otram galam jāapstiprina vietējo un attālināto infrastruktūras elementu sasniedzamība un IP savienotība.

4.2.3. *Pilnas sistēmas ("no gala līdz galam") testi*

Šos testus paredzēts veikt katrā galā, un rezultātus dara zināmus otrai pusei.

Kad sakaru kanāli un katrs atsevišķais abu reģistru komponents ir testēts, katrā galā sagatavo virkni simulētu darījumu un saskaņošanu, kas reprezentē visas sasaistes ietvaros izmantojamās funkcijas.

4.2.4. *Drošības testi*

Paredzēts, ka šos testus katrā galā veic un/vai ierosina reģistru administratori tā, kā izklāstīts 5.4. iedaļā "Drošības testēšanas vadlīnijas" un 5.5. iedaļā "Riska novērtēšanas noteikumi".

Tikai pēc tam, kad katrs no četriem posmiem/blokiem ir noslēdzies ar paredzamiem rezultātiem, pastāvīgo reģistru sasaisti var uzskatīt par operacionālu.

Testēšanas resursi

Katrai pusei ir īpaši testēšanas resursi (īpaša IKT infrastruktūras programmatūra un aparatūra), un katra puse savās sistēmās iestrādā testēšanas funkcijas, kas dotu iespēju platformu manuāli un pastāvīgi validēt. Reģistru administratori jebkurā laikā var veikt manuālas individuālas vai sadarbīgas testēšanas procedūras. Pati operacionālā statusa aktivizēšana ir manuāls process.

Tāpat ir paredzēts, ka platforma regulāri veiks automātiskas pārbaudes. Šo pārbaužu mērķis ir palielināt platformas pieejamību, jau agrīni atklājot iespējamas infrastruktūras vai programmatūras problēmas. Šis platformas monitorēšanas plāns sastāv no diviem elementiem:

— IKT infrastruktūras monitorēšana: infrastruktūru katrā galā monitorē IKT infrastruktūras pakalpojumu sniedzēji. Automātiskie testi aptvers visus dažādos infrastruktūras elementus un sakaru kanālu pieejamību;

— lietotņu monitorēšana: pastāvīgās reģistru sasaistes programmatūras moduļi nodrošinās sistēmu komunikācijas monitorēšanu lietotņu līmenī (manuāli un/vai ar regulāriem intervāliem), kā ietvaros sasaistes pieejamība tiks testēta no viena gala līdz otram, sasaistē simulējot dažus darījumus.

4.3. **Akceptēšanas vide / testēšanas vide**

Savienības reģistra un Šveices reģistra arhitektūru veido šādas trīs vides:

— darba vide (*PROD*): šajā vidē glabājas reālie dati un tiek apstrādāti reālie darījumi;

— akceptēšanas vide (*ACC*): šajā vidē tiek izmantoti nereāli vai anonimizēti reprezentatīvi dati. Tā ir vide, kurā abu pušu sistēmu operatori validē jaunus laidumus;

— testēšanas vide (*TEST*): šajā vidē tiek izmantoti nereāli vai anonimizēti reprezentatīvi dati. Šo vidi izmanto tikai reģistru administratori, un tā domāta tam, lai abas puses veiktu integrācijas testus.

Izņemot *VPN*, šīs trīs vides ir cita no citas pilnīgi neatkarīgas, proti, aparatūra, programmatūra, datubāzes, virtuālās vides, IP adreses un porti ir ierīkoti un darbojas neatkarīgi.

Kas attiecas uz *VPN* izkārtojumu, komunikācijai starp visām trim vidēm jābūt pilnīgi neatkarīgai, un to nodrošina, izmantojot *STESTA*.

5. **KONFIDENCIALITĀTES UN INTEGRITĀTES NOTEIKUMI**

Drošības mehānismi un procedūras attiecībā uz operācijām, kas notiek sasaistē starp Savienības reģistru un Šveices reģistru, paredz divu personu lomu (četru acu princips). Divu personu lomu izmanto, kad vien nepieciešams. Tomēr šī loma var nebūt vajadzīga visos reģistru administratoru soļos.

Drošības prasības ir ņemtas vērā un aplūkotas drošības pārvaldības plānā, kas ietver arī procesus, kuri saistīti ar drošības incidentu risināšanu pēc eventuāla drošības pārkāpuma. Šo procesu operacionālā daļa ir aprakstīta KDP.

5.1 **Drošības testēšanas infrastruktūra**

Katra puse apņemas izveidot drošības testēšanas infrastruktūru (izmantojot kopīgu programmatūru un aparatūru, ko izmanto, lai atklātu ievainojamības izstrādes un darbības posmos),

— nošķirti no darba vides,

— tā, ka drošību analizē no sistēmas izstrādes un darbības neatkarīga komanda.

Katra puse apņemas veikt gan statisko, gan dinamisko analīzi.

Dinamiskās analīzes gadījumā (piem., ielaušanās testēšana) abas puses apņemas izvērtējumus parasti attiecināt tikai uz testēšanas un akceptēšanas vidēm (kas definētas 4.3. iedaļā "Akceptēšanas vide / testēšanas vide"). Šīs politikas izņēmumus apstiprina abas puses.

Pirms ieviešanas darba vidē katram sasaistes programmatūras modulim (kas definēts 3.1. iedaļā "Komunikācijas līnijas arhitektūra") veic drošības testēšanu.

Testēšanas infrastruktūrai gan tīkla, gan infrastruktūras līmenī jābūt nodalītai no darba infrastruktūras. Drošības testus, kas vajadzīgi, lai pārbaudītu atbilstību drošības prasībām, veic testēšanas infrastruktūrā.

5.2 **Sasaistes apturēšanas un reaktivizēšanas noteikumi**

Ja ir aizdomas, ka Šveices reģistra, *SSTL*, Savienības reģistra vai *EUTL* drošība ir kompromitēta, attiecīgā puse nekavējoties par to informē otru un sasaisti starp *SSTL* un *EUTL* aptur.

Informācijas kopīgošanas, apturēšanas lēmuma un reaktivizēšanas lēmuma procedūras ir KDP pieprasījuma izpildes procesa daļa.

Apturēšana

Reģistru sasaistes apturēšana saskaņā ar Nolīguma II pielikumu var notikt šādu iemeslu dēļ:

— administratīvi iemesli (piemēram, uzturēšana), kas ir plānoti,

— drošības apsvērumi (vai IT infrastruktūras bojājumi), kas ir neplānoti.

Ārkārtas gadījumā viena no pusēm informē otru pusi un reģistru sasaisti vienpusēji aptur.

Ja tiek pieņemts lēmums reģistru sasaisti apturēt, katra puse nodrošina, ka sasaiste tiek pārtraukta tīkla līmenī (bloķējot daļu ienākošo un izejošo savienojumu vai tos visus).

Lēmums par reģistru sasaistes apturēšanu neatkarīgi no tā, vai tā ir plānota vai neplānota, tiks pieņemts saskaņā ar KDP noteikto izmaiņu pārvaldības vai drošības incidentu pārvaldības procedūru.

Komunikācijas reaktivizēšana

Lēmums par reģistru sasaistes reaktivizēšanu tiks pieņemts tā, kā norādīts KDP, un jebkurā gadījumā ne pirms tam, kad sekmīgi pabeigtas drošības testēšanas procedūras, kas izklāstītas 5.4. iedaļā "Drošības testēšanas vadlīnijas" un 4.2. iedaļā "Inicializēšanas, komunikācijas reaktivizēšanas un testēšanas plāns".

5.3 **Noteikumi par drošības pārkāpumiem**

Par drošības pārkāpumu uzskata drošības incidentu, kas ietekmē jebkādas sensitīvas informācijas konfidencialitāti un integritāti un/vai tās sistēmas pieejamību, kas ar šo informāciju rīkojas.

Sensitīva informācija ir norādīta sensitīvās informācijas sarakstā, un to var apstrādāt sistēmā vai jebkurā ar sistēmu saistītā daļā.

Informāciju, kas tieši saistīta ar drošības pārkāpumu, uzskata par sensitīvu, atzīmē ar grifu "*SPECIAL HANDLING: ETS Critical*" un, ja vien nav norādīts citādi, apstrādā saskaņā ar rīkošanās instrukcijām.

Katrs drošības pārkāpums tiks risināts saskaņā ar KDP nodaļu par drošības incidentu pārvaldību.

5.4 **Drošības testēšanas vadlīnijas**

5.4.1 *Programmatūra*

Lai novērtētu sasaistes drošību un ar to saistītos riskus, vismaz visiem jauniem nozīmīgiem programmatūras laidumiem saskaņā ar STS noteiktajām drošības prasībām veic drošības testus, attiecīgā gadījumā arī ielaušanās testus.

Ja pēdējo 12 mēnešu laikā nozīmīga jauna laiduma nav bijis, veic tābrīža sistēmas drošības testu, ņemot vērā kiberdraudu dinamiku pēdējos 12 mēnešos.

Reģistru sasaistes drošības testēšanu veic akceptēšanas vidē un, ja vajadzīgs, darba vidē, abām pusēm koordinējoties un savstarpēji vienojoties.

Tīmekļa lietotņu testēšanā tiks ievēroti starptautiskie atvērtie standarti, piem., tie, kas izstrādāti atvērtā tīmekļa lietotņu drošības projektā (*OWASP*).

5.4.2 *Infrastruktūra*

Darba sistēmas atbalsta infrastruktūru regulāri (vismaz reizi mēnesī) skenē, meklējot ievainojamības, un atklātās ievainojamības novērš pēc tā paša principa, kas noteikts iepriekšējā iedaļā, izmantojot atjauninātu ievainojamību datubāzi.

5.5 **Riska novērtēšanas noteikumi**

Ja ir piemērojama ielaušanās testēšana, tā jāiekļauj drošības testēšanā.

Katra puse var par drošības testēšanas veikšanu noslēgt līgumu ar specializētu uzņēmumu, ja ir izpildīti šādi nosacījumi:

— uzņēmumam ir šādai drošības testēšanai vajadzīgās prasmes un pieredze,

— uzņēmums nav tieši pakļauts izstrādātājam un/vai tā darbuzņēmējam un nav ne iesaistīts sasaistes programmatūras izstrādē, ne arī izstrādātāja apakšuzņēmējs,

— uzņēmums ir parakstījis informācijas neizpaušanas līgumu, kurā apņemas saglabāt rezultātu konfidencialitāti un tos apstrādāt līmenī "*SPECIAL HANDLING: ETS Critical*" saskaņā ar rīkošanās instrukcijām.