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]

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 3. panta 7. punktu un 13. panta 2. punktu,

tā kā:

(1) Ar Apvienotās komitejas 2019. gada 5. decembra Lēmumu Nr. 2/2019 [2] tika grozīts Nolīguma I un II pielikums, tādējādi izpildot Nolīgumā izklāstītos sasaistes nosacījumus.

(2) Pēc Apvienotās komitejas Lēmuma Nr. 2/2019 pieņemšanas un saskaņā ar Nolīguma 21. panta 3. punktu puses apmainījās ar saviem ratifikācijas vai apstiprināšanas instrumentiem, jo uzskatīja, ka visi Nolīgumā noteiktie sasaistes nosacījumi ir izpildīti.

(3) Saskaņā ar Nolīguma 21. panta 4. punktu Nolīgums stājās spēkā 2020. gada 1. janvārī.

(4) Lai nodrošinātu vienmērīgu pāreju Šveicei pirmo reizi iedalīto gaisa kuģu operatoru administrēšanā, ņemot vērā progresu, kas panākts reģistru sasaistē, saskaņā ar Nolīguma 13. panta 2. punktu būtu jāgroza Nolīguma I pielikums.

(5) Lai ņemtu vērā jaunākās norises un nodrošinātu lielāku elastību Nolīgumā prasītajā reģistru sasaistē, Nolīguma II pielikums saskaņā ar 13. panta 2. punktu būtu jāgroza, lai sasaistes izveidei paredzētu lielāku, bet līdzvērtīgu tehnoloģiju kopumu.

(6) Nolīguma 3. panta 7. punkts paredz, ka Šveices reģistra administrators un Savienības centrālais administrators, balstoties uz Nolīguma II pielikumā izklāstītajiem principiem, izstrādā sasaistes tehniskos standartus (STS). STS būtu sīki jāapraksta prasības stabila un droša savienojuma izveidei starp Šveices papildu darījumu žurnālu (*SSTL*) un Eiropas Savienības darījumu žurnālu (*EUTL*). STS būtu jāstājas spēkā, kad tie ir pieņemti ar Apvienotās komitejas lēmumu.

(7) Saskaņā ar Nolīguma 13. panta 1. punktu Apvienotajai komitejai būtu jāvienojas par tehniskām vadlīnijām nolūkā nodrošināt pareizu Nolīguma īstenošanu, arī – izveidot stabilu un drošu savienojumu starp *SSTL* un *EUTL*. Tehniskās vadlīnijas var izstrādāt darba grupa, ko izveido saskaņā ar Nolīguma 12. panta 5. punktu. Darba grupā būtu jāiekļauj vismaz Šveices reģistra administrators un Savienības centrālais administrators, un tai būtu jāpalīdz Apvienotajai komitejai veikt tās funkcijas saskaņā ar Nolīguma 13. pantu.

(8) Ņemot vērā vadlīniju tehnisko raksturu un vajadzību tās pielāgot situācijas attīstībai, Šveices reģistra administratora un Savienības centrālā administratora izstrādātās tehniskās vadlīnijas būtu jāiesniedz Apvienotajai komitejai informēšanas vai – attiecīgā gadījumā – apstiprināšanas nolūkā,

---

[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 2019. gada 5. decembra Lēmums Nr. 2/2019, ar ko groza Nolīguma starp Eiropas Savienību un Šveices Konfederāciju par siltumnīcefekta gāzu emisijas kvotu tirdzniecības sistēmu sasaisti I un II pielikumu (OV L 314, 29.9.2020., 68. lpp.).

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Nolīguma I pielikuma B daļas 17. punkta otro daļu aizstāj ar šādu tekstu:

"Gaisa kuģu operatorus, kurus Šveicei pirmo reizi iedala pēc šā nolīguma stāšanās spēkā, Šveice sāk administrēt pēc iedalīšanas gada 30. aprīļa un kad notikusi provizoriskā reģistru sasaiste."

2. pants

Nolīguma II pielikuma ceturto daļu aizstāj ar šādu tekstu:

"STS norāda, ka komunikācija starp *SSTL* un *EUTL* notiek kā tīmekļa pakalpojumu ziņojumu droša apmaiņa, izmantojot šādas (*) vai līdzvērtīgas tehnoloģijas:

— tīmekļa pakalpojumi, kuros izmanto vienkāršo objektpiekļuves protokolu (*SOAP*),

— virtuāls privātais tīkls (*VPN*) uz datortehnikas bāzes,

— XML (paplašināmās iezīmēšanas valoda),

— digitālais paraksts un

— tīkla laika protokoli.

_____

(*) Šīs tehnoloģijas pašlaik izmanto, lai nodrošinātu savienojumu starp Savienības reģistru un Starptautisko darījumu žurnālu, kā arī starp Šveices reģistru un Starptautisko darījumu žurnālu."

3. pants

Ar šo tiek pieņemti šim lēmumam pievienotie sasaistes tehniskie standarti (STS).

4. pants

Ar šo izveido darba grupu saskaņā ar Nolīguma 12. panta 5. punktu. Tā palīdz Apvienotajai komitejai ar mērķi nodrošināt pareizu Nolīguma īstenošanu, arī izstrādāt STS īstenošanas tehniskās vadlīnijas.

Darba grupā ietilpst vismaz Šveices reģistra administrators un Savienības centrālais administrators.

5. pants

Šis lēmums stājas spēkā tā pieņemšanas dienā.

Briselē, 2020. gada 5. novembrī

Apvienotās komitejas vārdā –	priekšsēdētāja	sekretāre no Šveices puses
sekretāre no Eiropas Savienības puses	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

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

PAGAIDU RISINĀJUMA STANDARTI

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 ES ETS vai Šveices ETS prasību izpildei.
CH	Šveices Konfederācija
CHU	Šveices vispārīgās kvotas (apzīmējumu *CHU2* izmanto 2. saistību perioda *CHU* apzīmēšanai)
CHUA	Šveices aviācijas kvota
KDP	Kopējās darbības procedūras, ko kopīgi izstrādājušas Nolīguma puses, lai nodrošinātu ES ETS un Šveices ETS sasaistes funkcionēšanu.
ETR	Emisijas kvotu tirdzniecības reģistrs
ETS	Emisijas kvotu tirdzniecības sistēma
ES	Eiropas Savienība
EUA	ES vispārīgā kvota
EUAA	ES aviācijas kvota
EUCR	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.

Akronīms	Definīcija
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.
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.
IPsec	IP drošība (*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*) 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, līdz 2020. gada maijam vai iespējami drīz pēc tam ievieš pagaidu risinājumu. Puses sadarbojas, lai reģistru sasaistes pagaidu risinājumu iespējami drīz aizstātu ar pastāvīgu sasaisti (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.

Šajā dokumentā izklāstītos STS Apvienotā komiteja grasās pieņemt ar Lēmumu Nr. 2/2020. Saskaņā ar šo lēmumu Apvienotā komiteja prasa Šveices reģistra administratoram un Savienības centrālajam administratoram izstrādāt sīkākas tehniskās vadlīnijas, kas nepieciešamas, lai nodrošinātu sasaistes funkcionēšanu, tās pastāvīgu pielāgošanu tehnikas attīstībai un jaunām prasībām, kuras saistītas ar sasaistes drošumu un drošību, un tās rezultatīvu un efektīvu darbību.

2.1. *Darbības joma*

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 sasaiste 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 atsevišķā kopējo darbības procedūru (KDP) dokumentā, ko Apvienotā komiteja ar attiecīgu lēmumu pieņems atsevišķi.

2.2. *Adresāti*

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

3. **Vispārīgie 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. Lai gan paredzētā pastāvīgā reģistru sasaiste balstīsies uz tīmekļa pakalpojumiem, pagaidu risinājumā tā vietā tiks izmantots datņu apmaiņas mehānisms.

Tehniskajā risinājumā izmanto šādus elementus:

— drošas ziņojumu apmaiņas pārsūtīšanas protokols,

— XML ziņojumi,

— uz XML balstīts digitālais paraksts un šifrēšana,

— *VPN* ierīce vai līdzvērtīgs drošs datu pārsūtīšanas tīkls.

3.1.1. Ziņojumu apmaiņa

Komunikācija starp Savienības reģistru un Šveices reģistru balstīsies uz ziņojumu apmaiņas mehānismu, kurā tiks izmantoti droši kanāli. Katrai sistēmai būs savs saņemto ziņojumu repozitorijs.

Abas puses saņemtos ziņojumus reģistrēs 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 tiks ievērotas darbības procedūras, kas noteiktas KDP incidentu pārvaldības procesā.

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.

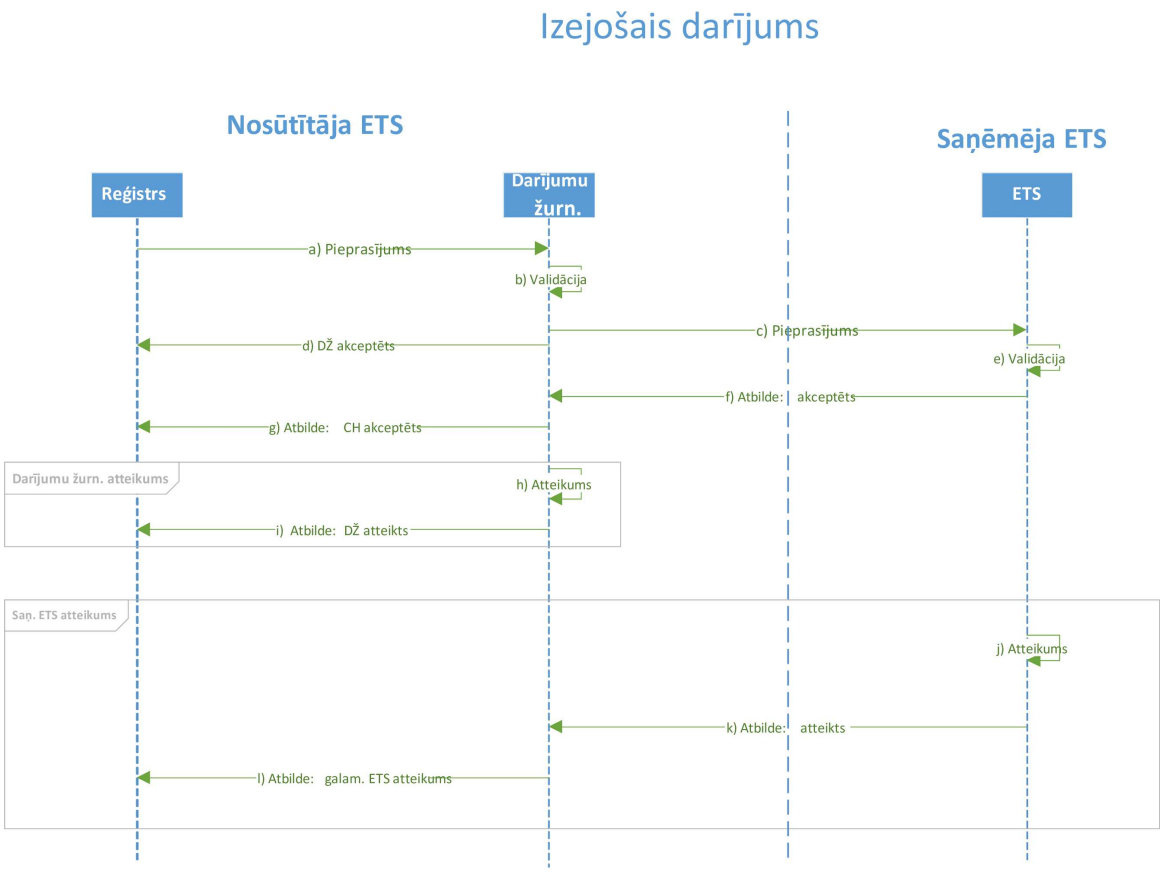
3.1.3. Uzņemšanas logi

Pagaidu risinājums ir balstīts 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 jebkura šā notikuma 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. Augstāk redzamajā secības diagrammā ir attēlotas visas specifiskās izejošās darījumu plūsmas.

Pamatplūsma "Parasts darījums" (ar soļiem, kas redzami attēlā):

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.

Alternatīvā plūsma "Darījumu žurnāla atteikums" (ar iepriekš attēlā redzamajiem soļiem, kas tāpat sākas ar a) soli):

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

pēc tam:

b) darījumu žurnāls pieprasījumu nevalidē;

c) izcelsmes reģistram tiek nosūtīts atteikuma ziņojums.

Alternatīvā plūsma "ETS atteikums" (ar iepriekš attēlā redzamajiem soļiem, kas sākas ar a) soli):

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.

Pēc tam:

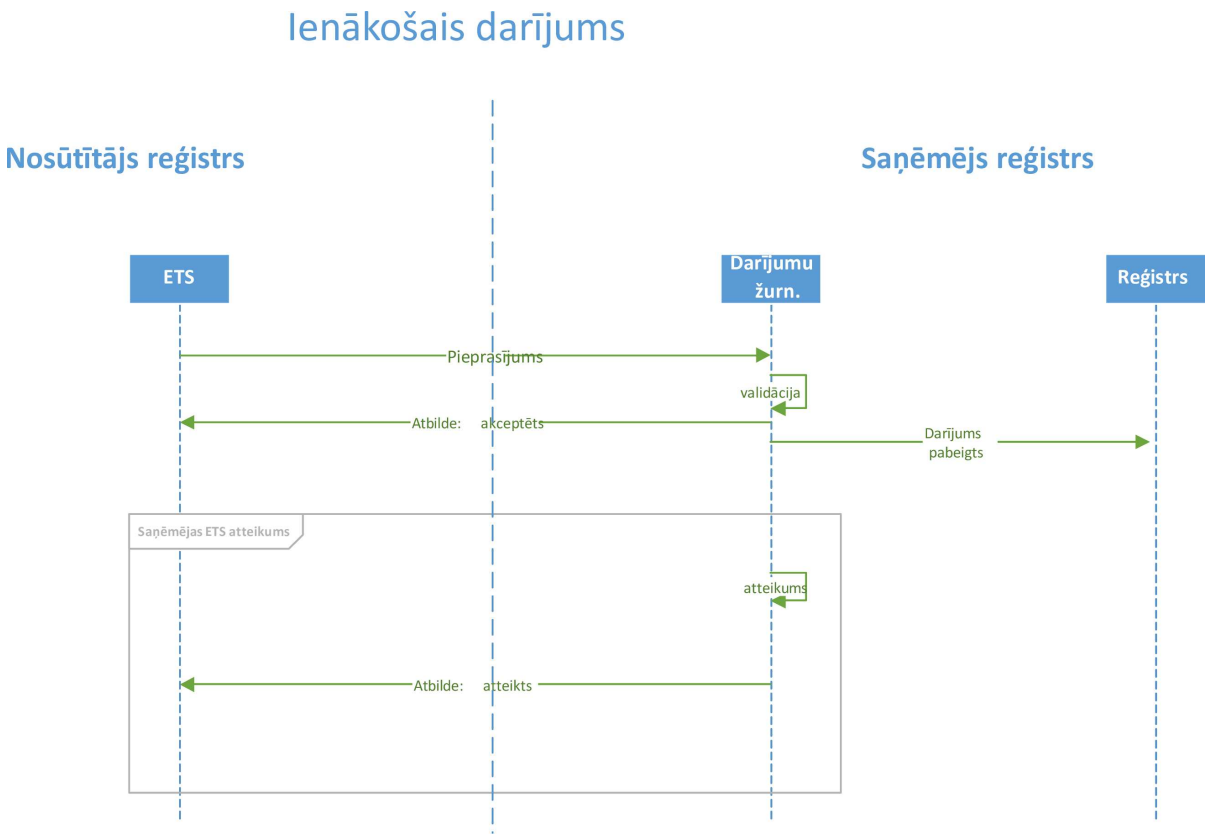
e) saņēmējas ETS darījumu žurnāls darījumu nevalidē;

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 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* vai līdzvērtīgs drošs datu transportēšanas tīkls;

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 drošu datu transportēšanas tehnoloģiju. Virtuālā privātā tīkla (*VPN*) gadījumā infrastruktūras pamatā vajadzētu būt vai nu aparatūrai, vai virtuālām ierīcēm. *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.

Jebkuram citam līdzvērtīgam risinājumam jābūt atbilstīgam iepriekš minētajiem principiem.

3.2.3. *IPsec* ieviešana

Ja izmanto *VPN* risinājumu, *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, pagaidu risinājums balstās uz vairākiem šifrēšanas slāņiem. Abas sistēmas un to dažādās vides tīkla līmenī ir starpsavienotas, izmantojot *VPN* tuneļus vai līdzvērtīgus drošus datu transportēšanas tīklus. Lietotnes līmenī datnes tiek pārsūtītas, izmantojot drošas ziņojumu apmaiņas 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 saknes elementa 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. *Tīmekļa pakalpojumu standarti*

Tīmekļa pakalpojumi pagaidu risinājumā izmantoti netiks. Tomēr ir vērts atzīmēt, ka XML ziņojumu forma un formāts lielā mērā paliks tāds pats. Līdz ar pastāvīgas reģistru sasaistes ieviešanu nākotnē tīmekļa pakalpojumiem būtu jānodrošina XML ziņojumu apmaiņa reāllaikā.

3.5. *Specifiskā tīmekļa pakalpojumu definīcija*

Šī iedaļa uz pagaidu risinājumu neattiecas. Kā minēts iepriekšējā iedaļā, tīmekļa pakalpojumi tiks izmantoti tikai gaidāmajā pastāvīgajā reģistru sasaistē.

3.6. *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 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". Pagaidu risinājumā saskaņošanas ziņojumi ir neatņemama savstarpēji nosūtīto ziņojumu daļa.

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.

3.7. *Operacionālās prasības*

Pagaidu risinājumā datu apmaiņa starp abām sistēmām nav pilnīgi autonoma; tas nozīmē, ka sasaistes operacionalizēšanai ir vajadzīgi operatori un procedūras.

4. **Pieejamības noteikumi**

4.1. *Komunikācijas pieejamības nodrošināšana*

Pagaidu risinājuma arhitektūra būtībā ir IKT infrastruktūra un programmatūra, kas nodrošina saziņu starp Šveices ETS un ES ETS. Tāpēc, izstrādājot pagaidu risinājumu un 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 pagaidu sasaisti tiek izveidots noturīgs *VPN* (vai līdzvērtīgs tīkls) 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

Pagaidu risinājumā datu apmaiņa starp pusēm notiek iepriekš noteiktos laikos visu gadu. 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 izpildei paredz ievērojamus laika logus,

— pagaidu risinājuma 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 pagaidu risinājuma arhitektūru, iztur vairākus individuālus un kolektīvus testus. Šie operacionālie testi ir obligāts priekšnoteikums katru reizi, kad platformas pagaidu risinājuma 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 katra puse 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

Šos 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 (vai līdzvērtīgs drošs transportēšanas tīkls) un ir nodrošināta starptīklu IP savienotība. Tad otrā galā būtu 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 pārbaudīts, 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 abas puses 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, pagaidu 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 agri 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: pagaidu 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 jaunas versijas,

— 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* (vai līdzvērtīgu tīklu), 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, to veido divās dažādās vidēs, no kurām viena ir PROD, bet otra (neatkarīga) – ACC un TEST.

5. **Konfidencialitātes un integritātes noteikumi**

Drošības mehānismi un procedūras attiecībā uz operācijām, kas notiek sasaistē starp Savienības reģistru un Šveices reģistru, paredz divu personu pieeju (četru acu princips). Šo divu personu pieeju izmanto, kad vien nepieciešams. Tomēr tā var nebūt piemērojama visiem soļiem, ko veic reģistra administratori.

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 to saistītā sistēmas daļā.

Informāciju, kas tieši saistīta ar drošības pārkāpumu, uzskata par sensitīvu, atzīmē ar grifu "ETS KRITISKI SVARĪGA INFORMĀCIJA" 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 visām jaunām nozīmīgām programmatūras versijām saskaņā ar STS noteiktajām drošības prasībām veic drošības testus, attiecīgā gadījumā arī ielaušanās testus.

Ja pēdējo 12 mēnešu laikā nozīmīgu jaunu versiju 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. Testēšanu veic saskaņā ar 5.4.1. iedaļā izklāstīto metodi, 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 "ETS KRITISKI SVARĪGA INFORMĀCIJA" saskaņā ar rīkošanās instrukcijām.