EUROPOS SĄJUNGOS IR ŠVEICARIJOS KONFEDERACIJOS SUSITARIMU DĖL JŲ ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ APYVARTINIŲ TARŠOS LEIDIMŲ PREKYBOS SISTEMŲ SUSIEJIMO ĮSTEIGTO JUNGTINIO KOMITETO SPRENDIMAS Nr. 2/2020

2020 m. lapkričio 5 d.

dėl Susitarimo I ir II priedų pakeitimo ir susiejimo techninių standartų priėmimo (2021/1034)

JUNGTINIS KOMITETAS,

atsižvelgdamas į Europos Sąjungos ir Šveicarijos Konfederacijos susitarimą dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo [1] (toliau – Susitarimas), ypač į jo 3 straipsnio 7 dalį ir 13 straipsnio 2 dalį,

kadangi:

(1) 2019 m. gruodžio 5 d. Jungtinio komiteto sprendimu Nr. 2/2019 [2] Susitarimo I ir II priedai buvo iš dalies pakeisti ir taip buvo įvykdytos Susitarime nustatytos susiejimo sąlygos;

(2) Jungtiniam komitetui priėmus Sprendimą Nr. 2/2019, Šalys, vadovaudamosi Susitarimo 21 straipsnio 3 dalimi, apsikeitė ratifikavimo arba patvirtinimo dokumentais, nes, jų manymu, visos Susitarime apibrėžtos susiejimo sąlygos buvo įvykdytos;

(3) pagal Susitarimo 21 straipsnio 4 dalį Susitarimas įsigaliojo 2020 m. sausio 1 d.;

(4) siekiant užtikrinti sklandų Šveicarijai pirmą kartą priskirto orlaivių naudotojų administravimo pereinamąjį etapą ir atsižvelgiant į padarytą registrų jungties kūrimo pažangą, Susitarimo I priedas turėtų būti iš dalies pakeistas pagal Susitarimo 13 straipsnio 2 dalį;

(5) siekiant prisitaikyti prie naujausių pokyčių ir užtikrinti didesnį lankstumą kuriant Susitarime reikalaujamą jungtį, Susitarimo II priedą reikėtų iš dalies pakeisti pagal Susitarimo 13 straipsnio 2 dalį, kad būtų galima numatyti didesnį, tačiau lygiavertį registrų jungties diegimo technologijų paketą;

(6) pagal Susitarimo 3 straipsnio 7 dalį Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius, vadovaudamiesi Susitarimo II priede išdėstytais principais, turėtų parengti susiejimo techninius standartus (toliau – STS). STS turėtų būti išdėstyti išsamūs patikimos ir saugios Šveicarijos papildomų sandorių žurnalo (angl. *Swiss Supplementary Transaction Log*, toliau – SSTL) ir Europos Sąjungos sandorių žurnalo (toliau – ESSŽ) jungties kūrimo reikalavimai. STS turėtų įsigalioti, kai juos sprendimu patvirtina Jungtinis komitetas;

(7) pagal Susitarimo 13 straipsnio 1 dalį Jungtinis komitetas turėtų susitarti dėl techninių gairių, kuriomis būtų užtikrintas tinkamas Susitarimo įgyvendinimas, įskaitant techninius ar kitus klausimus, būtinus saugiai ir patikimai SSTL ir ESSŽ jungčiai sukurti. Technines gaires gali parengti pagal Susitarimo 12 straipsnio 5 dalį sudaryta darbo grupė. Į ją turėtų būti įtraukti bent Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius; ji turėtų padėti Jungtiniam komitetui vykdyti Susitarimo 13 straipsnyje nurodytas funkcijas;

(8) atsižvelgiant į techninį gairių pobūdį ir tai, kad jas reikės koreguoti atsižvelgiant į vykstančius pokyčius, Šveicarijos registro administratoriaus ir Sąjungos vyriausiojo administratoriaus parengtos techninės gairės turėtų būti teikiamos Jungtiniam komitetui susipažinti arba, jei reikia, patvirtinti,

[1] OL L 322, 2017 12 7, p. 3.

[2] 2019 m. gruodžio 5 d. Europos Sąjungos ir Šveicarijos Konfederacijos susitarimu dėl jų apyvartinių taršos leidimų prekybos sistemų susiejimo įsteigto Jungtinio komiteto sprendimas Nr. 2/2019, kuriuo iš dalies keičiami Europos Sąjungos ir Šveicarijos Konfederacijos susitarimo dėl jų apyvartinių taršos leidimų prekybos sistemų susiejimo I ir II priedai (OL L 314, 2020 9 29, p. 68).

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Susitarimo I priedo B dalies 17 punkto antra pastraipa pakeičiama taip:

„Orlaivių naudotojus, kurie bus pirmą kartą priskirti Šveicarijai po to, kai įsigalios šis Susitarimas, Šveicarija pradeda administruoti po priskyrimo metų balandžio 30 d., kai pradės veikti laikina registrų jungtis.“

2 straipsnis

Susitarimo II priedo ketvirta pastraipa pakeičiama taip:

„STS turi būti nurodyta, kad SSTL ir ESSŽ ryšys palaikomas saugiai keičiantis saityno paslaugų pranešimais ir yra grindžiamas šiomis (*) arba lygiavertėmis technologijomis:

— saityno paslaugomis, kurioms naudojamas paprastosios kreipties į objektus (SOAP) protokolas;

— aparatine įranga grindžiamu virtualiuoju privačiuoju tinklu (VPN);

— XML kalba (angl. *Extensible Markup Language*);

— skaitmeniniu parašu ir

— tinklo laiko protokolais.“

(*) Šios technologijos šiuo metu naudojamos ryšiui tarp Sąjungos registro ir Tarptautinio sandorių žurnalo, taip pat ryšiui tarp Šveicarijos registro ir Tarptautinio sandorių žurnalo užmegzti.

3 straipsnis

Priimami prie šio sprendimo pridėti susiejimo techniniai standartai (toliau – STS).

4 straipsnis

Vadovaujantis Susitarimo 12 straipsnio 5 dalimi, sudaroma darbo grupė. Ji padeda Jungtiniam komitetui užtikrinti tinkamą Susitarimo įgyvendinimą, tarp kitų dalykų – parengti STS įgyvendinti reikalingas technines gaires.

Į darbo grupę įtraukiamas bent Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius.

5 straipsnis

Šis sprendimas įsigalioja jo priėmimo dieną.

Priimta Briuselyje 2020 m. lapkričio 5 d.

Jungtinio komiteto vardu	Pirmininkė	Šveicarijos sekretorė
Europos Sąjungos sekretorė	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

PRIEDAS

Susiejimo techniniai standartai (STS) pagal Europos Sąjungos ir Šveicarijos Konfederacijos susitarimo dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo 3 straipsnio 7 dalį

LAIKINI STANDARTAI

1. **Sąvokų žodynėlis**

1-1 lentelė

Su veikla susijusios santrumpos ir apibrėžtys

Santrumpa, sąvoka	Apibrėžtis
Apyvartinis taršos leidimas	Vienos tonos anglies dioksido ekvivalento išmetimo per nustatytą laiką leidimas, kuris galioja tik siekiant, kad būtų laikomasi ES ATLPS arba Šveicarijos ATLPS reikalavimų
ŠK	Šveicarijos Konfederacija
CHU	Šveicarijos paprastieji apyvartiniai taršos leidimai (angl. *Swiss general allowances*) (Santrumpa „CHU2“ vartojama kalbant apie antrojo įsipareigojimų laikotarpio CHU leidimus)
CHUA	Šveicarijos aviacijos apyvartiniai taršos leidimai
BDP	Susitarimo šalių kartu parengtos bendros darbo procedūros, skirtos ES ATLPS ir Šveicarijos ATLPS praktiškai susieti
ATLR	Apyvartinių taršos leidimų registras
ATLPS	Apyvartinių taršos leidimų prekybos sistema
ES	Europos Sąjunga
EUA	ES paprastasis apyvartinis taršos leidimas (angl. *EU General Allowance*)
EUAA	ES aviacijos apyvartinis taršos leidimas (angl. *EU Aviation Allowance*)
ESKR	Europos Sąjungos konsoliduotas registras
ESSŽ	Europos Sąjungos sandorių žurnalas
Registras	Pagal ATLPS išduotų leidimų apskaitos sistema, suteikianti galimybę stebėti elektroninėse sąskaitose laikomų leidimų nuosavybę
SSTL	Šveicarijos papildomų sandorių žurnalas (angl. *Swiss Suplementary Transaction Log*)
Sandoris	Registre vykdomas procesas, per kurį apyvartinis taršos leidimas perkeliamas iš vienos sąskaitos į kitą
Sandorių žurnalo sistema	Sandorių žurnale saugomi kiekvieno pasiūlymo dėl sandorio, išsiųsto iš vieno registro į kitą, įrašai

1-2 lentelė

Techninės santrumpos ir apibrėžtys

Santrumpa	Apibrėžtis
Asimetrinė kriptografija	Viešųjų ir privačiųjų raktų naudojimas duomenims užšifruoti ir iššifruoti
Skaitmeninius sertifikatus teikianti organizacija	Skaitmeninius sertifikatus išduodantis subjektas

Santrumpa	Apibrėžtis
Kriptografinis raktas	Informacijos vienetas, pagal kurį nustatomas kriptografinio algoritmo funkcinis rezultatas
Iššifravimas	Užšifravimui priešingas procesas
Skaitmeninis parašas	Matematinis metodas, naudojamas pranešimo, programinės įrangos arba skaitmeninio dokumento autentiškumui ir vientisumui patvirtinti
Užšifravimas	Procesas, per kurį informacija arba duomenys paverčiami kodu, ypač siekiant užkirsti kelią neleistinai prieigai
Failo nuskaitymas	Failo skaitymo procesas
Užkarda	Tinklo apsaugos taikomoji programa arba programinė įranga, kuria pagal apibrėžtas taisykles stebimi ir kontroliuojami tinkle gaunami ir siunčiami duomenys
Veikimo stebėsena	Periodiškas signalas, kuris skleidžiamas ir stebimas aparatine arba programine įranga siekiant stebėti, ar darbas vyksta įprasta tvarka arba siekiant sinchronizuoti kitas kompiuterinės sistemos dalis (angl. *heartbeat monitoring*)
IPSec	„IP SECurity“ tinklo protokolų komplektas, kuriuo patvirtinamas duomenų autentiškumas ir užšifruojami duomenų paketai, kad tarp dviejų kompiuterių būtų užtikrintas saugus užšifruotas interneto protokolo tinklo ryšys
Prasiskverbimo bandymai	Kompiuterinės sistemos, tinklo arba saityno taikomosios programos bandymai siekiant nustatyti saugumo požiūriu pažeidžiamas vietas, kuriomis galėtų pasinaudoti išpuolių rengėjai
Suderinimo procesas	Procesas, kuriuo užtikrinama, kad du įrašų rinkiniai atitiktų vienas kitą
VPN	Virtualusis privatusis tinklas (angl. *Virtual Private Network*)
XML	XML kalba. Ja naudodamiesi projektuotojai rengia savas individualizuotas žymes, suteikiančias galimybę duomenis apibrėžti, perduoti, patvirtinti ir aiškinti įvairiose taikomosiose programose ir įvairiose organizacijose.

2. **Įžanga**

2017 m. lapkričio 23 d. Europos Sąjungos ir Šveicarijos Konfederacijos susitarime dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo (toliau – Susitarimas) numatytas abipusis apyvartinių taršos leidimų, kuriuos galima naudoti atitikčiai užtikrinti pagal Europos Sąjungos apyvartinių taršos leidimų prekybos sistemą (toliau – ES ATLPS) arba Šveicarijos apyvartinių taršos leidimų prekybos sistemą (toliau – Šveicarijos ATLPS), pripažinimas. Siekiant praktiškai susieti ES ATLPS ir Šveicarijos ATLPS bus sukurta tiesioginė jungtis tarp Sąjungos registro Europos Sąjungos sandorių žurnalo (toliau – ESSŽ) ir Šveicarijos registro Šveicarijos papildomų sandorių žurnalo (angl. *Swiss Supplementary Transaction Log*, toliau – SSTL), kad pagal bet kurią iš šių dviejų ATLPS išduoti apyvartiniai taršos leidimai galėtų būti perkelti iš vieno registro į kitą (Susitarimo 3 straipsnio 2 dalis). Siekiant praktiškai susieti ES ATLPS ir Šveicarijos ATLPS, iki 2020 m. gegužės mėn. arba kuo anksčiau po šios datos pradedamas taikyti laikinas sprendimas. Šalys bendradarbiauja siekdamos kuo anksčiau pakeisti šį laikiną sprendimą nuolatine registrų jungtimi (Susitarimo II priedas).

Pagal Susitarimo 3 straipsnio 7 dalį Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius, remdamiesi II priede nustatytais principais, parengia susiejimo techninius standartus (toliau – STS) ir juose išdėsto išsamius reikalavimus, kaip turi būti sukurta patikima ir saugi SSTL ir ESSŽ jungtis. Administratorių parengti STS įsigalioja, kai juos sprendimu patvirtina Jungtinis komitetas.

Šiame dokumente išdėstytus STS sprendimu Nr. 2/2020 turi patvirtinti Jungtinis komitetas. Pagal šį sprendimą Jungtinis komitetas prašo Šveicarijos registro administratoriaus ir Sąjungos vyriausiojo administratoriaus parengti išsamesnes susiejimo praktinio įgyvendinimo technines gaires ir užtikrinti, kad jos būtų nuolat tikslinamos atsižvelgiant į technikos pažangą ir naujus reikalavimus, susijusius su jungties sauga ir saugumu ir jos veiksmingu ir efektyviu veikimu.

2.1. *Taikymo sritis*

Šiame dokumente įtvirtintas bendras Susitarimo šalių susitarimas dėl jungties tarp ES ATLPS ir Šveicarijos ATLPS registrų kūrimo techninių pagrindų. Nors šiame dokumente yra išdėstytos pagrindinės techninės specifikacijos, t. y. architektūriniai, paslaugų ir saugumo reikalavimai, tam, kad jungtis imtų veikti praktiškai, bus reikalingos tam tikros papildomos išsamios techninės gairės.

Kad jungtis tinkamai veiktų, bus reikalingi tolesni jos praktinio veikimo procesai ir procedūros. Pagal Susitarimo 3 straipsnio 6 dalį šie aspektai aprašomi Jungtinio komiteto sprendimu atskirai priimtose bendrose darbo procedūrose (toliau – BDP).

2.2. *Adresatai*

Šis dokumentas skirtas Šveicarijos registro administratoriui ir Sąjungos vyriausiajam administratoriui.

3. **Bendrosios nuostatos**

3.1. *Ryšio jungties architektūra*

Šiame skirsnyje aprašoma bendra ES ATLPS ir Šveicarijos ATLPS jungties bei įvairių ją sudarančių komponentų praktinio veikimo architektūra.

Kadangi apibrėžiant registrų jungties architektūrą viena iš sričių, kuriai skiriama daugiausia dėmesio, yra saugumas, buvo imtasi visų priemonių, kad architektūra būtų patikima. Nors numatyta nuolatinė registrų jungtis veiks saityno paslaugų pagrindu, pagal laikiną sprendimą bus naudojamas keitimosi failais mechanizmas.

Pagal techninį sprendimą naudojami:

— saugaus keitimosi pranešimais protokolas;

— XML pranešimai;

— XML pagrindu veikiantis skaitmeninis parašas ir užšifravimas;

— „VPN Appliance“ arba lygiavertis saugaus duomenų persiuntimo tinklas.

3.1.1. Keitimasis pranešimais

Ryšys tarp Sąjungos registro ir Šveicarijos registro bus užtikrinamas naudojant keitimosi pranešimais saugiais kanalais mechanizmą. Kiekviename galiniame taške bus remiamasi savomis gautų pranešimų saugyklomis.

Abi Šalys tvarkys gautų pranešimų žurnalą ir saugos pranešimų tvarkymo duomenis.

Apie klaidas arba nenumatytą būklę reikės pranešti siunčiant perspėjimus, o priežiūros grupių specialistai turės palaikyti tiesioginį ryšį.

Klaidos ir nenumatyti įvykiai bus tvarkomi laikantis BDP aprašytų incidentų valdymo proceso darbo procedūrų.

3.1.2. XML pranešimas – bendras apibūdinimas

XML pranešimą sudaro vienas arba keli iš šių elementų:

— viena arba kelios sandorio užklausos ir (arba) vienas arba keli atsakymai dėl sandorio;

— viena operacija ir (arba) atsakymas, susijęs su suderinimu;

— vienas bandomasis pranešimas.

Kiekviename pranešime yra antraštė, kurioje įrašoma:

— ATLPS sistema, iš kurios siunčiamas pranešimas;

— sekos numeris.

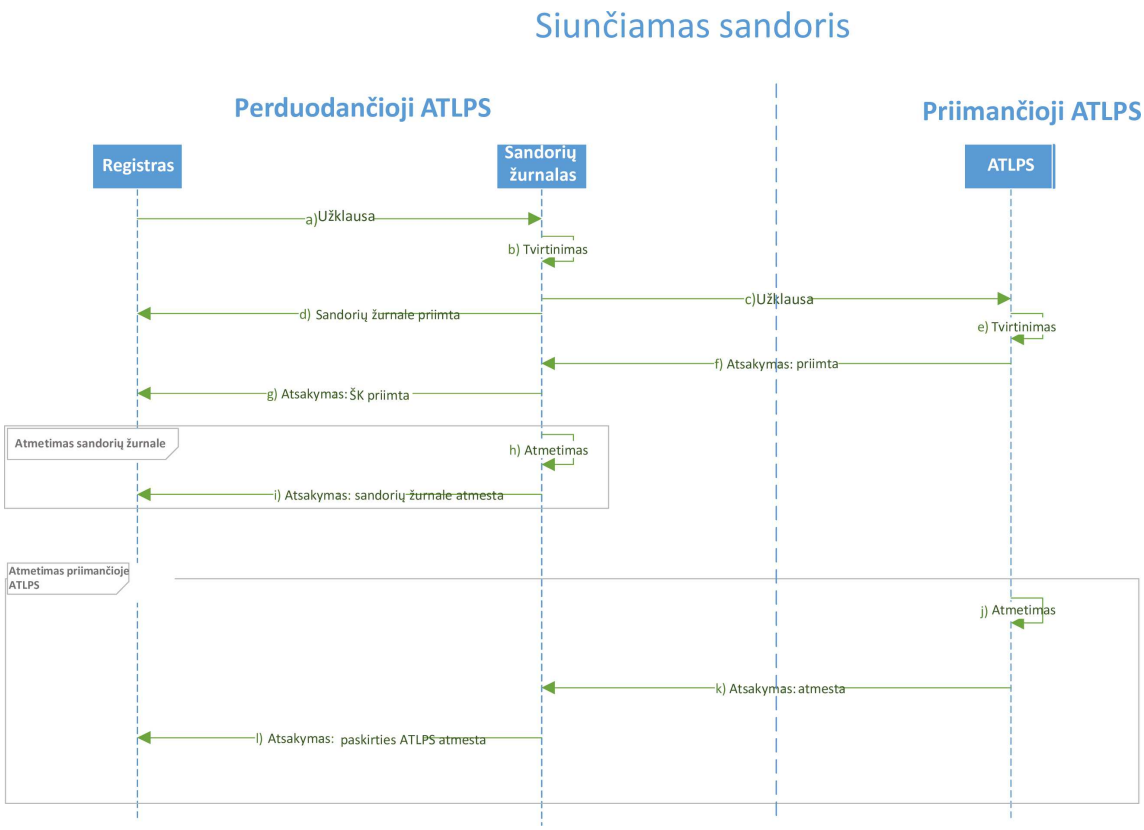
3.1.3. Pranešimų nuskaitymo langai

Taikant laikiną sprendimą naudojami iš anksto apibrėžti pranešimų nuskaitymo langai ir įvardytų įvykių rinkiniai. Sandorių užklausos, gautos per jungtį, bus nuskaitomos tik nustatytais intervalais. Pranešimų nuskaitymo langų procesai apima techninį siunčiamų ir gaunamų sandorių užklausų tvirtinimą. Taip pat pažymėtina, kad suderinimas gali būti vykdomas kasdien ir jį galima įjungti rankiniu būdu.

Bet kurių iš šių įvykių periodiškumo ir (arba) laiko pakeitimai bus tvarkomi laikantis BDP aprašytų užklausų vykdymo proceso darbo procedūrų.

3.1.4. Pranešimų dėl sandorių procesai

Siunčiami sandoriai



Šioje dalyje procesai aprašyti iš perduodančiosios ATLPS perspektyvos. Pirmiau pateiktoje procesų diagramoje pavaizduoti visi sandorių siuntimo procesui būdingi etapai.

Pagrindinis procesas „įprastas sandoris“ (jo etapai nurodyti pirmiau pateiktoje diagramoje):

a) užklausą perduodančiojoje ATLPS sandorio užklausa siunčiama iš registro į sandorių žurnalą, kai pasibaigia visi veiklos užlaikymai (jei taikoma, po 24 val.);

b) sandorių žurnale sandorio užklausa tvirtinama;

c) sandorio užklausa siunčiama į paskirties ATLPS;

d) pranešimas apie priėmimą yra siunčiamas į užklausą išsiuntusios ATLPS registrą;

e) paskirties ATLPS sandorio užklausa tvirtinama;

f) iš paskirties ATLPS pranešimas apie priėmimą siunčiamas į užklausą atsiuntusios ATLPS sandorių žurnalą;

g) iš sandorių žurnalo į registrą siunčiamas atsakymas apie priėmimą.

Alternatyvus procesas „atmetimas sandorių žurnale“ (etapai parodyti pirmiau pateiktoje diagramoje, taip pat pradedant nuo a)):

a) užklausą siunčiančioje ATLPS sandorio užklausa siunčiama iš registro į sandorių žurnalą, kai pasibaigia visi veiklos užlaikymai (jei reikia, po 24 val.);

po to:

b) sandorių žurnale užklausa nepatvirtinama;

c) į užklausą atsiuntusį registrą siunčiamas atsakymas apie atmetimą.

Alternatyvus procesas „atmetimas ATLPS“ (etapai parodyti pirmiau pateiktoje diagramoje, pradedant nuo a)):

a) užklausą siunčiančioje ATLPS sandorio užklausa siunčiama iš registro į sandorių žurnalą, kai pasibaigia visi veiklos užlaikymai (jei reikia, po 24 val.);

b) sandorių žurnale sandorio užklausa tvirtinama;

c) sandorio užklausa siunčiama į paskirties ATLPS;

d) pranešimas apie priėmimą yra siunčiamas į užklausą atsiuntusios ATLPS registrą;

po to:

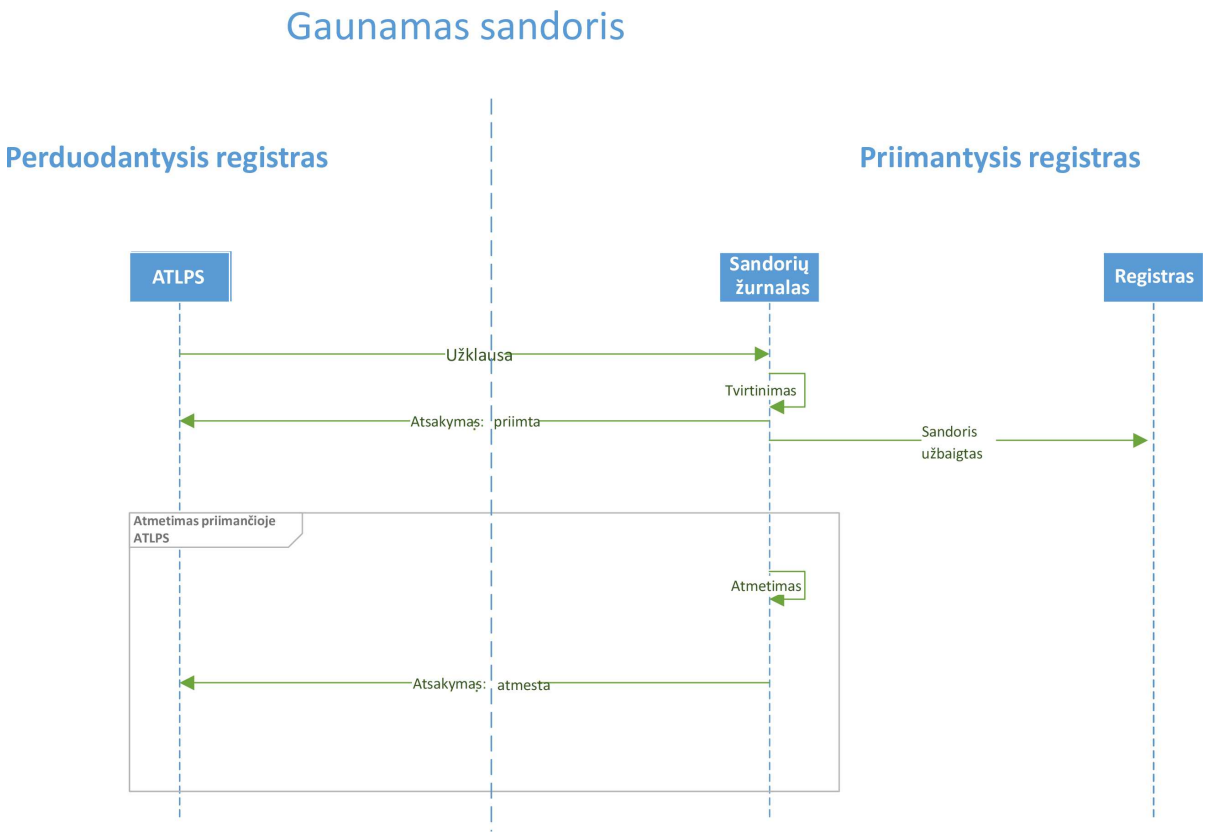
e) užklausą priėmusios ATLPS sandorių žurnale sandoris nepatvirtinamas;

f) iš užklausą priėmusios ATLPS siunčiamas pranešimas apie atmetimą į užklausą atsiuntusios ATLPS sandorių žurnalą;

g) iš sandorių žurnalo į registrą siunčiamas pranešimas apie atmetimą.

Gaunami sandoriai

Šioje dalyje procesai aprašyti iš priimančiosios ATLPS perspektyvos. Konkretus procesas yra pavaizduotas toliau pateiktoje procesų diagramoje:



Diagramoje parodyta:

1. kai priimančiosios ATLPS sandorių žurnale užklausa patvirtinama, užklausą perduodančiai ATLPS yra siunčiamas pranešimas apie priėmimą, o į užklausą priimančios ATLPS registrą siunčiamas pranešimas, kad „sandoris užbaigtas“;

2. jeigu priimančiame sandorių žurnale gauta užklausa atmetama ir nepriimama, sandorio užklausa į priimančiosios ATLPS registrą nesiunčiama.

Protokolas

Pranešimo dėl sandorio ciklą sudaro tik du pranešimai:

— perduodančiosios ATLPS sandorio pasiūlymas priimančiajai ATLPS;

— priimančiosios ATLPS atsakymas dėl sandorio perduodančiajai ATLPS: priimtas arba atmestas (įskaitant atmetimo priežastį):

  — priimta: sandoris užbaigtas;

  — atmesta: sandoris nutrauktas.

Sandorio būklė

— Kai užklausa išsiunčiama, perduodančiojoje ATLPS sandorio būklė bus nustatyta į „pasiūlytas“.

— Kai užklausa gaunama ir kol ji nagrinėjama, priimančiojoje ATLPS sandorio būklė bus nustatyta į „pasiūlytas“.

— Pasiūlymą sutvarkius, priimančiojoje ATLPS sandorio būklė bus pakeista į „užbaigtas“ arba „nutrauktas“. Tada iš priimančiosios ATLPS bus nusiųstas atitinkamas pranešimas apie priėmimą arba atmetimą.

— Kai bus gautas pranešimas apie priėmimą arba atmetimą ir pranešimas bus apdorotas, perduodančioje ATLPS sandorio būklė bus pakeista į „užbaigtas“ arba „nutrauktas“.

— Jeigu nebus gauta jokio atsakymo, perduodančiojoje ATLPS sandorio būklė liks „pasiūlytas“.

— Jeigu pasiūlyto sandorio būklė „pasiūlytas“ nesikeis ilgiau negu 30 minučių, priimančioje ATLPS sandorio būklė bus pakeista į „nutrauktas“.

Su sandoriais susiję incidentai bus tvarkomi laikantis BDP aprašytų incidentų valdymo proceso darbo procedūrų.

3.2. *Duomenų perdavimo saugumas*

Yra keturi duomenų perdavimo apsaugos lygiai:

1) prieigos prie tinklo kontrolė: užkarda ir tinklo vidaus jungčių lygmuo;

2) užšifravimas siuntimo lygmeniu: VPN arba lygiavertis saugaus duomenų persiuntimo tinklas;

3) užšifravimas seanso lygmeniu: saugaus keitimosi pranešimais ir pranešimų perdavimo protokolas;

4) užšifravimas taikomosios programos lygmeniu: XML turinio užšifravimas ir parašas.

3.2.1. Užkarda ir tinklo vidaus jungtys

Jungtis turi būti kuriama aparatine užkarda apsaugotame tinkle. Užkarda konfigūruojama taip, kad prie VPN serverio galėtų jungtis tik registruoti klientai.

3.2.2. Virtualusis privatusis tinklas (toliau – VPN)

Visi Šalių tarpusavio pranešimai apsaugomi naudojant saugias duomenų siuntimo technologijas. Jeigu naudojamas VPN, infrastruktūra turi veikti aparatinės įrangos arba virtualių įrenginių pagrindu. VPN technologijos suteikia galimybę tinkle, pavyzdžiui, internete, sukurti duomenų perdavimo „tunelį“ nuo vieno taško iki kito ir taip apsaugoti visus pranešimus. Prieš sukuriant VPN tunelį numatomo kliento galinio taško įrenginiui išduodamas skaitmeninis sertifikatas, suteikiantis galimybę klientui įrodyti savo tapatybę, kai prašoma prisijungimo. Kiekviena Šalis yra atsakinga už sertifikato įdiegimą į savo VPN galinio taško įrenginį. Naudodamas skaitmeninius sertifikatus kiekvienas VPN serveris kreipiasi į centrinę instituciją, kad jam būtų suteikti autentiškumo patvirtinimo rekvizitai. Per duomenų perdavimo tunelio kūrimo procesą susitariama dėl užšifravimo užtikrinant, kad visi tuo tuneliu perduodami pranešimai būtų apsaugoti.

Kliento VPN galinio taško įrenginiai sukonfigūruojami taip, kad VPN tunelis būtų pastovus ir būtų galima užtikrinti visą laiką veikiantį patikimą, dvikryptį tikralaikį ryšį tarp Šalių.

Bet kuris lygiavertis sprendimas turi atitikti pirmiau išdėstytus principus.

3.2.3. IPSec diegimas

Jeigu naudojamas VPN sprendimas, naudojant IPSec protokolą sukuriama skirtingose vietose esančius įrenginius jungianti VPN infrastruktūra, kurioje tarp tų vietų užtikrinamas autentiškumo patvirtinimas, duomenų vientisumas ir duomenų užšifravimas. IPSec VPN konfigūracija VPN jungtyje užtikrinamas tinkamas autentiškumo patvirtinimas tarp dviejų galinių taškų įrenginių. Šalys nustato nuotolinio kliento tapatybę ir patvirtina jo autentiškumą naudodamosi IPSec jungtimi ir kitos Šalies pripažintos skaitmeninius sertifikatus teikiančios organizacijos išduotu skaitmeniniu sertifikatu.

IPSec taip pat užtikrina visų VPN tuneliu perduodamų pranešimų duomenų vientisumą. Duomenų paketų maiša atliekama ir jie pasirašomi naudojant VPN nustatyto autentiškumo patvirtinimo informaciją. Duomenų konfidencialumas taip pat užtikrinamas naudojantis IPSec užšifravimo funkcija.

3.2.4. Saugaus keitimosi pranešimais ir pranešimų perdavimo protokolas

Siekiant užtikrinti keitimosi duomenimis tarp Šalių saugumą, pagal laikiną sprendimą yra naudojami keli užšifravimo lygmenys. Abi sistemos ir jų aplinka yra sujungtos tarpusavyje tinklo lygmeniu sukuriant VPN tunelius arba lygiaverčius saugius duomenų siuntimo tinklus. Taikomosios programos lygmeniu failai yra perduodami per seansą naudojantis saugiu keitimosi pranešimais ir pranešimų perdavimo protokolu.

3.2.5. XML užšifravimas ir parašas

XML failuose pasirašymas ir užšifravimas vyksta dviem lygmenimis. Kiekviena sandorio užklausa, atsakymas dėl sandorio ir kiekvienas suderinimo pranešimas yra pasirašomi atskirai skaitmeniniu būdu.

Antruoju lygmeniu atskirai užšifruojamas kiekvienas pranešimą sudarantis elementas.

Be to, trečiuoju etapu, siekiant užtikrinti viso pranešimo vientisumą ir tai, kad visas pranešimas nebūtų atmestas, skaitmeniniu būdu pasirašomas pagrindinis pranešimo elementas. Tokiu būdu užtikrinamas aukštas XML įterptųjų duomenų apsaugos lygis. Techninio įgyvendinimo etapu laikomasi Pasaulinio saityno konsorciumo standartų.

Kai pranešimą norima iššifruoti ir patvirtinti, visas procesas atliekamas atvirkštine tvarka.

3.2.6. Kriptografiniai raktai

Užšifravimui ir pasirašymui bus naudojama viešųjų raktų kriptografija.

Konkrečiu IPSec atveju naudojami tik skaitmeninius sertifikatus teikiančios organizacijos, kuria pasitiki abi Šalys, išduoti skaitmeniniai sertifikatai. Skaitmeninius sertifikatus teikianti organizacija patikrina sertifikato turėtojo tapatybę bei išduoda sertifikatus, pagal kuriuos nustatoma organizacijos tapatybė ir tarp Šalių sukuriami saugūs duomenų perdavimo kanalai.

Kriptografiniai raktai yra naudojami ryšio kanalams ir duomenų failams pasirašyti ir užšifruoti. Šalys keičiasi viešais sertifikatais skaitmeniniu būdu, naudodamosi saugiais kanalais. Sertifikatai patvirtinami atskiru duomenų perdavimo kanalu. Ši procedūra yra neatskiriama BDP aprašyto informacijos saugumo valdymo proceso dalis.

3.3. *Jungčiai priskirtų funkcijų sąrašas*

Jungtis yra įvairių funkcijų, kuriomis įgyvendinami pagal Susitarimą vykdomi verslo procesai, perdavimo sistema. Į jungtį taip pat įtraukta suderinimo proceso ir bandymo pranešimų specifikacija, suteikianti galimybę įgyvendinti veikimo stebėseną (angl. *heartbeat monitoring*).

3.3.1. Verslo sandoriai

Verslo požiūriu per jungtį tvarkomos toliau nurodytų keturių (4) tipų sandorių užklausos.

— Išorinis perdavimas:

  — ATLPS jungčiai pradėjus veikti, ES ir ŠK apyvartiniai taršos leidimai galės būti keičiami vieni kitais, taigi Šalys juos galės visapusiškai perduoti viena kitai;

— tam, kad perdavimą būtų galima įvykdyti per jungtį, vienoje ATLPS reikės sukurti siuntimo, o kitoje ATLPS priėmimo paskyrą;

— gali būti perduodami šių keturių (4) tipų apyvartiniai taršos leidimai (bet koks jų skaičius):

— Šveicarijos paprastieji apyvartiniai taršos leidimai (CHU);

— Šveicarijos aviacijos apyvartiniai taršos leidimai (CHUA);

— ES paprastieji apyvartiniai taršos leidimai (EUA);

— ES aviacijos apyvartiniai taršos leidimai (EUAA).

— Tarptautinis paskirstymas

Vienos ATLPS administruojami orlaivių naudotojai, turintys įsipareigojimų kitai ATLPS ir turintys teisę gauti nemokamų apyvartinių taršos leidimų iš tos antrosios ATLPS, iš antrosios ATLPS gaus nemokamų aviacijos apyvartinių taršos leidimų pagal tarptautinį paskirstymo sandorį.

— Tarptautinio paskirstymo panaikinimas

Šis sandoris įvyks, jeigu visus orlaivio naudotojui kitos ATLPS suteiktus nemokamus apyvartinius taršos leidimus reikės panaikinti.

— ATL pertekliaus grąžinimas

Šis atvejis panašus į panaikinimą, tačiau paskirtus apyvartinius taršos leidimus (tik perteklinius paskirtus apyvartinius taršos leidimus) reikės ne visiškai panaikinti, bet grąžinti juos skyrusiai ATLPS.

3.3.2. Suderinimo protokolas

Suderinimas bus atliekamas tik tada, kai bus uždaryti pranešimų nuskaitymo, patvirtinimo ir tvarkymo langai.

Suderinimas yra neatsiejama susiejimo saugumo ir nuoseklumo užtikrinimo dalis. Abi Šalys, prieš sudarydamos bet kokį tvarkaraštį, susitars dėl tikslaus suderinimo laiko. Jeigu abi Šalys sutinka, gali būti atliekamas kasdienis planinis suderinimas. Mažiausiai bent vienas planinis suderinimas bus atliekamas po kiekvieno nuskaitymo.

Bet kuriuo atveju kiekviena Šalis gali bet kuriuo metu inicijuoti suderinimą rankiniu būdu.

Planinio suderinimo periodiškumo ir (arba) laiko pakeitimai bus tvarkomi laikantis BDP aprašytų užklausų vykdymo proceso darbo procedūrų.

3.3.3. Bandomasis pranešimas

Bandomąjį pranešimą numatoma siųsti siekiant patikrinti ryšį tarp galinių taškų įrenginių. Pranešime bus pateikti duomenys, iš kurių bus galima matyti, kad pranešimas yra bandomasis. Iš kito galinio taško įrenginio, gavus pranešimą, bus atsiųstas atsakymas.

3.4. *Saityno paslaugų standartai*

Pagal laikiną sprendimą saityno paslaugos nebus naudojamos. Tačiau derėtų paminėti, kad XML pranešimų forma ir formatas iš esmės nesikeis. Ateityje pradėjus veikti nuolatinei registrų jungčiai, saityno paslaugos turėtų suteikti galimybę keistis XML pranešimais tikruoju laiku.

3.5. *Konkreti saityno paslaugų apibrėžtis*

Šis skirsnis pagal laikiną sprendimą netaikomas. Kaip paminėta ankstesniame skirsnyje, saityno paslaugomis bus naudojamasi tik ateityje, kai pradės veikti nuolatinė registrų jungtis.

3.6. *Duomenų registravimo reikalavimai*

Atsižvelgiant į tai, kad abi Šalys turi turėti tikslią ir nuoseklią informaciją, taip pat siekiant Šalims suteikti įrankius, kuriuos jos galėtų naudoti per suderinimo procesą, kad pašalintų nuoseklumo spragas, abi Šalys pildo keturių (4) tipų duomenų žurnalus:

— sandorių žurnalus;

— suderinimo žurnalus;

— pranešimų archyvą;

— vidaus audito žurnalus.

Visi duomenys šiuose žurnaluose saugomi ne trumpiau kaip tris (3) mėnesius problemų šalinimo tikslais, o tolesnis jų saugojimas priklauso nuo kiekvienai Šaliai taikytinų teisės aktų dėl duomenų saugojimo audito tikslais. Senesni negu trijų (3) mėnesių žurnalų failai gali būti archyvuojami saugioje vietoje, nepriklausomoje IT sistemoje, jei tik per pagrįstą laikotarpį juos galima rasti arba prie jų prieiti.

Sandorių žurnalai

Ir ESSŽ, ir SSTL posistemėse yra įdiegiami sandorių žurnalai.

Tiksliau, sandorių žurnaluose bus saugomi kiekvieno kitai ATLPS nusiųsto sandorio pasiūlymo įrašas. Kiekvieną įrašą sudaro visi sandorio turinio laukeliai ir gautas rezultatas (sandorio užklausą gavusios ATLPS atsakymas). Sandorių žurnaluose taip pat bus saugomas gaunamų sandorių ir sandorį atsiuntusiai ATLPS nusiųsto atsakymo įrašas.

Suderinimo žurnalai

Suderinimo žurnale saugomas kiekvieno Šalių viena kitai siųsto suderinimo pranešimo įrašas, įskaitant suderinimo identifikavimo žymą, laiko žymą ir suderinimo rezultatą: ar suderinimo būklė „sutampa“, ar „nesutampa“. Pagal laikiną sprendimą suderinimo pranešimai yra neatsiejama keitimosi pranešimais dalis.

Abi Šalys registruoja kiekvieną užklausą ir atsakymą į ją suderinimo žurnale. Nors suderinimo žurnale saugoma informacija per suderinimo procesą tiesiogiai nėra keičiamasi, prieigos prie šios informacijos gali prireikti tam, kad būtų pašalintos nuoseklumo spragos.

Pranešimų archyvas

Abi Šalys privalo saugoti duomenų (XML failų), kuriais dalijosi, kuriuos siuntė ir gavo, taip pat duomenų apie tai, ar XML pranešimų formatas buvo tinkamas ar netinkamas, archyvą.

Pagrindinis tikslas, kuriam saugomas archyvas, yra auditas. Archyvas taip pat saugomas tam, kad būtų turimi įrodymai apie tai, kas buvo siųsta kitai Šaliai ir iš jos gauta. Šiuo atžvilgiu kartu su failais į archyvą turi būti įrašomi ir susiję sertifikatai.

Iš šių failų taip pat bus galima gauti papildomos informacijos šalinant sutrikimus.

Vidaus audito žurnalas

Šiuos žurnalus kiekviena Šalis apibrėžia ir naudoja savarankiškai.

3.7. *Darbo reikalavimai*

Pagal laikiną sprendimą duomenimis tarp abiejų sistemų keičiamasi ne visiškai autonomiškai, tai yra, tam, kad jungtis veiktų praktiškai, reikalingi operatoriai ir procedūros.

4. **Nuostatos dėl prieinamumo**

4.1. *Ryšio prieinamumo struktūra*

Pagal laikino sprendimo architektūrą iš esmės naudojama IRT infrastruktūra ir programinė įranga, kuri suteikia galimybę palaikyti ryšį tarp Šveicarijos ATLPS ir ES ATLPS. Todėl kuriant ne tik laikiną sprendimą, bet ir nuolatinę registrų jungtį reikia atsižvelgti į tai, kad esminiu aspektu tampa užtikrinti didelį šio duomenų srauto prieinamumą, vientisumą ir konfidencialumą. Kadangi šiame projekte IRT infrastruktūra, individualizuota programinė įranga ir procesai yra neatsiejami vieni nuo kitų, norint sukurti atsparią sistemą reikia atsižvelgti į visus tris elementus.

IRT infrastruktūros atsparumas

Šio dokumento bendrųjų nuostatų skyriuje išsamiai aprašyti architektūriniai sudedamieji moduliai. Kalbant apie IRT infrastruktūrą, pagal laikiną sprendimą sukuriamas atsparus VPN (arba lygiavertis) tinklas, kuriame sukuriami saugūs ryšio tuneliai, kuriais galima saugiai siųsti pranešimus. Kiti infrastruktūros elementai yra sukonfigūruoti taip, kad būtų užtikrintas didelis jų prieinamumas, ir (arba) juose veiktų atsarginiai mechanizmai.

Individualizuotos programinės įrangos atsparumas

Individualizuotos programinės įrangos moduliuose atsparumas sustiprinamas tam tikrą laikotarpį pakartotinai bandant užmegzti ryšį su kitu galiniu tašku, jeigu dėl kokios nors priežasties ryšio nėra.

Paslaugų atsparumas

Pagal laikiną sprendimą Šalys keičiasi duomenimis nustatytais laiko intervalais visus metus. Kai kuriais etapais, kuriuos reikia atlikti keičiantis duomenimis pagal iš anksto parengtą planą, reikalinga sistemos operatorių ir (arba) registrų administratorių rankinė intervencija. Atsižvelgiant į šį aspektą ir siekiant padidinti keitimosi duomenimis prieinamumą ir sklandumą:

— darbo procedūrose numatyti svarbūs kiekvieno etapo laiko intervalai;

— laikino sprendimo programinės įrangos moduliuose naudojamas asinchroninis ryšys;

— per automatinio suderinimo procesą nustatoma, ar kuriame nors galiniame taške kyla problemų nuskaitant duomenų failus;

— stebėsenos procesai (IRT infrastruktūra ir individualizuoti programinės įrangos moduliai) yra įtraukiami į incidentų valdymo procedūras ir yra pagrindas jas vykdyti (procedūros aprašytos bendrų darbo procedūrų dokumente). Šios procedūros, kuriomis siekiama sumažinti laiką, per kurį po incidentų atkuriamas įprastas darbas, yra itin svarbios dideliam prieinamumui užtikrinti.

4.2. *Darbo pradžia, ryšio atnaujinimas ir bandymų planas*

Visi į laikino sprendimo architektūrą įtraukti elementai yra tikrinami atliekant įvairius individualius ir kolektyvinius bandymus siekiant patvirtinti, kad platforma IRT infrastruktūros ir informacijos sistemos lygmeniu yra parengta. Šie darbiniai bandymai turi būti atlikti kaskart, kai pagal laikiną sprendimą platforma po sustabdymo pradeda veikti darbiniu režimu.

Kad jungtis galėtų pradėti veikti darbiniu režimu, reikia sėkmingai įvykdyti parengtą bandymų planą. Taip patvirtinama, kad kiekviename registre pirmiausia atlikti vidaus bandymai, paskui patvirtintas galinių taškų įrenginių tarpusavio ryšys ir tik tada Šalys darbiniu režimu pradeda siųsti viena kitai sandorių užklausas.

Bandymų plane turėtų būti paminėta bendra bandymų strategija ir išsamūs bandymų infrastruktūros duomenys. Tiksliau, kiekvieno elemento bandymo modulį turėtų sudaryti:

— bandymo kriterijai ir įrankiai;

— priskirtos bandymo vykdymo pareigos;

— numatomi rezultatai (teigiami ir neigiami);

— bandymo tvarkaraštis;

— bandymo rezultatų registravimo reikalavimai;

— sutrikimų šalinimo dokumentavimas;

— nuostatos dėl perdavimo į kitą sprendimų lygmenį.

Darbinio režimo aktyvavimo bandymų procesą galima padalinti į toliau nurodytus keturis (4) pagrindinius modulius arba etapus.

4.2.1. IRT infrastruktūros vidaus bandymai

Šiuos bandymus atlieka ir (arba) tikrina kiekviena Šalis individualiai kiekviename galiniame taške.

Kiekvienas IRT infrastruktūros elementas kiekviename galiniame taške išbandomas individualiai. Taip pat individualiai išbandomas kiekvienas infrastruktūros komponentas. Šie bandymai gali būti atliekami automatiškai arba rankiniu būdu, tačiau per juos turi būti patikrinta, ar kiekvienas infrastruktūros elementas veikia.

4.2.2. Ryšio bandymai

Šiuos bandymus individualiai inicijuoja bet kuri Šalis, o jiems užbaigti reikalingas kito galinio taško bendradarbiavimas.

Kai pavieniai elementai veikia, reikia išbandyti registrų tarpusavio ryšio kanalus. Tuo tikslu kiekviena Šalis patikrina, ar veikia interneto prieiga, ar sukurti VPN tuneliai (arba lygiavertis saugus duomenų siuntimo tinklas) ir ar veikia IP ryšys tarp skirtingose vietose esančių įrenginių. Tada vietos ir nuotolinių infrastruktūros elementų prieinamumas ir IP ryšys turėtų būti patvirtinti kitame galiniame taške.

4.2.3. Visos sistemos (galinių taškų įrenginių) bandymai

Šie bandymai turi būti atliekami kiekviename galiniame taške ir Šalys turi informuoti viena kitą apie bandymo rezultatus.

Kai ryšio kanalai ir kiekvienas abiejų registrų komponentas išbandomas, kiekviename galiniame taške parengiama keletas imituojamų sandorių ir suderinimų, apimančių visas funkcijas, kurios bus įdiegtos į jungtį.

4.2.4. Saugumo bandymai

Šiuos bandymus kiekviena Šalis turi atlikti ir (arba) inicijuoti kiekviename galiniame taške, kaip nurodyta 5.4 skirsnyje „Saugumo bandymų gairės“ ir 5.5 skirsnyje „Nuostatos dėl rizikos vertinimo“.

Tik tada, kai kiekvienas iš keturių etapų ir (arba) modulių yra užbaigiamas gavus prognozuojamus rezultatus, galima daryti išvadą, kad laikina jungtis veikia darbiniu režimu.

Bandymų ištekliai

Kiekviena Šalis naudojasi specialiais bandymų ištekliais (specialia IRT infrastruktūros programine ir aparatine įranga) ir bandymų funkcijas įtraukia į atitinkamas savo sistemas, kad rankiniu būdu ir pastoviai atliekamas platformos patikras atlikti būtų lengviau. Rankinio individualaus arba kolektyvinio bandymo procedūras registrų administratoriai gali atlikti bet kuriuo metu. Darbinio režimo aktyvavimas pagal pobūdį yra rankinis procesas.

Taip pat numatyta, kad platformoje bus reguliariai atliekami automatiniai patikrinimai. Šie patikrinimai skirti platformos prieinamumui padidinti, nes bus galima anksti nustatyti galimas infrastruktūros arba programinės įrangos problemas. Šį platformos stebėsenos planą sudaro du elementai:

— IRT infrastruktūros stebėsena: abiejų Šalių galinių įrenginių infrastruktūros stebėseną atliks IRT infrastruktūros paslaugų teikėjai. Automatiniai bandymai bus atliekami su įvairiais infrastruktūros elementais, taip pat bus išbandomas ryšio kanalų prieinamumas;

— taikomųjų programų stebėsena: laikinos jungties programinės įrangos moduliuose bus įdiegta sistemos ryšio stebėsena taikomųjų programų lygmeniu (bus atliekama rankiniu būdu ir (arba) reguliariais intervalais). Imituojant tam tikrus per jungtį vykdomus sandorius bus išbandomas jungties galinių įrenginių prieinamumas.

4.3. *Priėmimo ir bandymų aplinka*

Sąjungos registro ir Šveicarijos registro architektūrą sudaro šios trys aplinkos:

— darbinė (PROD) – šioje aplinkoje saugomi realūs duomenys ir tvarkomi realūs sandoriai;

— priėmimo (ACC) – šioje aplinkoje saugomi ne realūs arba anonimizuoti, reprezentaciniai duomenys. Būtent šioje aplinkoje abiejų Šalių sistemos operatoriai patvirtina naujas versijas;

— bandymų (TEST) – šioje aplinkoje saugomi ne realūs arba anonimizuoti, reprezentaciniai duomenys. Šia aplinka naudojasi tik registro administratoriai ir ji yra skirta abiejų Šalių integravimo bandymams atlikti.

Išskyrus VPN (arba lygiavertį tinklą), visos trys aplinkos yra viena nuo kitos visiškai nepriklausomos, t. y. aparatinė ir programinė įrangos, duomenų bazės, virtuali aplinka, IP adresai ir prievadai yra įrengti ir veikia nepriklausomai vieni nuo kitų.

Dėl VPN išdėstymo pažymėtina, kad jis veikia dviejose aplinkose, kurių viena yra susijusi su PROD aplinka, o kita atskira aplinka yra susijusi su ACC ir TEST aplinka.

5. **Nuostatos dėl konfidencialumo ir vientisumo**

Pagal saugumo mechanizmus ir procedūras yra numatytas metodas, pagal kurį operacijas, vykdomas per Sąjungos ir Šveicarijos registrų jungtį, atlieka po du asmenis (4 akių principas). Metodas, pagal kurį operacijas atlieka po du asmenis, taikomas visada, kai to reikia. Tačiau jis gali būti taikomas ne visais registrų administratorių vykdomais etapais.

Saugumo reikalavimai yra apsvarstomi ir išdėstomi saugumo valdymo plane, kuriame taip pat aprašomi procesai, susiję su saugumo incidentų, kurie kyla pažeidus saugumą, tvarkymu. Tai, kaip šie procesai vykdomi, aprašyta BDP.

5.1. *Saugumo bandymų infrastruktūra*

Kiekviena Šalis įsipareigoja sukurti saugumo bandymų infrastruktūrą (naudodama bendrą programinės ir aparatinės įrangos rinkinį, kuris yra naudojamas pažeidžiamoms vietoms nustatyti kūrimo ir eksploatavimo etapais):

— kuri yra atskirta nuo darbinės aplinkos;

— kurioje saugumą analizuoja grupė, nesusijusi su sistemos kūrimu ir eksploatavimu.

Kiekviena Šalis įsipareigoja atlikti ir statinę, ir dinaminę analizę.

Kai atliekama dinaminė analizė (pavyzdžiui, prasiskverbimo bandymai), abi Šalys įsipareigoja įprastus vertinimus atlikti tik bandymo ir priėmimo aplinkose (kaip aprašyta 4.3 skirsnyje „Priėmimo ir bandymų aplinka“). Šios politikos išimtis abi Šalys turi patvirtinti.

Prieš kiekvieną jungties programinės įrangos modulį pradedant naudoti darbinėje aplinkoje, atliekamas kiekvieno modulio saugumo bandymas (kaip aprašyta 3.1 skirsnyje „Ryšio jungties architektūra“).

Bandymų infrastruktūra ir tinklo, ir infrastruktūros lygmeniu turi būti atskirta nuo darbinės infrastruktūros. Saugumo bandymai, kurie yra reikalingi atitikčiai saugumo reikalavimams patikrinti, atliekami bandymų infrastruktūroje.

5.2. *Nuostatos dėl jungties veikimo sustabdymo ir veikimo atnaujinimo*

Jei įtariama, kad Šveicarijos registro, SSTL, Sąjungos registro ar ESSŽ saugumui yra pakenkta, bet kuri Šalis nedelsdama apie tai informuoja kitą Šalį ir sustabdo SSTL ir ESSŽ jungties veikimą.

Keitimosi informacija, sprendimo sustabdyti jungties veikimą ir sprendimo jungties veikimą atnaujinti procedūros yra BDP aprašyto užklausų vykdymo proceso dalis.

Veikimo sustabdymas

Registrų jungties veikimas gali būti sustabdytas pagal Susitarimo II priedą dėl:

— administracinių priežasčių (pvz., techninės priežiūros), t. y. planuotai;

— saugumo priežasčių (arba IT infrastruktūros gedimų), t. y. neplanuotai.

Iškilus nenumatytam atvejui, kiekviena Šalis informuoja kitą Šalį ir vienašališkai sustabdo registrų jungties veikimą.

Jeigu priimamas sprendimas sustabdyti registrų jungties veikimą, kiekviena Šalis užtikrina, kad jungties veikimas būtų nutrauktas tinklo lygmeniu (užblokuodama prievadus arba visus gaunamus ir siunčiamus ryšio duomenis).

Sprendimas sustabdyti registrų jungties veikimą, nepriklausomai nuo to, ar tai daroma planuotai, ar neplanuotai, priimamas pagal BDP aprašytą pakeitimų valdymo arba saugumo incidentų valdymo procedūrą.

Ryšio atnaujinimas

Sprendimas dėl registrų jungties atnaujinimo priimamas BDP aprašyta tvarka ir bet kuriuo atveju tik tada, kai sėkmingai atliekamos saugumo bandymų procedūros, aprašytos 5.4 skirsnyje „Saugumo bandymų gairės“ ir 4.2 skirsnyje „Darbo pradžia, ryšio atnaujinimas ir bandymų planas“.

5.3. *Nuostatos dėl saugumo pažeidimų*

Saugumo pažeidimas yra laikomas saugumo incidentu, darančiu poveikį bet kurios neskelbtinos informacijos konfidencialumui ir vientisumui ir (arba) sistemos, kurioje tai tvarkoma, prieinamumui.

Neskelbtina informacija yra nurodyta neskelbtinos informacijos sąraše ir gali būti tvarkoma sistemoje arba bet kurioje susijusioje jos dalyje.

Su saugumo pažeidimu tiesiogiai susijusi informacija bus laikoma neskelbtina, žymima žyma ETS CRITICAL ir tvarkoma pagal tvarkymo instrukcijas, nebent nurodoma kitaip.

Kiekvienas saugumo pažeidimas bus tvarkomas pagal BDP skyriaus „Saugumo incidentų valdymas“ nuostatas.

5.4. *Saugumo bandymų gairės*

5.4.1. Programinė įranga

Saugumo bandymai, įskaitant, jei taikoma, prasiskverbimo bandymus, atliekami bent su visomis naujomis programinės įrangos versijomis, laikantis STS išdėstytų saugumo reikalavimų, siekiant įvertinti jungties saugumą ir susijusią riziką.

Jeigu per paskutinius 12 mėnesių jokia didesnė versija nėra sukuriama, saugumo bandymas atliekamas su tuo metu naudojama sistema, atsižvelgiant į per paskutinius 12 mėnesių įvykusius kibernetinės grėsmės pokyčius.

Registrų jungties saugumo bandymas atliekamas priėmimo aplinkoje ir, jei reikia, darbinėje aplinkoje, o abi Šalys jį koordinuoja ir suderina tarpusavyje.

Saityno taikomųjų programų bandymai atliekami laikantis tarptautinių atvirųjų standartų, pavyzdžiui, standartų, parengtų pagal Saityno atvirųjų taikomųjų programų saugumo projektą (angl. *Open Web Applivation Security Project*, OWASP).

5.4.2. Infrastruktūra

Infrastruktūra, kuri naudojama darbinėje sistemoje, reguliariai (bent kartą per mėnesį) tikrinama siekiant nustatyti pažeidžiamas vietas, o nustatytos pažeidžiamos vietos yra ištaisomos. Bandymai atliekami vadovaujantis 5.4.1 skirsnyje aprašytu metodu ir naudojantis naujausia pažeidžiamumo duomenų baze.

5.5. *Nuostatos dėl rizikos vertinimo*

Jeigu turi būti atliekamas prasiskverbimo bandymas, jis įtraukiamas į saugumo bandymą.

Kiekviena Šalis gali sudaryti sutartį su specializuota įmone, kuri atliks saugumo bandymą, jeigu įmonė:

— turi tokio saugumo bandymų vykdymo įgūdžių ir patirties;

— nėra tiesiogiai atskaitinga programinės įrangos kūrėjui ir (arba) rangovui, nedalyvavo kuriant jungties programinę įrangą, taip pat nėra ją kuriančio subjekto subrangovas;

— pasirašė informacijos neatskleidimo sutartį, pagal kurią įsipareigojo saugoti rezultatus paslaptyje, tvarkyti juos laikydamasi ETS CRITICAL lygmeniu taikomų reikalavimų ir tvarkymo instrukcijų.