Europos Sąjungos
Taryba

Briuselis, 2024 m. kovo 22 d.
(OR. en)

8159/24
ADD 1

Tarpinstitucinė byla:
2024/0067 (NLE)

ENV 363
CLIMA 139
ENER 155
IND 187
COMPET 368
MI 359
ECOFIN 359
TRANS 176
AELE 24
CH 7

PASIŪLYMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2024 m. kovo 20 d.
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	COM(2024) 125 final
Dalykas:	PRIEDAS prie Pasiūlymo dėl Tarybos sprendimo dėl pozicijos, kurios Europos Sąjungos vardu turi būti laikomasi Europos Sąjungos ir Šveicarijos Konfederacijos susitarimu dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo įsteigtame Jungtiniame komitete, dėl Susitarimo II priedo, bendrų darbo procedūrų ir susiejimo techninių standartų dalinio pakeitimo

Delegacijoms pridedamas dokumentas COM(2024) 125 final.

Pridedama: COM(2024) 125 final

EUROPOS
KOMISIJA

Briuselis, 2024 03 20
COM(2024) 125 final

ANNEX

PRIEDAS

prie

Pasiūlymo dėl Tarybos sprendimo

dėl pozicijos, kurios Europos Sąjungos vardu turi būti laikomasi Europos Sąjungos ir Šveicarijos Konfederacijos susitarimu dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo įsteigtame Jungtiniame komitete, dėl Susitarimo II priedo, bendrų darbo procedūrų ir susiejimo techninių standartų dalinio pakeitimo

… m. ... ... d.

EUROPOS SĄJUNGOS IR ŠVEICARIJOS KONFEDERACIJOS SUSITARIMU DĖL JŲ ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ APYVARTINIŲ TARŠOS LEIDIMŲ PREKYBOS SISTEMŲ SUSIEJIMO ĮSTEIGTO JUNGTINIO KOMITETO SPRENDIMAS Nr. 1/2024

dėl Susitarimo II priedo, bendrų darbo procedūrų ir susiejimo techninių standartų dalinio pakeitimo

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 9 straipsnį ir 13 straipsnio 2 dalį,

kadangi:

(1) Jungtinio komiteto sprendime Nr. 2/2019[2] numatytas laikinas ES ATLPS ir Šveicarijos ATLPS praktinio susiejimo sprendimas;

(2) trečiajame posėdyje Jungtinis komitetas sutarė, kad reikia išanalizuoti nuolatinės jungties tarp Sąjungos registro ir Šveicarijos registro ekonominį efektyvumą;

(3) penktajame posėdyje Jungtinis komitetas sutarė dėl Jungtinio komiteto sprendimais Nr. 1/2020[3] ir Nr. 2/2020[4] įsteigtos darbo grupės ataskaitos, kurioje ji išnagrinėjo ir pateikė rekomendacijas, kaip diegti nuolatinę jungtį tarp Sąjungos registro ir Šveicarijos registro;

(4) siekiant paisyti nuolatinei jungčiai tarp Sąjungos registro ir Šveicarijos registro keliamų techninių reikalavimų ir, atsižvelgiant į technologinę plėtrą, supaprastinti Susitarimo II priedo nuostatas, turėtų būti iš dalies pakeistas Susitarimo II priedas;

(5) kad būtų užtikrintas bendrų darbo procedūrų ir susiejimo techninių standartų suderinamumas su Susitarimo II priedu, tie dokumentai taip pat turėtų būti iš dalies pakeisti,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

1. Susitarimo II priedas pakeičiamas šio sprendimo I priedo tekstu.

2. Susitarimo 3 straipsnio 6 dalyje nurodytos bendros darbo procedūros išdėstomos šio sprendimo II priede.

3. Susitarimo 3 straipsnio 7 dalyje nurodyti susiejimo techniniai standartai išdėstomi šio sprendimo III priede.

2 straipsnis

Šis sprendimas įsigalioja jo priėmimo dieną.

Priimta anglų kalba [Briuselyje] [Berne] [2024 m. xx xx d.].

---

1 OL L 322, 2017 12 7, p. 3.
2 OL L 314, 2020 9 29, p. 68.
3 OL L 226, 2021 6 25, p. 2.
4 OL L 226, 2021 6 25, p. 16.

Jungtinio komiteto vardu

Europos Sąjungos sekretorius / sekretorė	*Pirmininkas / Pirmininkė*	*Šveicarijos sekretorius / sekretorė*

I PRIEDAS

„II PRIEDAS

SUSIEJIMO TECHNINIAI STANDARTAI (STS)

Siekiant praktiškai susieti ES ATLPS ir Šveicarijos ATLPS, 2020 m. pradėtas taikyti laikinas sprendimas. Nuo 2023 m. šias dvi ATLPS siejanti registrų jungtis palaipsniui plėtojama siekiant, kad ji (kaip tikimasi) ne vėliau kaip 2024 m. taptų nuolatine registrų jungtimi, sudarančia sąlygas veikti susietoms rinkoms, kuriose galima naudotis jų likvidumo teikiama nauda ir sandorius tarp šių susietų sistemų vykdyti taip, kaip jie vykdomi vienoje rinkoje, sudarytoje iš dviejų sistemų. Taigi, rinkos dalyviai galės veikti taip, tarsi jie būtų vienoje rinkoje, tačiau turės paisyti atskirų Šalių reguliavimo nuostatų. STS turi būti išsamiai nustatyti šie aspektai:

– ryšio jungties architektūra,

– ryšys tarp SSTL ir ESSŽ,

– duomenų perdavimo saugumas,

– funkcijų sąrašas (sandoriai, suderinimas…),

– transporto lygmens apibrėžtis,

– duomenų registravimo reikalavimai,

– eksploataciniai aspektai (pagalbos tarnyba, pagalbos paslaugos),

– ryšio aktyvavimo planas ir bandymo procedūra,

– saugumo bandymo procedūra.

STS turi būti nurodyta, kad administratoriai turi imtis visų pagrįstų žingsnių, kad užtikrintų SSTL, ESSŽ ir jungties veikimą 24 valandas per parą 7 dienas per savaitę, ir kad SSTL, ESSŽ ir jungties veikimo trikdžiai turi būti kuo mažesni.

STS nustatomi papildomi Šveicarijos registro, SSTL, Sąjungos registro ir ESSŽ saugumo reikalavimai ir jie dokumentuojame saugumo valdymo plane. Visų pirma STS nurodoma, kad:

– jei įtariama, kad Šveicarijos registro, SSTL, Sąjungos registro ar ESSŽ saugumui buvo pakenkta, abi Šalys nedelsdamos viena kitą apie tai informuoja ir sustabdo SSTL ir ESSŽ jungties veikimą,

– Šalys įsipareigoja saugumo pažeidimo atveju nedelsdamos tarpusavyje dalytis informacija. Per 24 valandas nuo tada, kai saugumo incidentas identifikuojamas kaip saugumo pažeidimas, Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius pasidalija ataskaita, kurioje pateikiama išsami techninė informacija (data, priežastis, poveikis, taisomosios priemonės) apie incidentą.

Prieš užmezgant ryšį tarp SSTL ir ESSŽ, taip pat jei diegiama nauja SSTL arba ESSŽ versija ar laida, turi būti užbaigta STS išdėstyta saugumo bandymo procedūra.

STS, be darbinės aplinkos, turi būti numatytos dar dvi bandomosios aplinkos: kūrėjų bandomoji aplinka ir priėmimo aplinka.

Per Šveicarijos registro administratorių ir Sąjungos vyriausiąjį administratorių Šalys turi pateikti įrodymus, kad per ankstesnius dvylika mėnesių buvo atliktas nepriklausomas jų sistemų saugumo įvertinimas pagal STS nustatytus saugumo reikalavimus. Pagal STS nustatytus saugumo reikalavimus, programinės įrangos visos svarbios naujos versijos turi būti išbandytos atliekant saugumo bandymą ir, visų pirma, skverbimosi testavimą. Skverbimosi testavimą turi atlikti ne programinės įrangos kūrėjas ar programinės įrangos kūrėjo subrangovas.“

II PRIEDAS

BENDROS DARBO PROCEDŪROS (BDP)

pagal Europos Sąjungos ir Šveicarijos Konfederacijos susitarimo dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo 3 straipsnio 6 dalį

Su nuolatine registrų jungtimi susijusios procedūros

Turinys

1. SĄVOKŲ ŽODYNĖLIS

1-1 lentelė. Santrumpos ir apibrėžtys

Santrumpa / sąvoka	Apibrėžtis
skaitmeninius sertifikatus teikianti organizacija	skaitmeninius sertifikatus išduodantis subjektas

ŠK	Šveicarijos Konfederacija
ATLPS	apyvartinių taršos leidimų prekybos sistema
ES	Europos Sąjunga
IVG	incidentų valdymo grupė
informacijos išteklius	įmonei arba organizacijai vertingas informacijos vienetas
IT	informacinės technologijos
ITIB	informacinių technologijų infrastruktūros biblioteka
ITPV	IT paslaugų valdymas
STS	susiejimo techniniai standartai
registras	pagal ATLPS išduotų apyvartinių taršos leidimų apskaitos sistema, kurioje registruojami elektroninėse sąskaitose laikomų leidimų turėtojai
PkU	pakeitimo užklausa
NIS	neskelbtinos informacijos sąrašas
PslU	paslaugos užklausa
vikis	interneto svetainė, kurioje naudotojai gali keistis informacija ir duomenimis pildydami arba koreguodami turinį tiesiogiai interneto svetainės naršyklėje

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 (ESSŽ) ir Šveicarijos registro Šveicarijos papildomų sandorių žurnalo (SSTL), kad pagal bet kurią iš šių dviejų ATLPS išduoti apyvartiniai taršos leidimai galėtų būti perduoti iš vieno registro į kitą (Susitarimo 3 straipsnio 2 dalis). Siekiant praktiškai susieti ES ATLPS ir Šveicarijos ATLPS, 2020 m. pradėtas taikyti laikinas sprendimas. Nuo 2023 m. šias dvi ATLPS siejanti registrų jungtis palaipsniui plėtojama siekiant, kad ji (kaip tikimasi) ne vėliau kaip 2024 m. taptų nuolatine registrų jungtimi, sudarančia sąlygas veikti susietoms rinkoms, kuriose galima naudotis jų likvidumo teikiama nauda ir sandorius tarp šių susietų sistemų vykdyti taip, kaip jie vykdomi vienoje rinkoje, sudarytoje iš dviejų sistemų. Taigi, rinkos dalyviai galės veikti taip, tarsi jie būtų vienoje rinkoje, tačiau turės paisyti atskirų Šalių reguliavimo nuostatų (Susitarimo II priedas).

Pagal Susitarimo 3 straipsnio 6 dalį Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius, atsižvelgdami į Šalių vidaus teisės prioritetus, nustato su techniniais ar kitais klausimais, būtinais jungties veikimui užtikrinti, susijusias bendras darbo procedūras (BDP). Administratorių parengtos BDP įsigalioja, kai jas sprendimu patvirtina Jungtinis komitetas.

Jungtinis komitetas BDP patvirtino Sprendimu Nr. 1/2020. Šiame dokumente išdėstytas atnaujintas BDP Jungtinis komitetas patvirtins Sprendimu Nr. 1/2024. Laikydamiesi šio sprendimo ir atsižvelgdami į Jungtinio komiteto prašymus, Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius parengė bei atnaujins išsamesnes praktinio susiejimo technines gaires ir užtikrins, kad jos būtų nuolat tikslinamos atsižvelgiant į technikos pažangą ir naujus reikalavimus, susijusius su jungties sauga bei saugumu ir jos veiksmingu bei efektyviu veikimu.

2.1. Taikymo sritis

Šiame dokumente įtvirtintas bendras Susitarimo šalių susitarimas dėl jungties tarp ES ATLPS ir Šveicarijos APTLPS registrų kūrimo procedūrinių pagrindų. Nors šiame dokumente yra išdėstyti bendri procedūriniai jungties veikimo reikalavimai, tam, kad jungtis būtų įgyvendinta praktiškai, bus reikalingos tam tikros papildomos techninės gairės.

Kad jungtis tinkamai veiktų, bus reikalingos techninės jos tolesnio praktinio įgyvendinimo specifikacijos. Pagal Susitarimo 3 straipsnio 7 dalį šie aspektai aprašomi Jungtinio komiteto sprendimu atskirai priimtuose susiejimo techniniuose standartuose (STS).

BDP paskirtis – užtikrinti, kad su jungties tarp ES ATLPS ir Šveicarijos ATLPS registrų veikimu susijusios IT paslaugos būtų teikiamos veiksmingai ir efektyviai, ypač užtikrinti, kad paslaugų užklausos ir eilinės darbo užduotys būtų vykdomos ir aptarnavimo sutrikimai ir problemos būtų šalinami pagal tarptautinius IT paslaugų valdymo standartus.

Bus reikalingos tik šios šiame dokumente aprašytos su nuolatine registrų jungtimi susijusios BDP:

- incidentų valdymo,

- problemų valdymo,
- užklausų vykdymo,
- pakeitimų valdymo,
- versijų valdymo,
- saugumo incidentų valdymo,
- informacijos saugumo valdymo.

2.2. Adresatai

Šios BDP yra skirtos ES ir Šveicarijos registrų priežiūros grupėms.

3. METODIKA IR STANDARTAI

Visoms BDP taikomas principas:

- ES ir ŠK susitaria BDP aprašyti remdamosi ITIB (Informacinių technologijų infrastruktūros biblioteka, 4 versija). Šiame standarte apibrėžta praktika panaudojama ir pritaikoma pagal konkrečius su nuolatine registrų jungtimi susijusius poreikius;
- abi Šalys ryšį palaiko ir veiksmus koordinuoja, kai tai yra reikalinga vykdant BDP, per ŠK ir ES registrų aptarnavimo centrus. Užduotys visada skiriamos vienos Šalies struktūroje;
- jeigu dėl BDP tvarkymo nesutariama, nesutarimą analizuoja ir sprendžia abu aptarnavimo centrai. Jeigu susitarti nepavyksta, bendrą sprendimą perduodama priimti aukštesniu lygmeniu;

Sprendimų lygmenys	**ES**	**ŠK**
1-asis lygmuo	ES aptarnavimo centras	ŠK aptarnavimo centras
2-asis lygmuo	ES operacijų valdytojas	ŠK registro taikomosios programos valdytojas
3-asis lygmuo	Jungtinis komitetas (jis šią atsakomybę gali deleguoti pagal Susiejimo susitarimo 12 straipsnio 5 dalį)	
4-asis lygmuo	Jungtinis komitetas, jeigu 3-iojo lygmens atsakomybė yra deleguojama	

- kiekviena Šalis, atsižvelgdama į šių BDP reikalavimus ir su šiomis BDP susijusias sąsajas, nustato savo registro sistemos veikimo procedūras;
- BDP palaikyti yra naudojama IT paslaugų valdymo priemonė, konkrečiai incidentų valdymo, problemų valdymo ir užklausų vykdymo moduliai, taip pat Šalys tuo tikslu palaiko tarpusavio ryšį;
- taip pat leidžiama keistis informacija e. paštu;
- abi Šalys užtikrina, kad būtų laikomasi tvarkymo instrukcijose nustatytų informacijos saugumo reikalavimų.

4. INCIDENTŲ VALDYMAS

Incidentų valdymo proceso paskirtis – po incidento kuo greičiau ir kuo mažiau trukdant veiklai atkurti įprastą IT paslaugų lygį.

Incidentų valdymo specialistai taip pat turėtų tvarkyti incidentų registrą – jis reikalingas atskaitomybės tikslais, juo taip pat būtų remiamasi per kitus procesus, kad juos būtų galima nuolat tobulinti.

Incidentų valdymą bendrai sudaro ši veikla:

- incidentų nustatymas ir registravimas,
- klasifikavimas ir pradinė pagalba,
- tyrimas ir problemos nustatymas,
- sprendimas ir atkūrimas,
- incidentų sprendimo užbaigimas.

Per visą incidento gyvavimo ciklą incidentų valdymo proceso specialistai turi nuolat prižiūrėti, kas atsakingas už vykdomas užduotis, vykdyti stebėseną, sekti, kaip vykdomos užduotys, ir palaikyti ryšį.

4.1. Incidentų nustatymas ir registravimas

Incidentą gali nustatyti priežiūros grupė, jis gali būti nustatytas automatinėmis stebėsenos priemonėmis arba jį gali nustatyti įprastą stebėseną vykdantys techniniai darbuotojai.

Nustatytas incidentas turi būti registruojamas ir jam suteikiama unikalusis identifikatorius, kad incidentą būtų galima tinkamai sekti ir stebėti. Unikalusis incidento identifikatorius – tai identifikatorius, kurį incidentą užfiksavusios Šalies (ES arba ŠK) aptarnavimo centras priskiria bendroje pagalbos prašymų sistemoje (angl. *ticketing system*) ir kuris turi būti naudojamas visoje su incidentu susijusioje komunikacijoje.

Visais atvejais kontaktinio centro funkcijas atlieka pagalbos prašymą užregistravusios Šalies aptarnavimo centras.

4.2. Klasifikavimas ir pradinė pagalba

Incidentų klasifikavimo paskirtis – padėti suprasti ir nustatyti, kuriai sistemai ir (arba) paslaugai incidentas padarė poveikį ir kokio dydžio tas poveikis yra. Kad klasifikavimas būtų veiksmingas, juo remiantis incidentas turi būti nukreipiamas spręsti į reikiamą padalinį iš karto, kad incidentą būtų galima išspręsti greičiau.

Klasifikavimo etapu incidentas turėtų būti priskiriamas kuriai nors kategorijai ir pagal incidento poveikį bei sprendimo skubumą jam turėtų būti priskiriamas prioritetas, kad incidentas būtų sprendžiamas laikantis tą prioritetą atitinkančių terminų.

Jeigu dėl incidento gali būti padarytas poveikis neskelbtinų duomenų konfidencialumui ar vientisumui ir (arba) sistemos prieinamumui, incidentas taip pat pripažįstamas saugumo incidentu ir valdomas laikantis šio dokumento skyriuje „Saugumo incidentų valdymas“ aprašyta tvarka.

Jeigu įmanoma, pirminį įvertinimą atlieka pagalbos prašymą užregistravęs aptarnavimo centras. Tai darydamas aptarnavimo centras analizuoja, ar incidentas kilo dėl jau žinomos klaidos. Jeigu taip, incidento sprendimo būdas arba aplinkinis sprendimas jau yra žinomi ir užfiksuoti dokumentuose.

Jeigu aptarnavimo centrui incidentą pavyksta sėkmingai išspręsti, jis atlieka incidento sprendimo užbaigimo procedūrą, nes pagrindinis incidentų valdymo tikslas (būtent – greitai atkurti paslaugas galutiniam naudotojui) buvo pasiektas. Jeigu incidento išspręsti nepavyksta, aptarnavimo centras dėl incidento sprendimo kreipiasi į atitinkamą incidentų šalinimo grupę, kad ši jį toliau ištirtų ir nustatytų problemą.

4.3. Tyrimas ir problemos nustatymas

Incidento tyrimo ir problemos nustatymo procedūros vykdomos, kai aptarnavimo centrui išspręsti incidento atliekant pirminį įvertinimą nepavyksta ir dėl to incidentą perduodama spręsti kitu sprendimų lygmeniu. Incidento perdavimas spręsti kitu sprendimų lygmeniu yra atskira tyrimo ir problemos nustatymo proceso dalis.

Įprastai šiuo tyrimo ir problemos nustatymo etapu yra bandoma incidentą atkurti kontroliuojamomis sąlygomis. Incidentą tiriant ir nustatant problemą svarbu tinkamai suprasti įvykių, dėl kurių įvyko incidentas, seką.

Jeigu incidentas perduodamas spręsti kitu sprendimų lygmeniu, yra pripažįstama, kad incidento pradiniu pagalbos lygmeniu išspręsti nepavyko ir kad incidento sprendimą reikia perduoti aukštesnio lygmens pagalbos grupei arba kitai Šaliai. Incidentą spręsti kitu sprendimų lygmeniu gali būti perduodama dviem kryptimis: horizontaliai (pagal funkcijas) arba vertikaliai (pagal hierarchiją).

Už incidento sprendimo perdavimą atitinkamam padaliniui ir už bendros incidento sprendimo būklės ir jo perdavimo stebėjimą yra atsakingas aptarnavimo centras, kuris užregistravo incidentą ir inicijavo jo sprendimą.

Šalis, kuriai incidentas perduotas spręsti, yra atsakinga už reikiamų veiksmų įgyvendinimą laiku ir grįžtamosios informacijos pateikimą savo Šalies aptarnavimo centrui.

4.4. Sprendimas ir atkūrimas

Incidentą visapusiškai išsiaiškinus, jis išsprendžiamas ir padėtis atkuriama. Išspręsti incidentą reiškia rasti būdą, kaip ištaisyti nustatytą problemą. Pritaikyti sprendimą – tai atkurti padėtį.

Kai atitinkamas padalinys paslaugų sutrikimą pašalina, informacija apie incidentą vėl perduodama atitinkamam incidentą užregistravusiam aptarnavimo centrui ir šis susisiekia su apie incidentą pranešusiu asmeniu ir įsitikina, kad klaida ištaisyta ir kad galima atlikti incidento sprendimo užbaigimo procedūras. Per incidento sprendimo procesą padarytos išvados yra užregistruojamos, kad jomis būtų galima pasinaudoti ateityje.

Atkūrimo darbus gali atlikti IT priežiūros specialistai arba galutiniam naudotojui gali būti pateiktos instrukcijos, kaip tai padaryti.

4.5. Incidento sprendimo užbaigimo procedūra

Incidento sprendimo užbaigimo procedūra – tai paskutinis incidentų valdymo proceso etapas, vykdomas iškart po to, kai incidentas išsprendžiamas.

Svarbiausi atliktini veiksmai, įtraukti į incidento sprendimo užbaigimo procedūros veiksmų kontrolinį sąrašą:

- pradinės kategorijos, prie kurios buvo priskirtas incidentas, patikrinimas;
- tinkamas visos informacijos apie incidentą surinkimas;
- tinkamas incidento dokumentavimas ir žinių bazės atnaujinimas;

- tinkamas komunikavimas su kiekvienu suinteresuotuoju subjektu, kuriam incidentas yra tiesiogiai arba netiesiogiai aktualus.

Aptarnavimo centrui atlikus incidento sprendimo užbaigimo procedūrą ir informaciją apie tai perdavus kitai Šaliai, incidento sprendimas oficialiai užbaigiamas.

Atlikus incidento sprendimo užbaigimo procedūrą jis nebeatnaujinamas. Jeigu incidentas netrukus pasikartoja, ankstesnis incidentas neatnaujinamas, o užregistruojamas naujas incidentas.

Jeigu incidentą stebi ir ES, ir ŠK aptarnavimo centrai, už galutinę incidento sprendimo užbaigimo procedūrą yra atsakingas pagalbos prašymą užregistravęs aptarnavimo centras.

5. PROBLEMŲ VALDYMAS

Šią procedūrą reikėtų atlikti kaskart, kai nustatoma problema, taigi, kai atsiranda pagrindas vykdyti problemų valdymo procesą. Pagrindinis problemų valdymo proceso tikslas – gerinti kokybę ir mažinti kylančių incidentų skaičių. Problemos priežastis gali būti vienas arba keli incidentai. Kai gaunamas pranešimas apie incidentą, incidentų valdymo specialistai siekia kuo greičiau, jeigu galima – pasinaudodami aplinkiniais sprendimo būdais, atkurti paslaugas. Iškilus problemai, stengiamasi išsiaiškinti jos pagrindinę priežastį ir nustatyti, ką reikia pakeisti, kad problema ir su ja susiję incidentai ateityje nesikartotų.

5.1. Problemos nustatymas ir registravimas

Sprendžiant su problema susijusius klausimus kontaktinio centro funkcijas atlieka pagalbos prašymą užregistravęs ES arba ŠK aptarnavimo centras.

Problemos unikalus identifikatorius – tai per IT paslaugų valdymo procesą suteiktas identifikatorius. Jį reikia nurodyti visuose su šia problema susijusiuose pranešimuose.

Problema gali atsirasti dėl incidento arba būti iškelta savo iniciatyva siekiant ištaisyti kuriuo nors momentu pastebėtus sistemos sutrikimus.

5.2. Prioriteto priskyrimas problemai

Kad problemas būtų lengviau sekti, jas galima suskirstyti į kategorijas pagal problemos rimtumą ir pirmumą tokiu pačiu būdu kaip incidentus, atsižvelgiant į su problema susijusių incidentų poveikį ir dažnumą.

5.3. Problemos tyrimas ir nustatymas

Problemą gali iškelti bet kuri Šalis, o už jos užregistravimą, perdavimą spręsti atitinkamam padaliniui ir bendros būklės stebėjimą yra atsakingas problemos sprendimą inicijavusios Šalies aptarnavimo centras.

Problemos sprendimo grupė, kuriai perduota spręsti problemą, yra atsakinga už problemos išsprendimą laiku ir už ryšio su aptarnavimo centru palaikymą.

Gavusios prašymą, abi Šalys yra atsakingos už pavestų veiksmų įgyvendinimą ir grįžtamosios informacijos pateikimą savo Šalies aptarnavimo centrui.

5.4. Sprendimas

Problemos sprendimo grupė, kuriai pavesta spręsti problemą, yra atsakinga už problemos išsprendimą ir atitinkamos informacijos pateikimą savo Šalies aptarnavimo centrui.

Sprendžiant problemą padarytos išvados užregistruojamos, kad jomis būtų galima pasinaudoti ateityje.

5.5. Problemos sprendimo užbaigimas

Kai atliekami reikiami pakeitimai ir problema išsprendžiama, problemos sprendimas oficialiai užbaigiamas. Problemos sprendimo užbaigimo procedūrą atlieka aptarnavimo centras, kuris problemą užregistravo ir apie ją informavo kitos Šalies aptarnavimo centrą.

6. UŽKLAUSŲ VYKDYMAS

Užklausų vykdymo procesas – tai viso užklausos dėl naujos arba esamos paslaugos ciklo valdymas nuo to momento, kai užklausa užregistruojama ir patvirtinama, iki jos vykdymo užbaigimo. Paslaugų užklausos paprastai būna smulkios, iš anksto apibrėžtos, pasikartojančios, dažnos, iš anksto patvirtintos ir procedūrinės.

Toliau aprašyti pagrindiniai atliktini etapai.

6.1. Užklausos inicijavimas

Informacija, susijusi su paslaugos užklausa, pateikiama ES arba ŠK aptarnavimo centrui e. paštu, telefonu, naudojantis IT paslaugų valdymo priemone arba kitu sutartu ryšio kanalu.

6.2. Užklausos registravimas ir analizė

Visais paslaugų užklausų atvejais kontaktinio centro funkcijas turėtų atlikti ES arba ŠK aptarnavimo centras, priklausomai nuo to, kuri Šalis pateikė paslaugos užklausą. Šis aptarnavimo centras bus atsakingas už paslaugos užklausos registravimą ir pakankamai nuodugnią analizę.

6.3. Užklausos patvirtinimas

Paslaugos užklausą pateikusios Šalies aptarnavimo centro specialistas patikrina, ar iš kitos Šalies reikia gauti kokius nors patvirtinimus ir, jei reikia, imasi veiksmų, kad juos gautų. Jeigu paslaugos užklausa nepatvirtinama, aptarnavimo centras atnaujina informaciją ir užbaigia užklausą.

6.4. Užklausos vykdymas

Šis etapas skirtas paslaugų užklausoms efektyviai ir veiksmingai tvarkyti. Atvejai skirstomi į šias kategorijas:

- paslaugos užklausos vykdymas aktualus tik vienai Šaliai. Šiuo atveju ši Šalis parengia darbo nurodymus ir koordinuoja, kaip jie vykdomi;
- paslaugos užklausos vykdymas aktualus ir ES, ir ŠK. Šiuo atveju darbo nurodymus savo atsakomybės srityse parengia aptarnavimo centrai. Abu aptarnavimo centrai koordinuoja, kaip vykdoma paslaugų užklausa. Visa atsakomybė tenka aptarnavimo centrui, kuris priėmė paslaugos užklausą ir inicijavo jos vykdymą.

Kai paslaugos užklausa įvykdoma, jos būklė pakeičiama į įvykdytą.

6.5. Užklausos perdavimas kitam sprendimų lygmeniui

Jeigu reikia, aptarnavimo centras neįvykdytą paslaugos užklausą gali perduoti atitinkamam kito lygmens padaliniui (trečiajai šaliai).

Paslaugos užklausos vykdymas perduodamas atitinkamoms trečiosioms šalims: jeigu paslaugos užklausos vykdymą reikės perduoti ŠK trečiajai šaliai, ES aptarnavimo centras turės kreiptis į ŠK aptarnavimo centrą ir atvirkščiai.

Trečioji šalis, kuriai paslaugos užklausa perduodama vykdyti, yra atsakinga už tai, kad paslaugos užklausa būtų įvykdyta laiku ir kad su aptarnavimo centru, kuris perdavė paslaugos užklausą, būtų palaikomas ryšys.

Aptarnavimo centras, kuris užregistravo paslaugos užklausą, yra atsakingas už paslaugos užklausos bendros būklės stebėjimą ir užklausos perdavimą.

6.6. Užklausos vykdymo peržiūra

Atsakingas aptarnavimo centras, prieš atlikdamas paslaugos užklausos vykdymo užbaigimo procedūras, pateikia paslaugos užklausos įrašą galutinei kokybės kontrolei atlikti. Taip siekiama užtikrinti, kad paslaugos užklausa būtų faktiškai sutvarkyta ir kad visa informacija, reikalinga užklausos ciklui aprašyti, būtų pateikta ir būtų pakankamai išsami. Be to, per užklausos tvarkymo ciklą padarytos išvados yra užregistruojamos, kad jomis būtų galima pasinaudoti ateityje.

6.7. Užklausos vykdymo užbaigimas

Jeigu Šalys, kurioms paslaugos užklausa buvo perduota, sutinka, kad užklausa yra įvykdyta, ir prašymo pateikėjas laiko, kad klausimas išspręstas, užklausos būklė pakeičiama į „užbaigta“.

Paslaugos užklausos vykdymas oficialiai užbaigiamas, kai paslaugos užklausą užregistravęs aptarnavimo centras atlieka užklausos vykdymo užbaigimo procedūras ir informuoja kitos Šalies aptarnavimo centrą.

7. PAKEITIMŲ VALDYMAS

Tikslas – užtikrinti, kad visi IT infrastruktūros valdymo pakeitimai būtų tvarkomi efektyviai ir greitai pagal standartizuotus metodus ir procedūras ir taip būtų užtikrinta, kad su jais susijusių incidentų kiltų kuo mažiau ir visų atitinkamų incidentų poveikis paslaugoms būtų kuo mažesnis. IT infrastruktūra gali būti keičiama reaguojant į problemas arba į išorės reikalavimus, pvz., teisės aktų pakeitimus, pakeitimai taip pat gali būti įgyvendinami savo iniciatyva, siekiant didesnio veiksmingumo ir efektyvumo arba tam, kad būtų galima įgyvendinti veiklos iniciatyvas ar kad į jas būtų atsižvelgta.

Pakeitimų valdymo procesą sudaro įvairūs etapai, kuriais visi pakeitimo užklausos aspektai yra užregistruojami, kad ateityje juos būtų galima atsekti. Per šiuos procesus užtikrinama, kad perduodamas diegti pakeitimas būtų patvirtintas ir ištestuotas. Sėkmingas diegimas užtikrinamas versijų valdymo procesu.

7.1. Pakeitimo užklausa

Pakeitimo užklausa teikiama pakeitimų valdymo grupei tikrinti ir tvirtinti. Visų pakeitimų užklausų atvejais kontaktinio centro funkcijas turėtų atlikti ES arba ŠK aptarnavimo centras, priklausomai nuo to, kuri Šalis pateikė užklausą. Šis aptarnavimo centras bus atsakingas už užklausos registravimą ir reikiamo nuodugnumo analizę.

Galimos pakeitimų užklausų priežastys:

- incidentas, dėl kurio atsirado pakeitimo poreikis,
- esama problema, dėl kurios reikalingas pakeitimas,
- galutinio naudotojo užklausa dėl naujo pakeitimo,
- pakeitimo poreikis atsiranda vykdant nuolatinę techninę priežiūrą,
- teisės aktų pakeitimai.

7.2. Pakeitimo vertinimas ir planavimas

Šiuo etapu atliekama pakeitimo vertinimo ir planavimo veikla. Jis apima prioritetų priskyrimo ir planavimo veiklą, kad rizika ir poveikis būtų kuo mažesni.

Jeigu pakeitimo užklausos vykdymas yra aktualus ir ES, ir ŠK, pakeitimo užklausą užregistravusi Šalis pakeitimo įvertinimą ir planą sutikrina su kita Šalimi.

7.3. Pakeitimo patvirtinimas

Visos užregistruotos pakeitimų užklausos turi būti patvirtintos atitinkamu sprendimų lygmeniu.

7.4. Pakeitimo įgyvendinimas

Pakeitimas įgyvendinamas versijų valdymo procesu. Abiejų Šalių versijų valdymo grupės vykdo savo procesus, apimančius planavimą ir testavimą. Užbaigus įgyvendinimą, atliekama pakeitimo peržiūra. Kad viskas būtų daroma pagal planą, esamas pakeitimų valdymo procesas yra nuolat peržiūrimas ir prireikus atnaujinamas.

8. VERSIJŲ VALDYMAS

Versija – tai vienas arba keli į vieną versijos planą įtraukti IT paslaugos pakeitimai, dėl kurių turės būti gautas leidimas, kurie turės būti parengti, sudėti į visumą, ištestuoti ir visi kartu įdiegti. Versijos

paskirtis gali būti ištaisyti klaidą, atlikti aparatinės įrangos arba kitų komponentų pakeitimus, atlikti programinės įrangos pakeitimus, atnaujinti taikomosios programos versijas, atlikti dokumentų ir (arba) procesų pakeitimus. Kiekvienos versijos turinys yra valdomas, testuojamas ir diegiamas kaip vienas procesas.

Versijos valdymo paskirtis – suplanuoti, sudėti į visumą, ištestuoti, patvirtinti ir užtikrinti apibrėžtoms paslaugoms teikti reikalingus pajėgumus ir taip įvykdyti suinteresuotųjų subjektų reikalavimus bei pasiekti užsibrėžtus tikslus. Visų paslaugos pakeitimų priėmimo kriterijai bus apibrėžti ir dokumentuoti projekto derinimo etapu ir pateikti versijų valdymo grupėms.

Versiją paprastai sudaro keletas problemos ištaisymų ir paslaugos patobulinimų. Į ją įtraukiama nauja arba pakeista programinė įranga ir nauja arba pakeista aparatinė įranga, kurios yra reikalingos patvirtintiems pakeitimais įgyvendinti.

8.1. Versijos planavimas

Pirmuoju šio proceso etapu pakeitimai, dėl kurių gautas leidimas, suskirstomi į versijų paketus, apibrėžiama versijų apimtis ir turinys. Remdamasis šia informacija, už versijų planavimo paprocesį atsakingas padalinys parengia versijos kūrimo, testavimo ir diegimo tvarkaraštį.

Planavimo padalinys turėtų apibrėžti:

- versijos apimtį ir turinį,
- versijos rizikos įvertinimą ir rizikos pobūdį,
- klientus (naudotojus), kuriems versija aktuali,
- už versiją atsakingą grupę,
- versijos parengimo ir diegimo strategiją,
- versijai sudaryti ir diegti reikalingus išteklius.

Abi Šalys viena kitą informuoja apie versijų planavimo ir techninės priežiūros laikotarpius. Jeigu versija yra aktuali ir ES, ir ŠK, Šalys koordinuoja planus ir nustato bendrą techninės priežiūros laikotarpį.

8.2. Versijos paketo kūrimas ir testavimas

Versijai kurti ir testuoti skirtu versijų valdymo proceso etapu, prieš įdiegiant pakeitimą, pasirenkamas versijos arba versijos paketo kūrimo metodas ir kontroliuojamos aplinkos palaikymo metodas ir visi pakeitimai testuojami visose aplinkose, kuriose jie bus diegiami.

Jeigu versija yra aktuali ir ES, ir ŠK, Šalys koordinuoja parengimo planus ir testavimą. Koordinuojami šie aspektai:

- versijos modulių ir paslaugos komponentų parengimo būdai ir terminai,
- tipiniai vykdymo terminai, padėtis, jei bus vėluojama,
- vykdymo pažangos sekimo ir patvirtinimo gavimo būdai,
- stebėsenos parametrai ir parametrai, pagal kuriuos bus nustatoma, ar versija įdiegta sėkmingai,
- bendri svarbių funkcijų ir pakeitimų testavimo etapai.

Šio paprocesio pabaigoje visi reikalingi versijos komponentai turi būti parengti diegti praktiškai realioje aplinkoje.

8.3. Pasirengimas diegti

Per pasirengimo paprocesį užtikrinama, kad būtų tinkamai parengti komunikacijos planai ir pranešimai, kurie bus siunčiami visiems suinteresuotiesiems subjektams ir galutiniams naudotojams, kuriems tai aktualu, ir kad versija būtų įtraukta į pakeitimų valdymo procesą siekiant užtikrinti, kad visi pakeitimai būtų atliekami kontroliuojamu būdu ir dėl jų būtų gauti reikiamo lygmens patvirtinimai.

Jeigu versija yra aktuali ir ES, ir ŠK, Šalys koordinuoja šią veiklą:

- pakeitimo užklausos įrašo, kuriuo nustatomas diegimo tvarkaraštis ir pasirengiama diegti darbinėje aplinkoje, sukūrimą,
- įgyvendinimo plano sukūrimą,
- ankstesnės būklės atkūrimą, kad tuo atveju, jei diegimas nepavyktų, būtų galima atkurti ankstesnę būseną,
- pranešimų visoms reikiamoms Šalims siuntimą,
- leidimo diegti versiją gavimą iš atitinkamo sprendimų lygmens specialistų.

8.4. Ankstesnės versijos atkūrimas

Jeigu versijos įdiegti nepavyksta arba jeigu atliekant testavimą paaiškėja, kad diegimas buvo nesėkmingas arba kad jis neatitinka suderintų priėmimo ir (arba) kokybės kriterijų, abiejų Šalių versijų valdymo grupės turės atkurti ankstesnę būklę. Reikės informuoti visus reikiamus suinteresuotuosius subjektus, įskaitant galutinius naudotojus, kuriems tai aktualu, ir (arba) tikslinius galutinius naudotojus. Kol negautas patvirtinimas, procesą galima atnaujinti bet kuriame ankstesniame etape.

8.5. Versijos peržiūra ir diegimo užbaigimo procedūra

Atliekant diegimo peržiūrą, reikėtų atlikti šiuos veiksmus:

- surinkti grįžtamąją informaciją apie tai, ar atlikus diegimo darbus patenkinti vartotojų, naudotojų lūkesčiai ir lūkesčiai dėl paslaugos teikimo (surinkti grįžtamąją informaciją ir ją išnagrinėti, kad paslaugą būtų galima nuolat tobulinti);
- peržiūrėti visus neįvykdytus kokybės kriterijus;
- patikrinti, ar užbaigti visi veiksmai, reikalingi pataisymai ir pakeitimai;
- įsitikinti, kad diegimo pabaigoje neliko jokių pajėgumų, išteklių, gebėjimų arba veikimo problemų;
- patikrinti, ar visos problemos, žinomos klaidos ir aplinkiniai sprendimai yra dokumentuoti ir ar klientas, galutiniai naudotojai, operacijų palaikymo specialistai ir kitos Šalys, kurioms tai aktualu, jiems pritarė;
- stebėti incidentus ir problemas, kurių kilo atliekant diegimo darbus (iš anksto suteikti pagalbą operacijų specialistams, jeigu dėl versijos padidėtų darbo apimtys);
- atnaujinti pagalbinius dokumentus (t. y. techninės informacijos dokumentus);
- oficialiai perduoti įdiegtą versiją aptarnavimo operacijų specialistams;
- dokumentuoti įgytą patirtį;
- iš įgyvendinimo grupių gauti versijos santraukos dokumentą;
- patikrinti pakeitimo užklausos įrašą ir oficialiai atlikti versijos diegimo užbaigimo procedūrą.

9. SAUGUMO INCIDENTŲ VALDYMAS

Saugumo incidentų valdymas – tai saugumo incidentų tvarkymo procesas, suteikiantis galimybę pranešti apie incidentą suinteresuotiesiems subjektams, kuriems tai gali būti aktualu, incidento vertinimas ir prioriteto jam priskyrimas;, reagavimas į incidentą siekiant ištaisyti visus faktinius, įtariamus arba galimus konfidencialumo, neskelbtinos informacijos išteklių prieinamumo arba vientisumo pažeidimus.

9.1. Informacijos saugumo incidentų skirstymas į kategorijas

Visi incidentai, darantys poveikį Sąjungos registro ir Šveicarijos registro jungčiai, yra analizuojami siekiant nustatyti galimus visos neskelbtinos informacijos, įtrauktos į neskelbtinos informacijos sąrašą (NIS), konfidencialumo, vientisumo arba prieinamumo pažeidimus.

Jeigu tokį poveikį darantis incidentas įvyksta, jis laikomas informacijos saugumo incidentu, nedelsiant užregistruojamas naudojantis IT paslaugų valdymo priemone ir tvarkomas kaip toks incidentas.

9.2. Informacijos saugumo incidentų tvarkymas

Atsakomybė už saugumo incidentus yra priskirta 3-iojo sprendimų lygmens specialistams. Incidentus sprendžia speciali incidentų valdymo grupė.

Incidentų valdymo grupė atsakinga už tai, kad būtų:

- atlikta pirminė analizė, nustatyta incidento kategorija ir rimtumas;
- koordinuojami visų suinteresuotųjų subjektų veiksmai, įskaitant visą incidento analizės dokumentavimą, sprendimus, priimtus siekiant pašalinti incidentą ir visas galimas nustatytas silpnąsias vietas;
- priklausomai nuo saugumo incidento rimtumo, laiku perduota informacija apie incidentą atitinkamo sprendimų lygmens specialistams siekiant juos informuoti ir (arba) kad tuo lygmeniu būtų priimtas sprendimas.

Per informacijos saugumo valdymo procesą visa informacija apie incidentus klasifikuojama aukščiausiu informacijos slaptumo lygmeniu, tačiau bet kuriuo atveju ne žemesniu negu „SENSITIVE: *ETS*“ lygmeniu.

Jeigu tyrimas dar vykdomas ir (arba) silpnoji vieta dar nėra pašalinta ir ja gali būti pasinaudota, informacija, kol spraga ištaisoma, priskiriama kategorijai „SPECIAL HANDLING: *ETS Critical*“.

9.3. Saugumo incidentų nustatymas

Atsižvelgdamas į saugumo įvykio pobūdį, informacijos saugumo specialistas nustato, kokias organizacijas įtraukti į Incidentų valdymo grupę.

9.4. Saugumo incidentų analizė

Incidentų valdymo grupė susisiekia su visomis įtrauktomis organizacijomis ir atitinkamais savo grupių nariais, kad incidentas būtų peržiūrėtas. Atliekant analizę nustatomas ištekliaus konfidencialumo, vientisumo arba prieinamumo praradimo mastas ir įvertinami padariniai visoms paveiktoms organizacijoms. Paskui apibrėžiami pradiniai ir paskesni incidento sprendimo ir jo poveikio valdymo veiksmai, įskaitant šiems veiksmams atlikti reikalingus išteklius.

9.5. Saugumo incidento rimtumo įvertinimas, perdavimas spręsti kitu sprendimų lygmeniu ir atsiskaitymas

Incidentų valdymo grupė įvertina kiekvieno naujo saugumo incidento, kuris prieš tai apibūdinamas kaip saugumo incidentas, rimtumą ir, atsižvelgdama į jį, nedelsdama imasi reikiamų veiksmų.

9.6. Reagavimo į saugumo incidentą ataskaita

Incidentų valdymo grupė įtraukia incidento sustabdymo ir pašalinimo rezultatus į reagavimo į informacijos saugumo incidentą ataskaitą. Ataskaita pateikiama 3-iojo sprendimų lygmens specialistams saugiu e. paštu arba kitomis abipusiai priimtinomis saugaus ryšio priemonėmis.

Atsakinga Šalis peržiūri incidento sustabdymo ir pašalinimo rezultatus ir:

- vėl prijungia registrą, jeigu prieš tai jis buvo atjungtas;
- pateikia informaciją apie incidentą registro grupėms;
- atlieka incidento sprendimo užbaigimo procedūrą.

Kad būtų užtikrintas nuoseklus informacijos registravimas ir teikimas ir būtų galima skubiai imtis reikiamų veiksmų incidentui sustabdyti, incidentų valdymo grupė turėtų į reagavimo į informacijos saugumo incidentą ataskaitą saugiai įtraukti atitinkamus duomenis. Incidentų valdymo grupė tinkamu laiku pateikia parengtą galutinę reagavimo į informacijos saugumo incidentą ataskaitą.

9.7. Stebėsena, gebėjimų stiprinimas ir nuolatinis tobulinimas

Incidentų valdymo grupė visų saugumo incidentų ataskaitas pateikia 3-iojo sprendimų lygmens specialistams. Naudojant ataskaitas šiuo sprendimų lygmeniu nustatoma:

- silpnosios saugumo kontrolės vietos ir (arba) tai, kurias operacijas reikia stiprinti;
- galimas poreikis tobulinti šią procedūrą, kad į incidentus būtų reaguojama efektyviau;
- mokymo ir gebėjimų stiprinimo galimybės siekiant toliau stiprinti registro sistemų informacijos saugumo patikimumą, mažinti incidentų riziką ateityje ir kuo labiau sumažinti jų poveikį.

10. INFORMACIJOS SAUGUMO VALDYMAS

Informacijos saugumo valdymo tikslas – užtikrinti organizacijos neskelbtinos informacijos, duomenų ir IT paslaugų konfidencialumą, vientisumą ir prieinamumą. Tam, kad būtų įvykdyti nuolatinės registrų jungties saugumo reikalavimai, be techninių komponentų, įskaitant projektavimą ir testavimą (žr. STS), reikia atlikti toliau nurodytas bendras darbo procedūras.

10.1. Neskelbtinos informacijos nustatymas

Informacijos vieneto slaptumas įvertinamas nustačius, kokį poveikį su šia informacija susijęs saugumo pažeidimas gali padaryti veiklai (pvz., gali būti patirta finansinių nuostolių, pablogėti įvaizdis, gali būti pažeisti įstatymai ir pan.).

Neskelbtinos informacijos ištekliai nustatomi pagal jų poveikį jungčiai.

Informacijos slaptumo lygis įvertinamas pagal šiai jungčiai taikytiną šio dokumento skirsnyje „Informacijos saugumo incidentų tvarkymas“ pateiktą slaptumo skalę.

10.2. Informacijos išteklių slaptumo lygiai

Tai nustačius, informacijos išteklius priskiriamas tam tikrai kategorijai, laikantis šių taisyklių:

- jeigu informacijos konfidencialumo, vientisumo arba prieinamumo lygis bent vienu atveju įvertinamas kaip „aukštas“, informacijos išteklius priskiriamas kategorijai „SPECIAL HANDLING: *ETS Critical*“;
- jeigu informacijos konfidencialumo, vientisumo arba prieinamumo lygis bent vienu atveju įvertinamas kaip „vidutinis“, informacijos išteklius priskiriamas kategorijai „SENSITIVE: *ETS*“;
- jeigu informacijos konfidencialumo, vientisumo arba prieinamumo lygis įvertinamas tik kaip „žemas“, informacijos išteklius pagal žymėjimą ES priskiriamas kategorijai „SENSITIVE: *ETS Joint Procurement*“, o o pagal žymėjimą Šveicarijoje – „LIMITED: ETS“.

10.3. Už informacijos išteklius atsakingo asmens paskyrimas

Turi būti paskirtas už kiekvieną informacijos išteklių atsakingas asmuo. ATLPS informacijos ištekliai, kurie priklauso ESSŽ ir SSTL jungčiai arba yra su ja susiję, turėtų būti įtraukti į abiejų Šalių tvarkomą bendrų išteklių sąrašą. ATLPS informacijos ištekliai, kurie nepriklauso ESSŽ ir SSTL jungčiai, turėtų būti įtraukti į atitinkamos Šalies tvarkomą išteklių sąrašą.

Šalys susitaria dėl atsakomybės už kiekvieną informacijos išteklių, kuris priklauso ESSŽ ir SSTL jungčiai arba yra su ja susijęs. Už informacijos išteklių atsakingas asmuo atsako už informacijos slaptumo įvertinimą.

Atsakingo asmens pareigų lygis turėtų atitikti priskirto (-ų) ištekliaus (-ių) vertę. Dėl atsakingo asmens atsakomybės už išteklių (-ius) ir jo pareigos užtikrinti reikalingą konfidencialumo, vientisumo ir prieinamumo lygį turėtų būti susitarta ir susitarimas turėtų būti įformintas.

10.4. Neskelbtinos informacijos registravimas

Visa neskelbtina informacija registruojama neskelbtinos informacijos sąraše (NIS).

Jeigu reikia, atsižvelgiama į neskelbtinos informacijos grupę, kuri gali lemti didesnį poveikį negu atskiras informacijos vienetas, ir tokia informacijos grupė yra registruojama NIS (pvz., informacijos rinkinys, saugomas sistemos duomenų bazėje).

NIS nėra statiškas. Su informacijos ištekliumi susijusių saugumo incidentų grėsmės, pažeidžiamos sritys, tikimybė arba padariniai gali keistis ir tai gali būti nepastebėta, o į registro sistemų darbą gali būti įtraukiami nauji ištekliai.

Todėl NIS turi būti reguliariai peržiūrimas ir visa nauja informacija, kuri nustatoma kaip neskelbtina, nedelsiant įtraukiama į NIS.

Kiekvieną NIS įrašą sudaro bent ši informacija:

- informacijos aprašymas;
- už informaciją atsakingas asmuo;
- slaptumo lygis;
- pastaba, ar informacija apima asmens duomenis;
- jeigu reikia, papildoma informacija.

10.5. Neskelbtinos informacijos tvarkymas

Neskelbtinos informacijos tvarkymas nesinaudojant Sąjungos registro ir Šveicarijos registro jungtimi atliekamas pagal tvarkymo instrukcijas.

Neskelbtinos informacijos tvarkymas naudojantis Sąjungos registro ir Šveicarijos registro jungtimi atliekamas pagal Šalių saugumo reikalavimus.

10.6. Prieigos valdymas

Prieigos valdymo tikslas – suteikti įgaliotiems naudotojams teisę naudotis paslauga ir neleisti ja naudotis reikiamo leidimo neturintiems naudotojams. Prieigos valdymas kartais taip pat vadinamas teisių valdymu arba tapatybės valdymu.

Nuolatinės registrų jungties ir naudojimosi ja tikslais abi Šalys turi turėti prieigą prie šių komponentų:

- vikio – bendradarbiavimo aplinkos, kurioje keičiamasi bendra informacija, pavyzdžiui, versijų išleidimo planais;
- IT paslaugų valdymo priemonės, skirtos incidentams ir problemoms valdyti (žr. 3 skyrių „Metodika ir standartai“);
- keitimosi pranešimais sistemos – kiekviena Šalis pasirūpina saugia keitimosi pranešimais ir pranešimų perdavimo sistema, kuria naudojantis būtų perduodami pranešimai su sandorio duomenimis.

Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius užtikrina, kad prieiga būtų atnaujinta, ir prieigos valdymo tikslais atlieka savo Šalių kontaktinių centrų funkcijas. Prieigos užklausos yra tvarkomos pagal užklausų vykdymo procedūras.

10.7. Sertifikato ir (arba) rakto valdymas

Kiekviena Šalis yra atsakinga už savo sertifikato ir (arba) rakto valdymą (sukūrimą, registravimą, saugojimą, įdiegimą, naudojimą, atnaujinimą, panaikinimą, atsarginės kopijos išsaugojimą ir atkūrimą). Kaip nurodyta susiejimo techniniuose standartuose (STS), naudojami tik skaitmeninius sertifikatus teikiančios organizacijos, kuria pasitiki abi Šalys, išduoti skaitmeniniai sertifikatai. Sertifikatai ir (arba) raktai tvarkomi ir saugomi laikantis tvarkymo instrukcijų nuostatų.

Visus sertifikatų ir raktų panaikinimo ir (arba) atnaujinimo veiksmus suderina abi Šalys. Tai atliekama pagal užklausų vykdymo procedūras.

Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius vienas kitam sertifikatus ir (arba) raktus perduoda saugiomis ryšio priemonėmis, laikydamiesi tvarkymo instrukcijose išdėstytų nuostatų.

Visa sertifikatų ir (arba) raktų patikra tarp Šalių atliekama naudojantis atskiru duomenų perdavimo kanalu.

III 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

Nuolatinės registrų jungties standartas

Turinys

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 bet kurio subjekto ATLPS reikalavimų
ŠK	Šveicarijos Konfederacija
CHU	ŠK išduotas stacionarių įrenginių apyvartinis taršos leidimas, dar vadinamas CHU2 (daroma nuoroda į 2-ąjį įsipareigojimų pagal Kioto protokolą laikotarpį)
CHUA	Šveicarijos aviacijos apyvartinis taršos leidimas (angl. *Swiss Aviation Allowance*)
BDP	bendros darbo procedūros kartu parengtos procedūros, skirtos ES ATLPS ir Šveicarijos ATLPS praktiškai susieti
ATLR	apyvartinių taršos leidimų registras
ATLPS	apyvartinių taršos leidimų prekybos sistema
ES	Europos Sąjunga

Santrumpa / sąvoka	Apibrėžtis
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 apyvartinių taršos leidimų apskaitos sistema, kurioje registruojami elektroninėse sąskaitose laikomų leidimų turėtojai
SSTL	Šveicarijos papildomų sandorių žurnalas (angl. *Swiss Suplementary Transaction Log*)
sandoris	registre vykdomas procesas, per kurį apyvartinis taršos leidimas perduodamas 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
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 parodyti, 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
skverbimosi testavimas	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*)

Santrumpa	Apibrėžtis
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, sukuriama tiesioginė jungtis tarp Sąjungos registro Europos Sąjungos sandorių žurnalo (ESSŽ) ir Šveicarijos registro Šveicarijos papildomų sandorių žurnalo (SSTL), kad pagal bet kurią iš šių dviejų ATLPS išduoti apyvartiniai taršos leidimai galėtų būti perduoti iš vieno registro į kitą (Susitarimo 3 straipsnio 2 dalis). Siekiant praktiškai susieti ES ATLPS ir Šveicarijos ATLPS, 2020 m. pradėtas taikyti laikinas sprendimas. Nuo 2023 m. šias dvi ATLPS siejanti registrų jungtis palaipsniui plėtojama siekiant, kad ji (kaip tikimasi) ne vėliau kaip 2024 m. taptų nuolatine registrų jungtimi, sudarančia sąlygas veikti susietoms rinkoms, kuriose galima naudotis jų likvidumo teikiama nauda ir sandorius tarp šių susietų sistemų vykdyti taip, kaip jie vykdomi vienoje rinkoje, sudarytoje iš dviejų sistemų. Taigi, rinkos dalyviai galės veikti taip, tarsi jie būtų vienoje rinkoje, tačiau turės paisyti atskirų Šalių reguliavimo nuostatų (Susitarimo II priedas).

Pagal Susitarimo 3 straipsnio 7 dalį Šveicarijos registro administratorius ir Sąjungos registro vyriausiasis administratorius, remdamiesi Susitarimo II priede išdėstytais kriterijais, parengia susiejimo techninius standartus (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.

Jungtinis komitetas STS patvirtino Sprendimu Nr. 2/2020. Šiame dokumente išdėstytus atnaujintus STS Jungtinis komitetas patvirtins Sprendimu Nr. 1/2024. Pagal šį sprendimą ir atsižvelgdami į Jungtinio komiteto prašymus Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius parengė bei atnaujins išsamesnes praktinio susiejimo technines gaires ir užtikrins, kad jos būtų nuolat tikslinamos atsižvelgiant į technikos pažangą ir (arba) naujus reikalavimus, susijusius su jungties sauga ir saugumu ir jos veiksmingu bei efektyviu veikimu.

2.1. Taikymo sritis

Šiame dokumente įtvirtintas bendras Susitarimo šalių susitarimas dėl jungties tarp ES ATLPS ir Šveicarijos APTLPS 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 tolesnio jos praktinio įgyvendinimo procesai ir procedūros. Pagal Susitarimo 3 straipsnio 6 dalį šie aspektai aprašomi Jungtinio komiteto sprendimu atskirai priimtose bendrose darbo procedūrose (BDP).

2.2. Adresatai

Šis dokumentas skirtas Šveicarijos registro administratoriui ir Sąjungos registro 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 susiejimo architektūra.

Kadangi apibrėžiant architektūrą viena iš sričių, kuriai skiriama daugiausia dėmesio, yra saugumas, buvo imtasi visų priemonių, kad architektūra būtų patikima. Nuolatinėje registrų jungtyje naudojamas keitimosi failais mechanizmas, kuriuo užtikrinama saugi izoliuotoji jungtis.

Pagal techninį sprendimą naudojami:

- saugaus keitimosi pranešimais protokolas;
- XML pranešimai;
- XML pagrindu veikiantis skaitmeninis parašas ir užšifravimas;
- VPN.

Tolesniame paveiksle pavaizduota bendra nuolatinės registrų jungties architektūra.

3.1.1. Keitimasis pranešimais

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

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

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

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

3.1.2. XML pranešimas – bendras apibūdinimas

XML pranešimą sudaro vienas 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 nurodoma:

- ATLPS sistema, iš kurios siunčiamas pranešimas;
- sekos numeris.

3.1.3. Pranešimų nuskaitymo langai

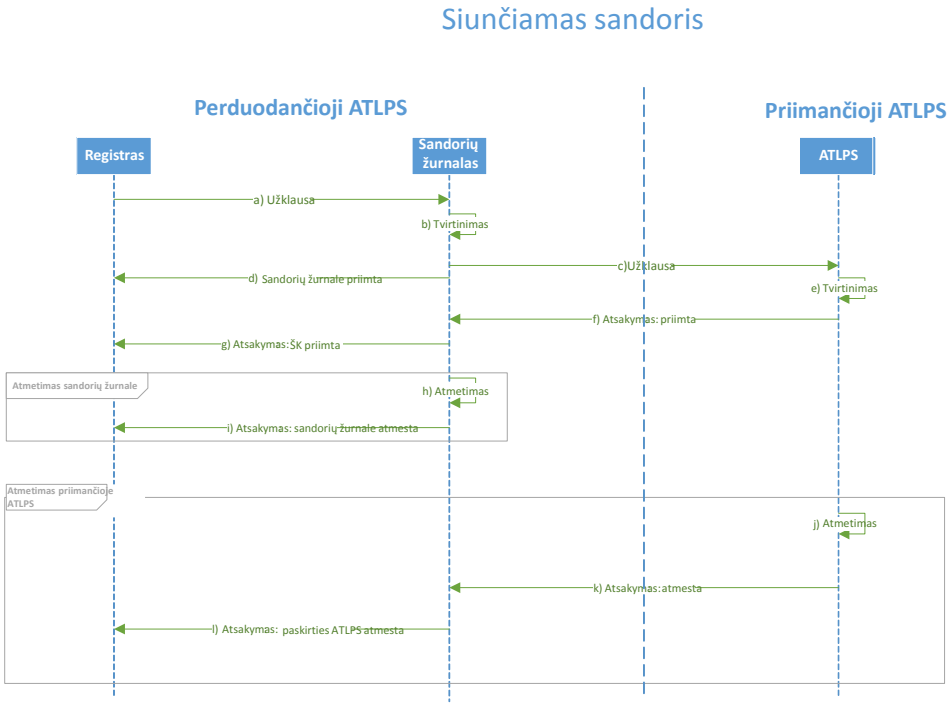
Nuolatinei registrų jungčiai naudojami iš anksto apibrėžti pranešimų nuskaitymo langai ir įvardytų įvykių rinkiniai. Sandorių užklausos, gautos per jungtį, bus nuskaitomos tik nustatytais intervalais. Nuskaitymo procesas apima techninį siunčiamų ir gaunamų sandorių užklausų tvirtinimą. Taip pat pažymėtina, 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. Konkretus procesas yra pavaizduotas toliau pateiktoje procesų diagramoje.



Pagrindinį procesą sudaro šie etapai (kaip parodyta pirmiau pateiktoje diagramoje):

(a) 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 siunčiamas į užklausą atsiuntusios ATLPS registrą;
(e) paskirties ATLPS sandorio užklausa tvirtinama;
(f) iš paskirties ATLPS siunčiamas pranešimas apie priėmimą į užklausą atsiuntusios ATLPS sandorių žurnalą;
(g) iš sandorių žurnalo į registrą siunčiamas atsakymas apie priėmimą.

Alternatyvus procesas „atmetimas sandorių žurnale“ (kaip parodyta pirmiau pateiktoje diagramoje, pradedant nuo a veiksmo pagrindiniame procese):

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

(b) sandorių žurnale užklausa nepatvirtinama;

(c) į užklausą atsiuntusį registrą siunčiamas atsakymas apie atmetimą.

Alternatyvus procesas „atmetimas ATLPS“ (kaip parodyta pirmiau pateiktoje diagramoje, pradedant nuo d veiksmo pagrindiniame procese):

(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;

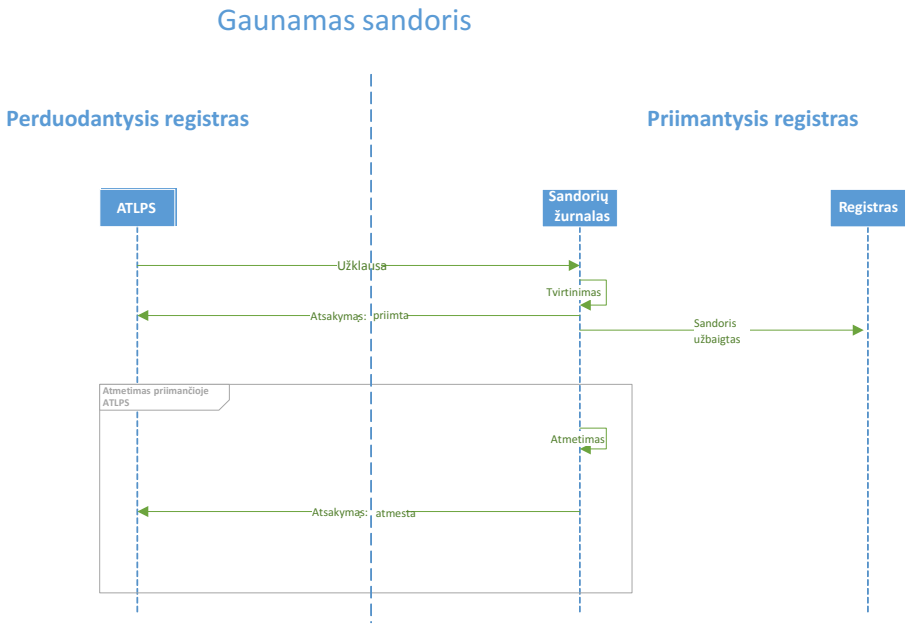
(d) pranešimas apie priėmimą yra siunčiamas į užklausą atsiuntusios ATLPS registrą;

(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 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 lygmenys:

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

(2) užšifravimas siuntimo lygmeniu: VPN;

(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 (VPN)

Visi Šalių tarpusavio pranešimai apsaugomi naudojant VPN technologijas. 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 galinio taško 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.

Apskritai Europos Sąjungoje, kaip privatus IP grindžiamas tinklas, naudojamas saugus telematikos paslaugų tarp Europos administracijų tinklas (STESTA). Todėl šis tinklas taip pat yra tinkamas naudoti nuolatinei registrų jungčiai.

3.2.3. IPSec diegimas

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, nuolatinėje registrų jungtyje naudojami keli užšifravimo lygmenys. Abi sistemos ir jų aplinka yra sujungtos tarpusavyje tinklo lygmeniu sukuriant VPN tunelius. 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

Užšifruojant ir pasirašant 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 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. Bus atliekamas bent planinis suderinimas, tačiau tik po nuskaitymo.

Kiekviena Šalis vis tiek gali bet kuriuo metu inicijuoti suderinimą rankiniu būdu.

Planinio suderinimo periodiškumo ir 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, pagal kuriuos bus galima suprasti, kad pranešimas yra bandomasis. Iš kito galinio taško įrenginio bus atsiųstas atsakymas.

3.4. Duomenų registravimo reikalavimai

Atsižvelgiant į tai, kad abi Šalys turi turėti tikslią ir nuoseklią informaciją, taip pat siekiant Šalims suteikti priemones, kurias 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 problemų šalinimo tikslais saugomi ne trumpiau kaip tris (3) mėnesius, o tolesnis jų saugojimas priklauso nuo kiekvienam galinio taško įrenginiui taikytinų teisės aktų dėl duomenų saugojimo audito tikslais. Senesni negu trijų (3) mėnesių žurnalo failai gali būti archyvuojami saugioje vietoje nepriklausomoje IT sistemoje, kurioje juos būtų galima nuskaityti arba prie kurios būtų galima prisijungti per pagrįstą laikotarpį.

Sandorių žurnalai

Sandorių žurnalai įdiegiami tiek ESSŽ, tiek SSTL posistemėje ir patikrinama, ar jie dera abejose ATLPS sistemose.

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: suderinimo būklė „sutampa“ arba „nesutampa“. Per nuolatinę registrų jungtį siunčiami suderinimo pranešimai yra neatsiejama pranešimų, kuriais keičiamasi, dalis, todėl jie saugomi, kaip aprašyta skirsnyje „Pranešimų archyvas“.

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, kuriuo saugomas archyvas, yra auditas. Archyvas taip pat saugomas tam, kad būtų turimi įrodymai apie tai, kas buvo siųsta kitai Šaliai ir iš jos gauta. Todėl 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.

3.5. Darbo reikalavimai

Duomenimis tarp abiejų sistemų per nuolatinę registrų jungtį keičiamasi ne visiškai autonomiškai, tai yra, tam, kad jungtis veiktų praktiškai, reikalingi operatoriai ir procedūros. Todėl išsamiai aprašomi keli šiame procese atliekami vaidmenys ir naudojamos priemonės.

4. NUOSTATOS DĖL PRIEINAMUMO

4.1. Ryšio prieinamumo struktūra

Nuolatinės registrų jungties architektūrą iš esmės sudaro IRT infrastruktūra ir programinė įranga, kuri suteikia galimybę palaikyti ryšį tarp Šveicarijos ATLPS ir ES ATLPS. Kuriant 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, įdiegiant nuolatinę registrų jungtį sukuriamas atsparus VPN, 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

Per nuolatinę registrų jungtį Šalys duomenimis keičiasi iš anksto nustatytais intervalais. 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 kiekvieno etapo laiko intervalai;
- nuolatinės registrų jungties 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 nuolatinės registrų jungties 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 atliekami kaskart, kai nuolatinėje registrų jungtyje 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 bandymų modulį turėtų sudaryti:

- bandymų kriterijai ir priemonės;
- priskirtos bandymų vykdymo pareigos;
- numatomi rezultatai (teigiami ir neigiami);
- bandymų tvarkaraštis;
- bandymų rezultatų registravimo reikalavimai;
- sutrikimų šalinimo dokumentavimas;
- nuostatos dėl perdavimo į kitą sprendimų lygmenį.

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

4.2.1. IRT infrastruktūros vidaus bandymai

Šiuos bandymus kiekviename galiniame taške turi individualiai atlikti ir (arba) tikrinti registrų administratoriai.

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 pradeda kiekviena Šalis individualiai, o jie užbaigiami abiem Šalims bendradarbiaujant.

Kai pavieniai elementai veikia, reikia išbandyti registrų tarpusavio ryšio kanalus. Tuo tikslu kiekviena Šalis patikrina, ar veikia interneto prieiga, ar sukurti VPN tuneliai ir ar veikia IP ryšys tarp skirtingose vietose esančių įrenginių. Tada kitam galiniam taškui turėtų būti patvirtintas vietos ir nuotolinių infrastruktūros elementų prieinamumas ir IP ryšys.

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 kiekviename galiniame taške turi atlikti ir (arba) inicijuoti registrų administratoriai, kaip nurodyta skirsniuose „Saugumo bandymų gairės“ ir „Nuostatos dėl rizikos vertinimo“.

Tik tada, kai kiekvienas iš keturių etapų ir (arba) modulių yra užbaigiamas gavus prognozuojamus rezultatus, galima daryti išvadą, kad nuolatinė registrų 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

nuolatines 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: nuolatinės registrų 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 / 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.

Visos trys aplinkos yra viena nuo kitos visiškai nepriklausomos, t. y. aparatinė, programinė įranga, duomenų bazės, virtuali aplinka, IP adresai, prievadai yra įrengti ir veikia nepriklausomai vieni nuo kitų; tai nepasakytina apie VPN.

Dėl VPN sandaros pažymėtina, kad ryšys tarp šių trijų aplinkų turi būti visiškai nepriklausomas; tai užtikrinama naudojant STESTA.

5. NUOSTATOS DĖL KONFIDENCIALUMO IR VIENTISUMO

Pagal saugumo mechanizmus ir procedūras yra numatyta, kad operacijas, kurios vykdomos per Sąjungos ir Šveicarijos registrų jungtį, atlieka po du asmenis (4 akių principas). Principas, kai vieną operaciją atlieka du asmenys, taikomas visada, kai to reikia, tačiau jis gali būti taikomas ne visiems registrų administratorių veiksmams.

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 naudojamas pažeidžiamoms vietoms kūrimo ir eksploatavimo etapais nustatyti):

- 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, skverbimosi testavimas), abi Šalys įsipareigoja įprastus vertinimus atlikti tik bandymo ir priėmimo aplinkose (kaip aprašyta skirsnyje „Priėmimo / 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 skirsnyje „Ryšio jungties architektūra“).

Bandymų infrastruktūra ir tinklo, ir infrastruktūros lygmenimis turi būti atskirta nuo darbinės aplinkos ir joje turėtų būti sąlygos atlikti saugumo bandymus, kurie yra reikalingi atitikčiai saugumo reikalavimams patikrinti.

5.2. Nuostatos dėl jungties veikimo sustabdymo ir veikimo atnaujinimo

Jei įtariama, kad Šveicarijos registro, SSTL, Sąjungos registro ar ESSŽ saugumui buvo pakenkta, abi Šalys nedelsdamos viena kitą apie tai informuoja ir sustabdo SSTL ir ESSŽ jungties veikimą.

Nuostatos dėl keitimosi informacija, sprendimo sustabdyti jungties veikimą ir sprendimo jungties veikimą atnaujinti yra aprašytos BDP skirsnyje „Užklausų vykdymas“.

Veikimo sustabdymas

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

- administracinių priežasčių (techninės priežiūros ir pan.), t. y. planuotai;
- saugumo priežasčių (arba IT infrastruktūros gedimų), t. y. neplanuotai.

Nenumatytu kritiniu atveju kiekviena Šalis apie jį informuoja kitą Šalį ir vienašališkai sustabdo registrų jungties veikimą.

Jeigu priimamas sprendimas sustabdyti 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 ryšio atnaujinimo priimamas BDP aprašyta tvarka ir bet kuriuo atveju ryšys nėra atnaujinamas, kol nebus sėkmingai atliktos saugumo bandymų procedūros, aprašytos skirsniuose „Saugumo bandymų gairės“ ir „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 laikoma neskelbtina, yra žymima žyma „SPECIAL HANDLING: *ETS Critical*“ ir tvarkoma pagal tvarkymo instrukcijas, nebent nustatoma 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, skverbimosi testavimą, atliekami bent su visomis naujomis programinės įrangos versijomis, laikantis STS išdėstytų saugumo reikalavimų, kad būtų įvertintas jungties saugumas ir susijusi rizika.

Jeigu per paskutinius 12 mėnesių jokia didesnė versija nėra sukuriama, saugumo bandymas atliekamas su tuo metu naudojama sistema, atsižvelgiant į per pastaruosius 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 laikantis ankstesniame skirsnyje aprašytų principų ir naudojantis naujausia pažeidžiamumo duomenų baze.

5.5. Nuostatos dėl rizikos vertinimo

Jeigu turi būti atliekamas skverbimosi testavimas, jis įtraukiamas į saugumo bandymą.

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

- turi su tokiais saugumo bandymais susijusių įgūdžių ir patirties;
- nėra tiesiogiai atskaitinga programinės įrangos kūrėjui ir (arba) rangovui, nedalyvavo kuriant jungties programinę įrangą ir nėra ją kuriančio subjekto subrangovas;
- pasirašė informacijos neatskleidimo sutartį, pagal kurią įsipareigojo rezultatus saugoti paslaptyje, tvarkyti juos laikydamasi lygmeniu „SPECIAL HANDLING: *ETS Critical*“ taikomų reikalavimų ir tvarkymo instrukcijų.