



Europos Sąjungos
Taryba

Briuselis, 2020 m. spalio 6 d.
(OR. en)

10831/20

Tarpinstitucinė byla:
2020/0123 (NLE)

ENV 516
CLIMA 187
ENER 290
IND 135
COMPET 405
MI 333
ECOFIN 803
TRANS 397
AELE 52
CH 24

TEISĖS AKTAI IR KITI DOKUMENTAI

Dalykas: EUROPOS SAJUNGOS IR ŠVEICARIJOS KONFEDERACIJOS
SUSITARIMU DĖL JŲ ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ
APYVARTINIŲ TARŠOS LEIDIMŲ PREKYBOS SISTEMŲ SUSIEJIMO
ĮSTEIGTO JUNGTINIO KOMITETO SPRENDIMO dėl bendrų darbo
procedūrų (BDP) priėmimo projektas

PROJEKTAS

**EUROPOS SĄJUNGOS IR ŠVEICARIJOS KONFEDERACIJOS
SUSITARIMU DĖL JŲ ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ
APYVARTINIŲ TARŠOS LEIDIMŲ PREKYBOS SISTEMŲ SUSIEJIMO
ĮSTEIGTO JUNG TINIO KOMITETO
SPRENDIMAS Nr. 1/2020**

... m. ... d.

dėl bendrų darbo procedūrų (BDP) priėmimo

JUNGTINIS KOMITETAS

atsižvelgdamas į Europos Sąjungos ir Šveicarijos Konfederacijos susitarimą dėl jų šiltnamio efektą sukeliančių dujų apyvartinių taršos leidimų prekybos sistemų susiejimo¹ (toliau – Susitarimas), ypač į jo 3 straipsnio 6 dalį,

¹ OL L 322, 2017 12 7, p. 3.

kadangi:

- (1) 2019 m. gruodžio 5 d. Jungtinio komiteto sprendimu Nr. 2/2019¹ buvo iš dalies pakeisti Susitarimo I ir II priedai ir taip buvo išpildytos Susitarime nustatytos susiejimo sąlygos;
- (2) Jungtiniam komitetui priėmus Sprendimą Nr. 2/2019, vadovaudamosi Susitarimo 21 straipsnio 3 dalimi Šalys apsikeitė ratifikavimo arba patvirtinimo dokumentais, nes, jų manymu, visos Susitarime apibrėžtos susiejimo sąlygos buvo išpildytos;
- (3) pagal Susitarimo 21 straipsnio 4 dalį Susitarimas įsigaliojo 2020 m. sausio 1 d.;

¹ 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).

- (4) pagal Susitarimo 3 straipsnio 6 dalį Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius, atsižvelgdami į Šalių vidaus teisės prioritetus, turėtų nustatyti bendras darbo procedūras (toliau – BDP), kurios susijusios su techniniais ar kitais klausimais, būtinais jungties tarp Sąjungos registro Europos Sąjungos sandorių žurnalo (toliau – ESSŽ) ir Šveicarijos registro Šveicarijos papildomų sandorių žurnalo (angl. *Swiss Supplementary Transaction Log*) (toliau – SSTL) veikimui užtikrinti. BDP turėtų įsigaliooti, kai jas sprendimu patvirtina Jungtinis komitetas;
- (5) laikydamasis Susitarimo 13 straipsnio 1 dalies Jungtinis komitetas, atsižvelgdamas į Šalių vidaus teisės prioritetus, turėtų susitarti dėl techninių gairių, kuriomis būtų užtikrintas tinkamas Susitarimo įgyvendinimas, įskaitant techninius ar kitus klausimus, būtinus jungties veikimui užtikrinti. Technines gaires gali parengti pagal Susitarimo 12 straipsnio 5 dalį sudaryta darbo grupė. Į darbo grupę turėtų būti įtraukti bent Šveicarijos registro administratorius ir Sąjungos vyriausiasis administratorius; ji turėtų padėti Jungtiniam komitetui vykdyti jo funkcijas pagal Susitarimo 13 straipsnį;
- (6) atsižvelgiant į techninį gairių pobūdį ir poreikį koreguoti jas atsižvelgiant į vykstančius pokyčius, Šveicarijos registro administratoriaus ir Sąjungos vyriausiojo administratoriaus parengtos techninės gairės turėtų būti teikiamos Jungtiniam komitetui susipažinti arba, kai tikslinga, patvirtinti,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Prie šio sprendimo pridėtos bendros darbo procedūros (toliau – BDP) yra patvirtinamos.

2 straipsnis

Vadovaujantis Susitarimo 12 straipsnio 5 dalimi, sudaroma darbo grupė. Ji padeda Jungtiniam komitetui užtikrinti tinkamą Susitarimo įgyvendinimą, įskaitant techninių gairių, skirtų BDP įgyvendinimui, parengimą.

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

3 straipsnis

Šis sprendimas įsigalioja jo priėmimo dieną.

Priimta Briuselyje 2020 m. d.

Jungtinio komiteto vardu

Europos Sąjungos sekretorius

Pirmininkas

Šveicarijos sekretorius

PRIEDAS

BENDROS DARBO PROCEDŪROS (BDP)
PAGAL EUROPOS SAJUNGOS IR ŠVEICARIJOS KONFEDERACIJOS
SUSITARIMO DĖL JŲ ŠILTNAMIO EFEKTĄ SUKELIANČIŲ DUJŲ
APYVARTINIŲ TARŠOS LEIDIMŲ PREKYBOS SISTEMŲ SUSIEJIMO
3 STRAIPSNIO 6 DALĮ

Laikinam sprendimui skirtos procedūros

1. Sąvokų žodynėlis

1-1 lentelė. Santrumpos ir terminų apibrėžtys

Santrumpa / terminas	Termino apibrėžtis
Skaitmeninį sertifikatą teikianti organizacija (SSTO)	Skaitmeninius sertifikatus išduodantis subjektas.
ŠK	Šveicarijos Konfederacija
ATLPS	Apyvartinių taršos leidimų prekybos sistema
ES	Europos Sąjunga
IVG	Incidentų valdymo grupė
Informacijos išteklius	Įmonei ar organizacijai vertingas informacijos vienetas.

Santrumpa / terminas	Termino apibrėžtis
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 keisti informacija ir žiniomis papildydami ar koreguodami turinį tiesiogiai interneto svetainės naršyklėje.

2. Ižanga

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 pagal Europos Sąjungos apyvartinių taršos leidimų prekybos sistemą (toliau – ES ATLPS) arba Šveicarijos apyvartinių taršos leidimų prekybos sistemą (toliau – Šveicarijos ATLPS) užtikrinti, 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, ne vėliau kaip 2020 m. gegužės mėn. arba kuo anksčiau po šios datos pradedamas taikyti laikinas sprendimas. Šalys bendradarbiauja siekdamos kuo anksčiau pakeisti laikiną sprendimą nuolatine registro jungtimi (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, būtiniais jungties veikimui užtikrinti, susijusias bendras darbo procedūras (toliau – BDP). Administratorių parengtos BDP įsigalioja, kai jas sprendimu patvirtina Jungtinis komitetas.

Šiame dokumente išdėstytas BDP savo sprendimu Nr. 1/2020 turi patvirtinti Jungtinis komitetas. Pagal šį sprendimą Jungtinis komitetas prašo Šveicarijos registro administratoriaus ir Sąjungos vyriausiojo administratoriaus parengti išsamesnes technines gaires, kad jungtis būtų įgyvendinta praktiškai, ir užtikrinti, kad jos būtų nuolat koreguojamos atsižvelgiant į technikos pažangą ir naujus reikalavimus, susijusius su jungties sauga ir saugumu bei jos veiksmingu ir efektyviu veikimu.

2.1. Taikymo sritis

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

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

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

Pagal laikiną sprendimą, dėl kurio susitarta, bus reikalingos tik šios šiame dokumente aprašytos BDP:

- incidentų valdymas;
- problemų valdymas;
- užklausų vykdymas;
- pakeitimų valdymas;
- versijų valdymas;
- saugumo incidentų valdymas;
- informacijos saugumo valdymas.

Ateityje, kai bus įdiegta nuolatinė registų jungtis, reikiamas BDP nuostatas reikės koreguoti ir papildyti.

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 aprašyti BDP remiantis ITIB (Informacinių technologijų infrastruktūros biblioteka, 3 versija). Šiame standarte apibrėžta praktika naudojama ir koreguojama pagal konkrečius su laikinu sprendimu susijusius poreikius;
- abi Šalys ryšį palaiko ir BDP vykdymą koordinuoja, kai tai yra būtina BDP vykdyti, 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, bendras sprendimo priėmimas perduodamas į aukštesnį sprendimų lygmenį.

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 Susitarimo 12 straipsnio 5 dalį)	
4-asis lygmuo	Jungtinis komitetas, jeigu 3-iojo lygmens atsakomybė yra deleguojama	

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

4. Incidentų valdymas

Incidentų valdymo proceso tikslas – kuo greičiau po incidento 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 siekiant nuolatinio tobulėjimo.

Žvelgiant plačiau, incidentų valdymą sudaro ši veikla:

- incidentų nustatymas ir registravimas;
- klasifikavimas ir pradinė pagalba;
- tyrimas ir problemos nustatymas;
- sprendimas ir padėties atkūrimas;
- incidento užbaigimo procedūra.

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 vykdančys techniniai darbuotojai.

Nustačius incidentą, jis registruojamas ir jam suteikiama unikali identifikavimo žyma, kad incidentą būtų galima tinkamai sekti ir stebėti. Unikali incidento identifikavimo žyma – tai žyma, kurią incidentą užfiksavusios Šalies (ES arba ŠK) aptarnavimo centras priskiria bendroje pagalbos prašymų sistemoje (angl. *common ticketing system*) ir kuri turi būti naudojama visoje su incidentu susijusioje komunikacijoje.

Kiekvieno incidento atveju 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 incidentu padarytas poveikis ir kokio dydžio yra tas poveikis. 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 priskiriamas kuriai nors kategorijai bei pagal incidento poveikį ir sprendimo skubumą jam 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 tuomet valdomas laikantis šio dokumento skyriuje „Saugumo incidentų valdymas“ aprašyta tvarka.

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

Jeigu aptarnavimo centrui incidentą pavyksta sėkmingai išspręsti, jis atlieka incidento užbaigimo procedūrą, nes pirminė incidentų valdymo paskirtis (būtent – greitai atkurti paslaugas galutiniam naudotojui) buvo pasiekta. Jeigu incidento išspręsti nepavyksta, aptarnavimo centras dėl tolesnio incidento sprendimo kreipiasi į tinkamą incidentų šalinimo grupę, kad ši ištirtų incidentą ir nustatytų problemą.

4.3. Tyrimas ir problemos nustatymas

Incidento tyrimo ir problemos nustatymo procedūros vykdomos, kai aptarnavimo centrui per pradinį incidento įvertinimą incidento išspręsti nepavyksta ir dėl to incidentą spręsti perduodama kitam sprendimų lygmeniui. Incidento perdavimas spręsti kitam sprendimų lygmeniui 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 kitam sprendimų lygmeniui, yra pripažįstama, kad incidento pradiniu pagalbos lygmeniu išspręsti nepavyko ir kad incidento sprendimą reikia perduoti aukštesnio lygmens pagalbos grupei arba kitai Šaliai. Incidento perdavimas spręsti kitam sprendimų lygmeniui gali vykti dviem kryptimis: horizontaliai (pagal funkcijas) arba vertikalčiai (pagal hierarchiją).

Aptarnavimo centras, kuris užregistravo incidentą ir inicijavo jo sprendimą, yra atsakingas už incidento sprendimo perdavimą atitinkamam padaliniiui ir už bendros incidento sprendimo būklės ir jo paskyrimo sekimą.

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

4.4. Sprendimas ir padėties atkūrimas

Visapusiškai supratus incidentą, jis išsprendžiamas ir padėtis atkuriamą. Rasti incidento sprendimą reiškia, kad randamas būdas, kaip ištaisyti atsiradusią problemą. Sprendimo pritaikymo veiksmai sudaro padėties atkūrimo etapą.

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

Padėties atkūrimo darbus gali atlikti IT priežiūros specialistai arba galutiniam naudotojui gali būti pateiktos instrukcijos.

4.5. Incidento užbaigimo procedūra

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

Svarbiausi veiksmai, kuriuos reikia atlikti incidento užbaigimo etapu, veiksmų kontroliniame sąraše yra šie:

- pradinės kategorijos, prie kurios buvo priskirtas incidentas, patikrinimas;
- tinkamas visos informacijos, susijusios su incidentu surinkimas;
- tinkamas incidento dokumentavimas ir žinių bazės atnaujinimas;
- tinkamas komunikavimas su kiekvienu suinteresuotuoju subjektu, kuriam incidentas yra tiesiogiai ar netiesiogiai aktualus.

Incidentas oficialiai užbaigiamas, kai aptarnavimo centras baigia incidento užbaigimo etapą ir informaciją apie tai perduoda kitai Šaliai.

Atlikus incidento užbaigimo procedūras jis nebeatnaujinamas. Jeigu incidentas netrukus pasikartoja, ankstesnis incidentas nėra atnaujinamas ir yra registruojamas naujas incidentas.

Jeigu incidentą stebi ir ES, ir ŠK aptarnavimo centrai, už galutines incidento užbaigimo procedūras yra atsakingas pagalbos prašymą užregistravęs aptarnavimo centras.

5. Problemų valdymas

Šią procedūrą reikėtų vykdyti kaskart, kai nustatoma problema, taigi, kai atsiranda pagrindas vykdyti problemų valdymo procesą. Problemų valdymo proceso tikslas – gerinti kokybę ir mažinti kylančių incidentų skaičių. Problemos priežastis gali būti vienas ar keli incidentai. Kai gaunamas pranešimas apie incidentą, incidentų valdymo specialistų tikslas yra kuo greičiau atkurti paslaugas, jeigu galima – pasinaudojant aplinkiniais sprendimo būdais. Iškilus problemai, stengiamasi išsiaiškinti 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 inicijavęs ES arba ŠK aptarnavimo centras.

Problemos unikali identifikavimo žyma – tai per IT paslaugų valdymo (ITPV) procesą suteikta identifikavimo žyma. Ją reikia nurodyti visoje su šia problema susijusioje komunikacijoje.

Problema gali atsirasti dėl incidento arba gali būti iškelta savo iniciatyva siekiant ištaisyti bet kuriuo metu 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 įvertinimas

Problema gali iškelti kiekviena Šalis; už problemos registravimą, jos perdavimą spręsti atitinkamam padaliniui ir bendrą problemos būklės sekimą yra atsakingas problemos sprendimą inicijavusios Šalies aptarnavimo centras.

Problemos sprendimo grupė, kuriai perduotas problemos sprendimas, 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 užbaigimas

Problema oficialiai užbaigiama, kai atliekami reikiami pakeitimai ir problema išsprendžiama. Problemos užbaigimo etapas atliekamas aptarnavimo centro, kuris problemą užregistravo ir informavo apie ją kitos Šalies aptarnavimo centrą.

6. Užklausų vykdymas

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

Toliau aprašyti pagrindiniai etapai, kuriuos reikia atlikti.

6.1. Užklauso inicijavimas

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

6.2. Užklauso registravimas ir analizė

Visais paslaugų užklauso atvejais kontaktinio centro funkcijas turėtų atlikti ES arba ŠK aptarnavimo centras, priklausomai nuo to, kuri Šalis pateikė paslaugos užklauso. Šis aptarnavimo centras bus atsakingas už paslaugos užklauso registravimą ir tinkamo nuodugnumo analizę.

6.3. Užklauso patvirtinimas

Paslaugos užklauso 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 užklauso nepatvirtinama, aptarnavimo centras atnaujina ir užbaigia užklauso.

6.4. Užklauso vykdydas

Šis žingsnis skirtas paslaugų užklausoms efektyviai ir veiksmingai tvarkyti. Reikėtų atskirti šiuos atvejus:

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

Kai paslaugos užklausa įvykdoma, jos būklė pakeičiama į išspręsta.

6.5. Užklauso perdavimas spręsti kitam sprendimų lygmeniui

Jeigu reikia, aptarnavimo centras neįvykdytą paslaugos užklauso sprendimą gali perduoti tinkamiems kito lygmens padaliniais (trečiajai šaliai).

Paslaugos užklauso perdavimas spręsti kitam sprendimų lygmeniui vykdomas atitinkamoms trečiosioms šalims, t. y. jeigu paslaugos užklauso perdavimas spręsti kitam sprendimų lygmeniui vyks ŠK trečiajai šaliai, ES aptarnavimo centras turės kreiptis į ŠK aptarnavimo centrą ir atvirkščiai.

Trečioji šalis, kuriai buvo perduotas paslaugos užklauso sprendimas, yra atsakinga už tai, kad paslaugos užklausa būtų įvykdyta laiku ir kad su aptarnavimo centru, kuris perdavė paslaugos užklausa, būtų palaikomas ryšys.

Aptarnavimo centras, kuris užregistravo paslaugos užklausa, yra atsakingas už paslaugos užklauso bendros būklės ir paskyrimo sekima.

6.6. Užklauso vykdymo peržiūra

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

6.7. Užklauso užbaigimas

Jeigu Šalys, kurioms paslaugos užklausa buvo priskirta, sutinka, kad užklausa yra įvykdyta, o prašymo pateikėjas pripažįsta, kad atvejis išspręstas, užklauso būklė pakeičiama į „užbaigta“.

Paslaugos užklausa oficialiai užbaigiamas, kai paslaugos užklausa užregistravęs aptarnavimo centras baigia užklauso užbaigimo etapą 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 bei taip būtų užtikrinta, kad su jais susijusių incidentų kiltų kuo mažiau ir visų atitinkamų incidentų poveikis paslaugoms būtų kuo mažesnis. Pakeitimai IT infrastruktūroje gali būti atliekami reaguojant į problemas ar 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 verslo iniciatyvas ar kad į jas būtų atsižvelgta.

Pakeitimų valdymo procesą sudaro įvairūs žingsniai, kuriais visi pakeitimo užklauso aspektai yra užregistruojami, kad ateityje juos būtų galima atsekti. Per šiuos procesus užtikrinama, kad prieš diegiant pakeitimą, jis būtų patvirtintas ir ištestuotas. Versijų valdymo procesu užtikrinamas sėkmingas diegimas.

7.1. Pakeitimo užklausa

Pakeitimo užklausa (PU) teikiama pakeitimų valdymo grupei tikrinti ir tvirtinti. Visais PU atvejais kontaktinio centro funkcijas atlieka ES arba ŠK aptarnavimo centras, priklausomai nuo to, kuri Šalis pateikė užklausą. Šis aptarnavimo centras bus atsakingas už užklauso registravimą ir tinkamo nuodugnumo analizę.

Galimos pakeitimų užklausų priežastys:

- incidentas, dėl kurio atsirado pakeitimo poreikis;
- esama problema, dėl kurios reikalingas pakeitimas;
- galutinio naudotojo užklausa dėl naujo pakeitimo;
- pakeitimas atsiranda dėl nuolatinės techninės priežiūros;
- teisės aktų pakeitimai.

7.2. Pakeitimų 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 PU įgyvendinimas yra aktualus ir ES, ir ŠK, pakeitimo užklausa užregistravusi Šalis pakeitimo įvertinimą ir planą patikrina su kita Šalimi.

7.3. Pakeitimo patvirtinimas

Visos užregistruotos pakeitimų užklauskos turi būti patvirtintos atitinkamo sprendimų lygmens.

7.4. Pakeitimų įgyvendinimas

Pakeitimai įgyvendinami versijų valdymo proceso metu. Abiejų Šalių versijų valdymo grupės vykdo savo procesus, apimančius planavimą ir testavimą. Pakeitimų peržiūra vykdoma pabaigus įgyvendinimą. Siekiant užtikrinti, kad viskas būtų daroma pagal planą, esamas pakeitimų valdymo procesas yra nuolat peržiūrimas ir prireikus atnaujinamas.

8. Versijų valdymas

Versija – tai vienas ar keli į vieną versijos planą įtraukti IT paslaugos pakeitimai, dėl kurių turės būti gautas leidimas, kurie turės būti parengti, sudėti į visumą, ištestuoti ir įdiegti visi kartu. Versijos paskirtis gali būti ištaisyti klaidą, atlikti aparatinės įrangos ar kitų komponentų pakeitimus, atlikti programinės įrangos pakeitimus, atnaujinti taikomosios programos versijas, atlikti dokumentacijos ir (arba) procesų pakeitimus. Kiekvienos versijos turinys yra valdomas, testuojamas ir diegiamas kaip vienas vienetas.

Versijos planavimo paskirtis – suplanuoti, sudėti į visumą, ištestuoti ir patvirtinti bei parengti 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 bei pateikti versijų valdymo grupėms.

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

8.1. Versijos planavimas

Pirmuoju šio proceso žingsnio metu pakeitimai, dėl kurių gautas leidimas, priskiriami versijų paketams, apibrėžiama versijų apimtis ir turinys. Remdamasis šia informacija, Versijų planavimo padalinys parengia versijos sukūrimo, 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;
- parengimo ir diegimo strategiją;
- versijai sudaryti ir diegti jai 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

Versijų valdymo proceso versijos kūrimo ir testavimo žingsnio metu prieš pakeitimo rengimą nustatomas versijos ar versijos paketo kūrimo metodas, kontroliuojamos aplinkos palaikymo metodas, taip pat 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:

- kaip ir kada bus parengti versijos moduliai ir paslaugos komponentai;
- kokie yra tipiniai vykdymo terminai; kas nutiks, jei bus vėluojama;
- kaip sekti vykdymo pažangą ir gauti patvirtinimą;
- stebėsenos parametrai ir parametrai, pagal kuriuos bus nustatoma, ar versija įdiegta sėkmingai;

- bendri svarbių funkcijų ir pakeitimų testavimo etapai.

Šio paproceso pabaigoje visi reikalingi versijos komponentai yra parengti diegimo praktiškai realioje aplinkoje etapui.

8.3. Pasirengimas diegimui

Pasirengimo paproceso metu 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 kad dėl jų būtų gauti reikiami patvirtinimai.

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

- pakeitimo užklausos įrašo, kuriuo nustatomas diegimo tvarkaraštis ir pasirengiama diegimui darbinėje aplinkoje, sukūrimą;
- įgyvendinimo plano sukūrimą;
- ankstesnės būklės atkūrimo metodą, kad tuo atveju, jei diegimas nepavyktų, būtų galima atkurti ankstesnę būseną;

- visoms reikiamoms Šalims siunčiamus pranešimus;
- leidimo diegti versiją gavimą iš atitinkamo sprendimų lygmens.

8.4. Ankstesnės versijos atkūrimas

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

8.5. Versijos peržiūra ir užbaigimo procedūra

Atliekant diegimo peržiūrą, reikėtų atlikti šiuos veiksmus:

- surinkti grįžtamąjį ryšį apie tai, ar atlikus diegimo darbus patenkinti vartotojų, naudotojų lūkesčiai ir lūkesčiai dėl paslaugos teikimo (surinkti grįžtamąjį ryšį ir jį išnagrinėti, kad paslaugą būtų galima nuolat tobulinti);
- peržiūrėti visus neįvykdytus kokybės kriterijus;
- patikrinti, ar visi veiksmai, būtini pataisymai ir pakeitimai yra pabaigti;

- įsitikinti, kad diegimo pabaigoje neliko jokių pajėgumų, išteklių, gebėjimų ar 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 grupėms, jeigu dėl versijos padidėtų darbo apimtys);
- atnaujinti pagalbines dokumentacijas (t. y. techninės informacijos dokumentus);
- oficialiai perduoti įdiegtą versiją aptarnavimo operacijų specialistams;
- dokumentuoti įgytą patirtį;
- iš įgyvendinimo grupių gauti versijos santraukos dokumentą;
- patikrinti pakeitimo užklausoje įrašą ir oficialiai atlikti versijos užbaigimą.

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 ar galimus konfidencialumo, neskelbtinos informacijos išteklių prieinamumo ar 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 ar prieinamumo pažeidimus.

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

9.2. Informacijos saugumo incidentų tvarkymas

Atsakomybė už saugumo incidentus yra priskirta 3-iajam sprendimų lygmeniui; incidentus sprendžia speciali incidentų valdymo grupė (IVG).

IVG atsakinga už tai, kad būtų:

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

Informacijos saugumo valdymo proceso metu visa informacija apie incidentus klasifikuojama aukščiausiu informacijos slaptumo lygmeniu, tačiau bet kuriuo atveju ne žemesniu negu „ETS SENSITIVE“ (neskelbtina) lygmeniu.

Jeigu tyrimas dar vykdomas ir (arba) silpnoji vieta dar nėra pašalinta ir ja gali būti pasinaudota, iki spragos ištaisymo informacija priskiriama kategorijai „ETS CRITICAL“ (ypatingos svarbos).

9.3. Saugumo incidentų nustatymas

Atsižvelgdamas į saugumo įvykio pobūdį, informacijos saugumo specialistas nustato, kokias organizacijas įtraukti į IVG.

9.4. Saugumo incidentų analizė

IVG susisiečia su visomis įtrauktomis organizacijomis ir atitinkamais savo grupių nariais, kad incidentas būtų peržiūrėtas. Atliekant analizę nustatomas išteklių konfidencialumo, vientisumo ar prieinamumo praradimo mastas ir įvertinami padariniai visoms paveiktoms organizacijoms. Paskui apibrėžiami pradiniai ir tolesni incidento sprendimo ir jo poveikio valdymo veiksmai, įskaitant šiems veiksams atlikti reikalingus išteklius.

9.5. Saugumo incidento rimtumo įvertinimas, perdavimas spręsti kitam sprendimų lygmeniui ir ataskaitų teikimas

IVG įvertina kiekvieno naujo saugumo incidento rimtumą nustatydamą jo, kaip saugumo incidento, bruožus ir, atsižvelgdama į incidento rimtumą, nedelsdama imasi reikiamų veiksmų.

9.6. Ataskaitų apie reagavimą į saugumo incidentą teikimas

IVG įtraukia incidento sustabdymo ir padėties atkūrimo 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 padėties atkūrimo rezultatus ir:

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

Siekiant užtikrinti informacijos registravimo ir komunikacijos nuoseklumą, taip pat tam, kad būtų galima skubiai imtis reikiamų veiksmų incidentui sustabdyti, IVG turėtų į reagavimo į informacijos saugumo incidentą ataskaitą saugiai įtraukti atitinkamus duomenis. IVG laiku pateikia parengtą reagavimo į informacijos saugumo incidentą ataskaitą.

9.7. Stebėseną, gebėjimų stiprinimas ir nuolatinis tobulinimas

IVG visų saugumo incidentų ataskaitas pateikia 3-iojo sprendimų lygmens specialistams. Šiuo sprendimų lygmeniu ataskaitos analizuojamos ir 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 skaičių ateityje ir kuo labiau sumažinti incidentų 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 laikino sprendimo saugumo reikalavimai, be techninių komponentų, įskaitant jų projektavimą ir testavimą (žr. STS), būtina atlikti toliau nurodytas bendras procedūras.

10.1. Informacijos slaptumo nustatymas

Informacijos slaptumas įvertinamas nustatčius, kokį poveikį verslui gali padaryti su šia informacija susijęs saugumo pažeidimas (pvz., finansiniai nuostoliai, įvaizdžio pablogėjimas, teisės pažeidimas ir pan.).

Neskelbtinos informacijos ištekčiai nustatomi pagal jų poveikį susiejimui.

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

10.2. Informacijos išteklių slaptumo lygiai

Nustačius informacijos išteklių, jis priskiriamas tam tikrai kategorijai, laikantis šių taisyklių:

- jeigu informacijos konfidencialumo, vientisumo ar prieinamumo lygis įvertinamas kaip „aukštas“, informacijos išteklius priskiriamas kategorijai „ETS CRITICAL“ (ypatingos svarbos);
- jeigu informacijos konfidencialumo, vientisumo ar prieinamumo lygis įvertinamas kaip „vidutinis“, informacijos išteklius priskiriamas kategorijai „ETS SENSITIVE“ (neskelbtina);
- jeigu informacijos konfidencialumo, vientisumo ar prieinamumo lygis įvertinamas tik kaip „žemas“, informacijos išteklius priskiriamas kategorijai „ETS LIMITED“ (riboto naudojimo).

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 bendrą išteklių sąrašą. ATLPS informacijos ištekliai, kurie nepriklauso ESSŽ ir SSTL jungčiai, turėtų būti įtraukti į atitinkamos Šalies tvarkomą išteklių sąrašą.

Abi 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) išteklių (-ių) vertę. Dėl atsakingo asmens atsakomybės už išteklių (-ius) ir pareigos užtikrinti reikalingą konfidencialumo, vientisumo ir prieinamumo lygį turėtų būti susitarta ir susitarimas turi būti įformintas.

10.4. Neskelbtinos informacijos registravimas

Visa neskelbtina informacija registruojama neskelbtinos informacijos sąrašė (NIS).

Jeigu reikia, atsižvelgiama į neskelbtinos informacijos grupę, kuri gali lemti didesnę poveikį negu pavienė informacija, 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 ar padariniai gali keistis ir tai gali nebūti pastebėta, o į registro sistemų darbą gali būti įtraukiami nauji ištekliai.

Todėl NIS yra peržiūrimas reguliariai ir visa nauja informacija, kuri yra laikoma neskelbtina, nedelsiant įtraukiama į NIS.

Kiekvieną NIS įrašą sudaro bent ši informacija:

- informacijos aprašymas;
- informacijos savininkas;
- slaptumo lygis;
- pastaba, ar informacija apima asmens duomenis;
- jeigu reikalinga, papildoma informacija.

10.5. Neskelbtinos informacijos tvarkymas

Jeigu neskelbtina informacija yra tvarkoma ne Sąjungos registro ir Šveicarijos registro jungtyje, ji tvarkoma pagal tvarkymo instrukcijas.

Sąjungos registro ir Šveicarijos registro jungtyje informacija tvarkoma pagal Šalių saugumo reikalavimus.

10.6. Prieigos valdymas

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

Naudodamosi laikinu sprendimu ir vykdydamos operacijas pagal jį abi Šalys turi turėti prieigą prie šių komponentų:

- vikio – bendradarbiavimo aplinkos, kurioje keičiamasi bendra informacija, pavyzdžiui, versijų išleidimo planais;
- IT paslaugų valdymo (ITPV) 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 arba rakto valdymas

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

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

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

Visokia sertifikatų arba raktų patikra tarp Šalių atliekama naudojantis atskiru duomenų perdavimo kanalu.
