EUROOPA
KOMISJON

Brüssel, 20.3.2024
COM(2024) 125 final

ANNEX

LISA

järgmise dokumendi juurde:

Ettepanek: nõukogu otsus

Euroopa Liidu nimel võetava seisukoha kohta Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepinguga asutatud ühiskomitees seoses lepingu II lisa, ühiste töömenetluste ja ühenduse tehniliste standardite muutmisega

EUROOPA LIIDU JA ŠVEITSI KONFÖDERATSIOONI VAHELISE KASVUHOONEGAASIDE HEITKOGUSTEGA KAUPLEMISE SÜSTEEMIDE SIDUMISE LEPINGUGA ASUTATUD ÜHISKOMITEE OTSUS nr 1/2024, [...],
kokkuleppe II lisa, ühiste töömenetluste ja ühenduse tehniliste standardite muutmise kohta

ÜHISKOMITEE,

võttes arvesse Euroopa Liidu ja Šveitsi Konföderatsiooni vahelist kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingut (edaspidi „leping“),[1] eriti selle artiklit 9 ja artikli 13 lõiget 2,

ning arvestades järgmist:

(1) Ühiskomitee otsusega nr 2/2019[2] nähti ette ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamise ajutine lahendus.

(2) Oma kolmandal koosolekul nõustus ühiskomitee vajadusega analüüsida liidu registri ja Šveitsi registri vahelise alalise ühenduse kulutasuvust.

(3) Ühiskomitee leppis oma viiendal koosolekul kokku aruandes, mille esitas ühiskomitee otsustega 1/2020[3] ja 2/2020[4] loodud töörühm ning milles töörühm analüüsis ja soovitas lähenemisviisi liidu registri ja Šveitsi registri vahelise alalise ühenduse töölerakendamiseks.

(4) Selleks et kajastada liidu registri ja Šveitsi registri vahelise alalise ühenduse tehnilisi nõudeid ning ühtlustada lepingu II lisa sätteid tehnika arengut silmas pidades, tuleks lepingu II lisa muuta.

(5) Selleks et tagada ühiste töömenetluste ja ühenduse tehniliste standardite sidusus lepingu II lisaga, tuleks neid dokumente muuta,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

1. Lepingu II lisa asendatakse käesoleva otsuse lisaga.

2. Lepingu artikli 3 lõikes 6 osutatud ühised töömenetlused on esitatud käesoleva otsuse II lisas.

3. Lepingu artikli 3 lõikes 7 osutatud ühenduse tehniliste standardid on esitatud käesoleva otsuse III lisas.

Artikkel 2

Käesolev otsus jõustub selle vastuvõtmise päeval.

Koostatud inglise keeles [Brüsselis] [Bernis] [xx 2024].

[1] ELT L 322, 7.12.2017, lk 3.
[2] ELT L 314, 29.9.2020, lk 68.
[3] ELT L 226, 25.6.2021, lk 2.
[4] ELT L 226, 25.6.2021, lk 16.

Ühiskomitee nimel

Euroopa Liidu määratud sekretär	*esimees*	*Šveitsi määratud sekretär*

I LISA

„II LISA

ÜHENDUSE TEHNILISED STANDARDID

Selleks et rakendada tööle ELi HKSi ja Šveitsi HKSi vaheline ühendus, võeti 2020. aastal kasutusele ajutine lahendus. Alates 2023. aastast muutub kõnealuse kahe heitkogustega kauplemise süsteemi vaheline registriühendus järk-järgult alaliseks registriühenduseks, mis eelduste kohaselt rakendatakse tööle hiljemalt 2024. aastal ning mis võimaldab ühendatud turgudel toimida ja saada kasu turu likviidsusest ning teha tehinguid kahe ühendatud süsteemi vahel viisil, mis on samaväärne kahest süsteemist koosneva turuga ja võimaldab turuosalistel tegutseda nii, nagu nad oleksid ühel turul, tingimusel et lepinguosaliste üksikud õigusnormid on täidetud. Ühenduse tehnilised standardid hõlmavad järgmist:

– sideühenduse arhitektuur;

– Šveitsi täiendava tehingulogi (ŠTTL) ja Euroopa Liidu tehingulogi (ELTL) vaheline teabevahetus;

– andmeedastuse turvalisus;

– funktsioonide loetelu (tehingud, kooskõlastav võrdlemine …);

– transpordikihi määratlus;

– andmete logisse salvestamise nõuded;

– operatiivne töökorraldus (kõnekeskus, kasutajatugi);

– andmeside käivitamise kava ja testimine;

– turvatestimine.

Ühenduse tehnilistes standardites nähakse ette, et haldajad võtavad kõik mõistlikud meetmed, et tagada Šveitsi tehingulogi, ELi tehingulogi ja süsteemidevahelise ühenduse pidev töö 24 tundi ööpäevas ja 7 päeva nädalas minimaalsete katkestustega kummaski tehingulogis ja süsteemidevahelises ühenduses.

Ühenduse tehnilistes standardites nähakse ette Šveitsi registri, Šveitsi tehingulogi, liidu registri ja ELi tehingulogi täiendavad turvanõuded, mis dokumenteeritakse turbekavas. Eelkõige täpsustatakse ühenduse tehnilistes standardites järgmist:

– kui tekib kahtlus, et Šveitsi registri, Šveitsi tehingulogi, liidu registri ja ELi tehingulogi turvalisus on ohus, teavitavad lepinguosalised viivitamata teineteist ning peatavad Šveitsi tehingulogi ja ELi tehingulogi vahelise ühenduse;

– turvarikkumise korral kohustuvad lepinguosalised jagama viivitamata teineteisele teavet. Teadaolevaid tehnilisi üksikasju sisaldav aruanne juhtumi kohta (kuupäev, juhtumi põhjus, mõju, meetmed) edastatakse nii Šveitsi registri haldajale kui ka liidu registri põhihaldajale 24 tunni jooksul pärast seda, kui turvaintsident on tunnistatud turvarikkumiseks.

Ühenduse tehnilistes standardites ette nähtud turvatestimine peab olema lõpetatud enne Šveitsi tehingulogi ja ELi tehingulogi vahelise sideühenduse loomist ja iga kord, kui hakkab tööle Šveitsi tehingulogi või ELi tehingulogi uus versioon või väljalase.

Ühenduse tehnilistes standardites tuleb lisaks tootmiskeskkonnale näha ette kaks testimiskeskkonda: arendaja testimiskeskkond ja heakskiitmiskeskkond.

Lepinguosalised peavad Šveitsi registri haldaja ja liidu registri põhihaldaja kaudu esitama tõendid, et viimase 12 kuu jooksul on tehtud nende süsteemide turvalisuse sõltumatu hindamine vastavalt ühenduse tehnilistes standardites ette nähtud turvanõuetele. Turvatestimine, eelkõige läbistustestimine tehakse kõikide tarkvara uute suuremate väljalasetega vastavalt ühenduse tehnilistes standardites sätestatud turvanõuetele. Läbistustestimist ei tohi teha tarkvaraarendaja ega tema alltöövõtja.“

II LISA

ÜHISED TÖÖMENETLUSED

vastavalt Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingu artikli 3 lõikele 6

Alalise registriühenduse menetlused

Sisukord

1. Sõnastik....8
2. Sissejuhatus....10
2.1. Kohaldamisala....10
2.2. Adressaadid....11
3. Lähenemisviis ja standardid....11
4. Intsidendihaldus....11
4.1. Intsidendi identiftseerimine ja registreerimine....12
4.2. Klassifitseerimine ja esmane tugi....12
4.3. Intsidendi uurimine ja diagnoosimine....12
4.4. Intsidendi lahendamine ja teenuse taastamine....13
4.5. Intsidendi sulgemine....13
5. Probleemihaldus....14
5.1. Probleemi identifitseerimine ja registreerimine....14
5.2. Probleemi prioriseerimine....14
5.3. Probleemi uurimine ja diagnoosimine....14
5.4. Lahenduse leidmine....14
5.5. Probleemi sulgemine....14
6. Teenindussoovi täitmine....14
6.1. Teenindussoovi algatamine....15
6.2. Teenindussoovi registreerimine ja analüüsimine....15
6.3. Teenindussoovi heakskiitmine....15
6.4. Teenindussoovi täitmine....15
6.5. Teenindussoovi eskaleerimine....15
6.6. Teenindussoovi täitmise läbivaatamine....15
6.7. Teenindussoovi sulgemine....15
7. Muudatuste juhtimine....17
7.1. Muudatuse taotlus....17

7.2. Muudatuse hindamine ja planeerimine 17
7.3. Muudatuse heakskiitmine 17
7.4. Muudatuse teostamine 17
8. Väljalaskehaldus 17
8.1. Väljalaske planeerimine 18
8.2. Väljalaskepaketi loomine ja testimine 18
8.3. Juurutamise ettevalmistamine 18
8.4. Väljalaske tagasipööramine 19
8.5. Väljalaske hindamine ja sulgemine 19
9. Turvaintsidendi haldus 19
9.1. Turvaintsidendi kategoriseerimine 19
9.2. Turvaintsidendi käsitlemine 20
9.3. Turvaintsidendi identifitseerimine 20
9.4. Turvaintsidendi analüüs 20
9.5. Turvaintsidendi tõsiduse hindamine, intsidendi eskaleerimine ja aruandlus 20
9.6. Turvaintsidendi lahenduse aruanne 20
9.7. Järelevalve, suutlikkuse suurendamine ja pidev täiustamine 21
10. Infoturbe haldus 21
10.1. Tundliku teabe identifitseerimine 21
10.2. Teabevarade tundlikkustasemed 21
10.3. Teabevara omaniku määramine 21
10.4. Tundliku teabe registreerimine 22
10.5. Tundliku teabe käitlemine 22
10.6. Juurdepääsu haldamine 22
10.7. Sertifikaadi-/võtmehaldus 23

1. SÕNASTIK

Tabel 1-1. Akronüümid ja mõisted

Akronüüm/termin	Määratlus
Sertifitseerimisasutus	elektroonilisi sertifikaate väljastav üksus
CH	Šveitsi Konföderatsioon

HKS	heitkogustega kauplemise süsteem
EL	Euroopa Liit
IHR	intsidendihaldusrühm
Teabevara	teave, mis on ettevõttele või organisatsioonile väärtuslik
IT	infotehnoloogia
ITIA	infotehnoloogia infrastruktuuri andmik
ITTH	IT-teenuste haldus
ÜTS	ühenduse tehnilised standardid
Register	riist- või tarkvara poolt genereeritud ja jälgitav perioodiline signaal, mis annab märku tavapärasest tööst või sünkroniseerib arvutisüsteemi muud osad.
MT	muudatuse taotlus
TTL	tundliku teabe loetelu
TT	teenusetaotlus
Viki	veebisait, mille abil kasutajad saavad vahetada teavet ja teadmisi sisu lisamise või kohandamisega otse veebilehitseja kaudu.

2. SISSEJUHATUS

Euroopa Liidu ja Šveitsi Konföderatsiooni vahel 23. novembril 2017 sõlmitud kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepinguga (edaspidi „leping“) on ette nähtud selliste lubatud heitkoguse ühikute (edaspidi „LHÜd“) vastastikune tunnustamine, mida saab kasutada kohustuste täitmiseks Euroopa Liidu heitkogustega kauplemise süsteemis (edaspidi „ELi HKS“) või Šveitsi heitkogustega kauplemise süsteemis (edaspidi „Šveitsi HKS“). ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks luuakse otseside liidu registri ELi tehingulogi ja Šveitsi registri täiendava tehingulogi vahel, mis võimaldab kummaski HKSis välja antud LHÜde ülekandmist ühest registrist teise (lepingu artikli 3 lõige 2). Selleks et rakendada tööle ELi HKSi ja Šveitsi HKSi vaheline ühendus, võeti 2020. aastal kasutusele ajutine lahendus. Alates 2023. aastast muutub kõnealuse kahe heitkogustega kauplemise süsteemi vaheline registriühendus järk-järgult alaliseks registriühenduseks, mis eelduste kohaselt rakendatakse tööle hiljemalt 2024. aastal ning mis võimaldab ühendatud turgudel toimida ja saada kasu turu likviidsusest ning teha tehinguid kahe ühendatud süsteemi vahel viisil, mis on samaväärne kahest süsteemist koosneva turuga ja võimaldab turuosalistel tegutseda nii, nagu nad oleksid ühel turul, tingimusel et lepinguosaliste üksikud õigusnormid on täidetud. (Lepingu II lisa).

Lepingu artikli 3 lõike 6 kohaselt peavad Šveitsi registri haldaja ja liidu registri põhihaldaja (lepingus „keskregistrihaldaja“) koostama ühised töömenetlused (lepingus „ühine tegevuskord“), mis on seotud ühenduse toimimiseks vajalike tehniliste ja muude aspektidega, võttes arvesse riigisisestes õigusaktides sätestatud prioriteete. Haldajate koostatud ühised töömenetlused jõustuvad ühiskomitee otsuse alusel.

Ühiskomitee võttis ühised töömenetlused vastu oma otsusega nr 1/2020. Käesolevas dokumendis esitatud ajakohastatud ühised töömenetlused võtab ühiskomitee vastu oma otsusega nr 1/2024. Kooskõlas käesoleva otsusega ja ühiskomitee taotlusel on Šveitsi registri haldaja ja liidu registri põhihaldaja välja töötanud registritevahelise ühenduse töölerakendamise edasised tehnilised suunised, mida ajakohastatakse veelgi, et tagada nende pidev kohandamine tehnika arenguga ning ühenduse ohutuse ja turvalisuse ning selle tõhusa ja tulemusliku toimimisega seotud uute nõuetega.

2.1. Kohaldamisala

Käesolev dokument kujutab endast lepinguosaliste ühist arusaama ELi HKSi registri ja Šveitsi HKSi registri vahelise ühenduse menetluslike aluste loomisest. Selles kirjeldatakse ühenduse toimimisega seotud üldisi menetlusnõudeid, aga ühenduse töölerakendamiseks on vaja täiendavaid tehnilisi suuniseid.

Ühenduse nõuetekohaseks toimimiseks on vaja tehnilist kirjeldust, et ühenduse töölerakendamisega edasi liikuda. Lepingu artikli 3 lõike 7 kohaselt käsitletakse neid küsimusi üksikasjalikult ühenduse tehnilistes standardites, mille ühiskomitee eraldi otsusega vastu võtab.

Ühiste töömenetluste eesmärk on tagada, et ELi HKSi registri ja Šveitsi HKSi registri vahelise ühenduse toimimisega seotud IT-teenuseid osutatakse tulemuslikult ja tõhusalt, eelkõige teenindussoovide täitmiseks, teenusetõrgete kõrvaldamiseks, probleemide lahendamiseks ning rutiinsete operatiivülesannete täitmiseks vastavalt IT-teenuste halduse rahvusvahelistele standarditele.

Alalise registriühenduse jaoks on vaja üksnes järgmisi ühiseid töömenetlusi, mis on esitatud käesolevas dokumendis:

- intsidendihaldus;
- probleemihaldus;
- teenindussoovi täitmine;
- muudatusehaldus;
- väljalaskehaldus;
- turvaintsidendi haldus;
- infoturbe haldus.

2.2. Adressaadid

Ühised töömenetlused on mõeldud ELi ja Šveitsi registri tugirühmadele.

3. LÄHENEMISVIIS JA STANDARDID

Kõigi ühiste töömenetluste suhtes kohaldatakse järgmisi põhimõtteid:

- EL ja Šveits lepivad kokku, et ühised töömenetlused määratakse kindlaks ITILi (infotehnoloogia infrastruktuuri andmik, versioon 4) alusel. Selle standardi kohaseid tavasid taaskasutatakse ja neid kohandatakse alalise registriühendusega seotud erivajadustele;
- ühiste töömenetluste rakendamiseks vajalik teabevahetus ja koordineerimine toimub Šveitsi ja ELi registrite kasutajatugede kaudu. Ülesanded määratakse alati ühe lepinguosalise siseselt;
- kui ühise töömenetluse suhtes tekib lahkarvamusi, analüüsitakse seda ja lahendatakse see mõlema kasutajatoe koostöös. Kui kokkuleppele ei jõuta, eskaleeritakse ühise lahenduse leidmine järgmisele tasemele.

Eskalatsioonitasemed	EL	CH
1. tase	ELi kasutajatugi	Šveitsi kasutajatugi
2. tase	ELi käitusjuht	Šveitsi registri rakendusjuht
3. tase	Ühiskomitee (kes võib sidumisepingu artikli 12 lõiget 5 arvesse võttes selle ülesande delegeerida)	
4. tase	Ühiskomitee, kui 3. tase delegeeritakse	

- kumbki lepinguosaline võib määrata kindlaks oma registrisüsteemi toimimise korra, võttes arvesse käesolevate ühiste töömenetlustega seotud nõudeid ja liideseid;
- ühiste töömenetluste, eelkõige intsidendihalduse, probleemihalduse ja teenindussoovide täitmise, ning lepinguosaliste suhtluse toetamiseks kasutatakse IT-teenuste haldusvahendit;
- lisaks on lubatud teabevahetus e-posti teel;
- mõlemad lepinguosalised tagavad, et infoturbenõudeid täidetakse vastavalt käitlemisjuhistele.

4. INTSIDENDIHALDUS

Intsidendihaldusprotsessi eesmärk on taastada pärast intsidenti IT-teenuste tavapärane tase võimalikult kiiresti ja selliselt, et äritegevuse katkestus oleks minimaalne.

Intsidendihalduse raames tuleks samuti pidada intsidentide registrit aruandluse jaoks ja seda tuleks lõimida muude protsessidega, et soodustada pidevat täiustamist.

Intsidendihaldus hõlmab üldjoontes järgmisi toiminguid:

- intsidendi identifitseerimine ja registreerimine;
- klassifitseerimine ja esmane tugi;
- uurimine ja diagnoosimine;
- lahendamine ja teenuse taastamine;
- intsidendi sulgemine.

Intsidendi kogu elutsükli jooksul vastutab intsidendihaldusprotsess pidevalt intsidendiga tegelejate määramise, intsidendi seire, jälgimise ja intsidendiga seotud teabevahetuse korraldamise eest.

4.1. Intsidendi identiftseerimine ja registreerimine

Intsidendi võib identiftseerida tugirühm, automaatsed seirevahendid või rutiinset järelevalvet teostav tehniline personal.

Kui intsident on identifitseeritud, tuleb see registreerida ja sellele tuleb määrata kordumatu tunnuskood, mis võimaldab intsidenti nõuetekohaselt jälgida ja seirata. Intsidendi kordumatu tunnuskood on identifikaator, mille ühises piletisüsteemis määrab intsidendi tõstatanud lepinguosalise (ELi või Šveitsi) kasutajatugi, ning seda tuleb kasutada selle intsidendiga seotud kogu teabevahetuses.

Kõigi intsidentide puhul peaks kontaktpunkt olema pileti registreerinud lepinguosalise kasutajatugi.

4.2. Klassifitseerimine ja esmane tugi

Intsidentide klassifitseerimise eesmärk on mõista ja kindlaks teha, milline süsteem ja/või teenus on intsidendist mõjutatud ja mil määral. Selleks et klassifitseerimine oleks tõhus, peaks see suunama intsidendi esimese katsega õige ressursi juurde, et kiirendada intsidendi lahendamist.

Klassifitseerimisetapis tuleks intsident liigitada ja prioriseerida vastavalt selle mõjule ja kiireloomulisusele, et seda saaks käsitleda vastavalt prioriteetsusest sõltuvale ajakavale.

Kui intsident võib mõjutada tundlike andmete konfidentsiaalsust või terviklust ja/või mõjutab süsteemi käideldavust, loetakse intsident ka turvaintsidendiks ja seda käsitletakse vastavalt käesoleva dokumendi peatükis „Turvaintsidentide haldus“ kirjeldatud protsessile.

Võimaluse korral teostab pileti registreerinud kasutajatugi esmase diagnoosimise. Selleks kontrollib kasutajatugi, kas intsident on teadaolev viga. Kui see on nii, siis on lahendustee või hädalahendus juba teada ja dokumenteeritud.

Kui kasutajatugi suudab intsidendi edukalt lahendada, sulgeb ta intsidendi selles etapis, kuna intsidendihalduse peamine eesmärk (st lõppkasutaja jaoks teenuse kiire taastamine) on täidetud. Kui see nii ei ole, eskaleerib kasutajatugi juhtumi edasiseks uurimiseks ja diagnoosimiseks asjakohasele lahendajate rühmale.

4.3. Intsidendi uurimine ja diagnoosimine

Intsidenti uuritakse ja diagnoositakse juhul, kui kasutajatugi ei suuda esialgse diagnoosimise käigus intsidenti lahendada ning see eskaleeritakse. Intsidendi eskaleerimine on uurimise ja diagnoosimise protsessi lahutamatu osa.

Uurimis- ja diagnoosimisetapis on tavapärane proovida intsidenti kontrollitud tingimustes uuesti esile kutsuda. Intsidendi uurimisel ja diagnoosimisel on oluline mõista intsidendini viinud sündmuste õiget järjekorda.

Eskaleerimine tähendab tõdemust, et intsidenti ei suudeta asjaomasel kasutajatoe tasandil lahendada ning see tuleb edastada kõrgema tasandi tugirühmale või teisele lepinguosalisele. Eskaleerimine võib toimuda kahel viisil: horisontaalselt (funktsionaalne) või vertikaalselt (hierarhiline).

Intsidendi registreerinud ja käivitanud kasutajatugi vastutab intsidendi eskaleerimise eest asjakohasele ressursile ning intsidendi üldise seisu ja sellega tegelejate määramise jälgimise eest.

Lepinguosaline, kellele intsident on määratud, vastutab taotletud tegevuste õigeaegse elluviimise ja oma kasutajatoele tagasiside andmise eest.

4.4. Intsidendi lahendamine ja teenuse taastamine

Intsidendi lahendamine ja teenuse taastamine toimub siis, kui intsidendist on täielikult aru saadud. Intsidendile lahenduse leidmine tähendab, et on kindlaks tehtud viis vea parandamiseks. Lahenduse kohaldamine on teenuse taastamise etapp.

Kui asjakohane ressurss on teenusetõrke kõrvaldanud, suunatakse intsident tagasi asjaomasele intsidendi registreerinud kasutajatoele, kes küsib intsidendi algatajalt kinnitust, et viga on parandatud ja intsidendi võib sulgeda. Intsidendi käsitlemisel tehtud järeldused tuleb dokumenteerida edaspidiseks kasutamiseks.

IT-toe töötajad võivad teenuse ise taastada või anda lõppkasutajale juhised, mille järgi teenus taastada.

4.5. Intsidendi sulgemine

Sulgemine on intsidendihaldusprotsessi viimane etapp ja see toimub varsti pärast intsidendi lahendamist.

Sulgemisetapi tegevuste kontrollnimekirjas pööratakse erilist tähelepanu järgmisele:

- intsidendile algselt määratud kategooria kontrollimine;
- intsidendiga seotud kogu teabe nõuetekohane registreerimine;
- intsidendi nõuetekohane dokumenteerimine ja teadmusbaasi ajakohastamine;
- kõigi intsidendist otseselt või kaudselt mõjutatud huvirühmade teavitamine.

Intsident on ametlikult suletud pärast seda, kui kasutajatugi on intsidendi sulgemise etapi lõpule viinud ja teatanud sellest teisele lepinguosalisele.

Kui intsident on suletud, ei avata seda uuesti. Kui intsident kordub lühikese aja jooksul, ei avata algset intsidenti uuesti, vaid registreeritakse uus intsident.

Kui intsidenti jälgivad nii ELi kui ka Šveitsi kasutajatoed, vastutab lõpliku sulgemise eest pileti registreerinud kasutajatugi.

5. PROBLEEMIHALDUS

Seda menetlust tuleks järgida alati, kui avastatakse probleem, mis käivitab probleemihaldusprotsessi. Probleemihalduses keskendutakse kvaliteedi parandamisele ja intsidentide arvu vähendamisele. Probleem võib olla ühe või mitme intsidendi põhjus. Kui teatatakse intsidendist, on intsidendihalduse eesmärk taastada teenus võimalikult kiiresti. See võib hõlmata hädalahenduste kasutamist. Probleemi registreerimise korral on eesmärk uurida probleemi algpõhjust, et teha kindlaks muudatus, mis tagab, et probleemi ja sellega seotud intsidente enam ei esine.

5.1. Probleemi identifitseerimine ja registreerimine

Sõltuvalt sellest, kumb lepinguosaline pileti lõi, on probleemidega seotud küsimustes kontaktpunktiks kas ELi või Šveitsi kasutajatugi.

Probleemi kordumatu tunnuskood on IT-teenuse haldusvahendi määratud identifikaator. Seda tuleb kasutada selle probleemiga seotud kogu teabevahetuses.

Probleemi registreerimiseks võib anda tõuke intsident või seda võidakse teha omaalgatuslikult, et lahendada süsteemis mis tahes ajahetkel avastatud probleemid.

5.2. Probleemi prioriseerimine

Probleeme võib nende jälgimise lihtsustamiseks liigitada vastavalt nende raskusastmele ja tähtsusele samamoodi nagu intsidente, võttes arvesse nendega seotud intsidentide mõju ja esinemise sagedust.

5.3. Probleemi uurimine ja diagnoosimine

Probleemi võib tõstatada kumbki lepinguosaline ning algatava lepinguosalise kasutajatugi vastutab selle registreerimise, asjakohasele ressursile määramise ja probleemi üldise seisu jälgimise eest.

Lahendajate rühm, kellele probleem eskaleeriti, vastutab probleemi õigeaegse lahendamise ja kasutajatoega suhtlemise eest.

Taotluse korral vastutavad mõlemad lepinguosalised määratud ülesannete täitmise tagamise ja oma kasutajatoele tagasiside andmise eest.

5.4. Lahenduse leidmine

Lahendajate rühm, kellele probleem on määratud, vastutab selle lahendamise ja oma kasutajatoele asjakohase teabe esitamise eest.

Probleemi käsitlemisel tehtud järeldused tuleb dokumenteerida edaspidiseks kasutamiseks.

5.5. Probleemi sulgemine

Probleem on ametlikult suletud siis, kui see on muudatuse teostamisega lahendatud. Probleemi sulgemise etapi teostab see kasutajatugi, kes probleemi registreeris ja teise lepinguosalise kasutajatuge teavitas.

6. TEENINDUSSOOVI TÄITMINE

Teenindussoovi täitmise protsess on uue või olemasoleva teenuse taotluse täielik haldamine alates selle registreerimisest ja heakskiitmisest kuni sulgemiseni. Teenindussoovid on tavaliselt väikesed, eelnevalt määratletud, korratavad, sagedased, eelnevalt heaks kiidetud ja menetluslikud taotlused.

Allpool on kirjeldatud põhietappe, mida tuleb järgida.

6.1. Teenindussoovi algatamine

Teenindussooviga seotud teave esitatakse ELi või Šveitsi kasutajatoele e-posti, telefoni või IT-teenuse haldusvahendi või mis tahes muu kokkulepitud sidekanali kaudu.

6.2. Teenindussoovi registreerimine ja analüüsimine

Kõigi teenindussoovide puhul peaks kontaktpunkt olema ELi või Šveitsi kasutajatugi, olenevalt sellest, milline lepinguosaline teenindussoovi esitas. Selle kasutajatoe ülesanne on teenindussoov registreerida ja seda hoolikalt analüüsida.

6.3. Teenindussoovi heakskiitmine

Teenindussoovi esitanud lepinguosalise kasutajatoe spetsialist kontrollib, kas on vaja teise lepinguosalise heakskiitu, ja vajaduse korral hangib selle. Kui teenindussoovi heaks ei kiideta, ajakohastab kasutajatugi piletit ja sulgeb selle.

6.4. Teenindussoovi täitmine

Selle etapiga tagatakse teenindussoovi tulemuslik ja tõhus käsitlemine. Eristada tuleb kahte järgmist juhtu:

- teenindussoovi täitmine puudutab ainult ühte lepinguosalist. Sel juhul annab kõnealune lepinguosaline välja töökäsud ja koordineerib nende täitmist;
- teenindussoovi täitmine puudutab nii ELi kui ka Šveitsi. Sel juhul annavad kasutajatoed töökäsud oma vastutusalas. Kasutajatoed koordineerivad teenindussoovi täitmist omavahel. Üldine vastutus lasub teenindussoovi vastu võtnud ja algatanud kasutajatoel.

Kui teenindussoov on täidetud, tuleb selle seisuks määrata „täidetud“.

6.5. Teenindussoovi eskaleerimine

Vajaduse korral saab kasutajatugi eskaleerida täitmata teenindussoovid asjakohasele ressursile (kolmandale isikule).

Eskaleeritakse vastavatele kolmandatele isikutele, st ELi kasutajatugi peab Šveitsi kolmandale isikule eskaleerimiseks võtma ühendust Šveitsi kasutajatoega ja vastupidi.

Kolmas isik, kellele teenindussoov eskaleeriti, vastutab teenindussoovi õigeaegse täitmise ja selle eskaleerinud kasutajatoega suhtlemise eest.

Teenindussoovi registreerinud kasutajatugi vastutab teenindussoovi üldise seisu ja sellega tegelejate määramise jälgimise eest.

6.6. Teenindussoovi täitmise läbivaatamine

Vastutav kasutajatugi esitab teenindussoovi kirje lõplikuks kvaliteedikontrolliks enne selle sulgemist. Eesmärk on tagada, et teenindussoovi on tõepoolest käsitletud ja et teenindussoovi elutsükli kirjeldamiseks vajalik teave on esitatud piisavalt üksikasjalikult. Lisaks tuleb teenindussoovi käsitlemisel tehtud järeldused dokumenteerida edaspidiseks kasutamiseks.

6.7. Teenindussoovi sulgemine

Kui teenindussoovi täitma määratud osalejad nõustuvad, et teenindussoov on täidetud, ja teenindussoovi esitaja leiab, et juhtum on lahendatud, määratakse järgmiseks seisuks „suletud“.

Teenindussoov on ametlikult suletud pärast seda, kui teenindussoovi registreerinud kasutajatugi on teenindussoovi sulgemise etapi lõpule viinud ja teatanud sellest teisele lepinguosalisele.

7. MUUDATUSTE JUHTIMINE

Eesmärk on tagada, et IT-taristu kontrollimiseks kasutatakse kõigi muudatuste tõhusaks ja kiireks käsitlemiseks standardmeetodeid ja -menetlusi, et minimeerida mis tahes seotud intsidentide arvu ja nende mõju teenusele. Muudatused IT-taristus võidakse teha probleemide lahendamise või väljastpoolt kehtestatud nõuete (nt muudetud õigusnormid) tulemusena või ennetavalt, püüdes suurendada tõhusust ja tulemuslikkust, või et võimaldada või kajastada ärialgatusi.

Muudatusehalduse protsess hõlmab eri etappe, mis registreerivad muudatuse taotluse iga üksikasja edasiseks jälgimiseks. Need protsessid tagavad, et muudatus valideeritakse ja seda testitakse enne selle juurutamist. Eduka juurutamise eest vastutab väljalaskehalduse protsess.

7.1. Muudatuse taotlus

Muudatuse taotlus (MT) esitatakse muudatusehalduse rühmale valideerimiseks ja heakskiitmiseks. Kõigi muudatuse taotluste puhul peaks kontaktpunkt olema ELi või Šveitsi kasutajatugi, olenevalt sellest, milline lepinguosaline muudatuse taotluse esitas. Selle kasutajatoe ülesanne on muudatuse taotlus registreerida ja seda hoolikalt analüüsida.

Muudatuse taotlused võivad pärineda

- muutust põhjustavast intsidendist;
- olemasolevast probleemist, mis toob kaasa muudatuse;
- lõppkasutajalt, kes taotleb uut muudatust;
- käimasolevast hooldusest tulenevast muudatusest;
- õigusnormide muudatustest.

7.2. Muudatuse hindamine ja planeerimine

Selles etapis käsitletakse muudatuse hindamist ja planeerimist. See hõlmab prioriteetide seadmist ja planeerimist, et minimeerida riske ja mõju.

Kui taotletud muudatuse teostamine mõjutab nii ELi kui ka Šveitsi, kontrollib muudatuse taotluse registreerinud lepinguosaline muudatuse hindamist ja planeerimist koos teise lepinguosalisega.

7.3. Muudatuse heakskiitmine

Iga registreeritud muudatustaotlus tuleb heaks kiita asjaomasel eskalatsioonitasemel.

7.4. Muudatuse teostamine

Muudatus teostatakse väljalaskehalduse protsessis. Mõlema lepinguosalise väljalaskehalduse rühmad järgivad oma protsesse, mis hõlmavad planeerimist ja testimist. Muudatuse hindamine toimub pärast selle teostamist. Plaanipärase teostamise tagamiseks vaadatakse olemasolevat muudatusehalduse protsessi pidevalt läbi ja vajaduse korral seda ajakohastatakse.

8. VÄLJALASKEHALDUS

Väljalaskega tehakse IT-teenuses üks või mitu muudatust, mis koondatakse väljalaskekavasse ja mis tuleb koos heaks kiita, ette valmistada ja luua ning mida tuleb koos testida ja juurutada. Väljalase võib hõlmata veaparandust, muudatust riistvaras või muudes komponentides, tarkvaramuudatusi, rakenduse uut versiooni, muudatusi dokumentatsioonis ja/või protsessides. Iga väljalaske sisu hallatakse, testitakse ja juurutatakse ühe üksusena.

Väljalaskehalduse eesmärk on planeerida, luua, testida, valideerida ja tarnida võimet osutada kavandatud teenuseid, et täita huvirühmade nõuded ja saavutada seatud eesmärgid. Kõigi teenuses tehtavate muudatuste vastuvõtukriteeriumid määratakse kindlaks ja dokumenteeritakse kavandamise koordineerimise käigus ning need esitatakse väljalaskehalduse rühmadele.

Väljalase koosneb tavaliselt veaparandustest ja teenuse täiustustest. See sisaldab uut või muudetud tarkvara ja mis tahes uut või muudetud riistvara, mida on vaja heakskiidetud muudatuste teostamiseks.

8.1. Väljalaske planeerimine

Protsessi esimeses etapis jaotatakse loa saanud muudatused väljalaskepakettide vahel ning määratakse kindlaks väljalasete ulatus ja sisu. Selle teabe põhjal koostatakse väljalaske planeerimise alamprotsessis väljalaske loomise, testimise ja juurutamise graafik.

Planeerimisel tuleks määrata kindlaks

- väljalaske ulatus ja sisu;
- väljalaske riskihinnang ja riskiprofiil;
- kliendid/kasutajad, keda väljalase mõjutab;
- väljalaske eest vastutav rühm;
- tarne- ja juurutamisstrateegia;
- väljalaske ja selle juurutamise jaoks vajalikud vahendid.

Mõlemad lepinguosalised teavitavad teineteist oma väljalaskeplaanist ja hooldusajast. Kui väljalase mõjutab nii ELi kui ka Šveitsi, koordineerivad nad planeerimist ja määravad ühise hooldusaja.

8.2. Väljalaskepaketi loomine ja testimine

Väljalaskehaldusprotsessi loomise ja testimise etapis määratakse lähenemisviis väljalaske või väljalaskepaketi rakendamiseks ja kontrollitud keskkondade säilitamiseks enne toodangversiooni muutmist, samuti kõigi muudatuste testimiseks kõigis välja lastud keskkondades.

Kui väljalase mõjutab nii ELi kui ka Šveitsi, koordineerivad nad tarneplaane ja määravad ühise hooldusaja. See hõlmab järgmisi aspekte:

- kuidas ja millal väljalaskeüksused ja teenuse komponendid tarnitakse;
- millised on tüüpilised üleminekuajad; mis juhtub hilinemise korral;
- kuidas jälgida tarne edenemist ja saada kinnitus;
- parameetrid väljalaske juurutamisega seotud jõupingutuste edukuse jälgimiseks ja kindlakstegemiseks;
- ühised testjuhtumid asjakohaste funktsioonide ja muudatuste jaoks.

Selle alamprotsessi lõpuks on kõik nõutavad väljalaskekomponendid valmis liikuma tootmiskeskkonnas juurutamise etappi.

8.3. Juurutamise ettevalmistamine

Ettevalmistamise alamprotsessiga tagatakse, et teavituskavad on õigesti koostatud ja teated on valmis saatmiseks kõigile mõjutatud huvirühmadele ja lõppkasutajatele, ning et väljalase on lõimitud muudatusehalduse protsessiga, tagamaks, et kõik muudatused tehakse kontrollitud viisil ja et neil on nõutud üksuste heakskiit.

Kui väljalase mõjutab nii ELi kui ka Šveitsi, koordineerivad nad järgmisi tegevusi:

- muudatuse taotluse registreerimine tootmiskeskkonnas juurutamise ajastamiseks ja ettevalmistamiseks;
- teostusplaani loomine;
- tagasipööramiskava, et juurutamise ebaõnnestumise korral saaks eelmise oleku taastada;
- kõigile vajalikele osalistele teadete saatmine;
- asjakohaselt eskalatsioonitasemelt väljalaske rakendamiseks heakskiidu saamine.

8.4. Väljalaske tagasipööramine

Kui juurutamine ebaõnnestub või kui testimise käigus tehakse kindlaks, et juurutamine ei olnud edukas või ei vastanud kokkulepitud vastuvõtu-/kvaliteedikriteeriumidele, peavad mõlema lepinguosalise väljalaskehalduse rühmad pöörduma tagasi eelmise oleku juurde. Teavitada tuleb kõiki vajalikke huvirühmi, sealhulgas mõjutatud või sihtrühmaks olevaid lõppkasutajaid. Kuni heakskiidu saamiseni saab protsessi uuesti alustada mis tahes eelnevas etapis.

8.5. Väljalaske hindamine ja sulgemine

Väljalaske hindamise käigus tuleks teha järgmist:

- koguda tagasisidet selle kohta, milline on klientide ja kasutajate rahulolu väljalaske juurutamise ja teenuse osutamisega (arvestada saadud tagasisidet teenuse pidevaks täiustamiseks);
- vaadata läbi kvaliteedikriteeriumid, mida ei täidetud;
- kontrollida, et kõik toimingud, vajalikud parandused ja muudatused on teostatud;
- veenduda, et pärast juurutamist ei ole mingeid võimekuse, ressursside, suutlikkuse või tulemuslikkusega seotud probleeme;
- kontrollida, et kõik probleemid, teadaolevad vead ja hädalahendused on dokumenteeritud ning kliendi, lõppkasutaja, operatiivtoe ja teiste mõjutatud poolte jaoks vastuvõetavad;
- jälgida väljalaskest põhjustatud intsidente ja probleeme (pakkuda operatiivrühmadele sissetöötamistuge, kui väljalase on suurendanud töömahtu);
- ajakohastada tugidokumente (st tehnilise teabe dokumente);
- anda väljalaske juurutamine ametlikult üle teenuse käitusele;
- dokumenteerida saadud õppetunnid;
- koguda rakendusrühmadelt väljalaske kokkuvõtte dokumendid;
- sulgeda väljalase ametlikult pärast muudatuse taotluse kirje kontrollimist.

9. TURVAINTSIDENDI HALDUS

Turvaintsidentide haldus kujutab endast turvaintsidentide käsitlemise protsessi, mis võimaldab intsidendist potentsiaalselt mõjutatud huvirühmi teavitada; intsidenti hinnata ja prioriseerida ning intsidendile reageerida, et lahendada tundlike teabevarade konfidentsiaalsuse, käideldavuse või terviklusega seotud tegelik, kahtlustatav või võimalik rikkumine.

9.1. Turvaintsidendi kategoriseerimine

Kõiki liidu registri ja Šveitsi registri vahelist seost mõjutavaid intsidente analüüsitakse, et teha kindlaks tundliku teabe loetellu (TTL) kantud mis tahes tundliku teabe konfidentsiaalsuse, tervikluse või käideldavuse võimalik rikkumine.

Rikkumise korral kirjeldatakse intsidenti kui turvaintsidenti, mis registreeritakse viivitamata IT-teenuse haldusvahendis ja mida hallatakse sellisena.

9.2. Turvaintsidendi käsitlemine

Turvaintsidentide eest vastutab kolmas eskalatsioonitase ja intsidentide lahendamisega tegeleb spetsiaalne intsidendihaldusrühm (IHR).

IHRi ülesanded on järgmised:

- teha esimene analüüs, kategoriseerida intsident ja hinnata selle tõsidust;
- koordineerida kõigi huvirühmade tegevust, sealhulgas dokumenteerida täielikult intsidendi analüüs, intsidendi lahendamiseks tehtud otsused ja leitud võimalikud puudused;
- eskaleerida turvaintsident sõltuvalt selle tõsidusest aegsasti asjakohasele tasemele teabe saamiseks või otsuse tegemiseks.

Infoturbe haldamise protsessis klassifitseeritakse kogu intsidentidega seotud teave kõige kõrgemale tundlikkustasemele, kuid mitte madalamale kui „SENSITIVE: *ETS*“.

Käimasoleva uurimise ja/või puuduse korral, mida võidakse ära kasutada, ja kuni selle parandamiseni on teabe märgistus „SPECIAL HANDLING: *ETS Critical*“.

9.3. Turvaintsidendi identifitseerimine

Infoturbeametnik määrab turvasündmuse liigi põhjal kindlaks asjakohased organisatsioonid, kes kaasatakse ja kes hakkavad kuuluma IHRi.

9.4. Turvaintsidendi analüüs

IHR teeb vastavalt vajadusele koostööd kõigi kaasatud organisatsioonide ja nende vastavate rühmade asjaomaste liikmetega, et intsidenti hinnata. Analüüsi käigus tehakse kindlaks vara konfidentsiaalsuse, tervikluse või käideldavuse vähenemise ulatus ning hinnatakse tagajärgi kõigile mõjutatud organisatsioonidele. Seejärel määratakse kindlaks esialgsed ja järelmeetmed intsidendi lahendamiseks ja selle mõju ohjamiseks, sealhulgas nende meetmete mõju ressurssidele.

9.5. Turvaintsidendi tõsiduse hindamine, intsidendi eskaleerimine ja aruandlus

IHR hindab uue turvaintsidendi tõsidust pärast selle kirjeldamist turvaintsidendina ja alustab kohe nõuetekohast tegevust vastavalt intsidendi tõsidusele.

9.6. Turvaintsidendi lahenduse aruanne

IHR lisab turvaintsidendi lahendamise aruandesse intsidendi ohjeldamise ja sellest taastumise tulemused. Aruanne esitatakse kolmandale eskalatsioonitasemele turvatud e-kirja teel või muude mõlemapoolselt tunnustatud turvaliste sidevahendite abil.

Vastutav lepinguosaline vaatab intsidendi ohjeldamise ja sellest taastumise tulemused läbi ning

- taasühendab registri eelneva lahtiühendamise korral;
- annab registri meeskondadele intsidendi kohta teavet;
- sulgeb intsidendi.

IHR peaks turvalisel viisil lisama turvaintsidendi aruandesse asjakohased üksikasjad, et tagada järjepidev dokumenteerimine ja teabevahetus ning võimaldada kiireid ja sobivaid meetmeid intsidendi ohjeldamiseks. Pärast intsidendi lahendamist esitab IHR õigeaegselt turvaintsidendi lõpparuande.

9.7. Järelevalve, suutlikkuse suurendamine ja pidev täiustamine

IHR esitab aruande kõigi turvaintsidentide kohta kolmandale eskalatsioonitasemele. See eskalatsioonitase kasutab aruandeid selleks, et teha kindlaks järgmine:

- nõrgad kohad turvakontrollis ja/või käituses, mida tuleb parandada;
- võimalik vajadus seda menetlust tõhustada, et suurendada tulemuslikkust intsidentide lahendamisel;
- koolitus- ja suutlikkuse suurendamise võimalused, et veelgi suurendada registrisüsteemide infoturbealast vastupidavust, vähendada uute intsidentide ohtu ja minimeerida nende mõju.

10. INFOTURBE HALDUS

Infoturbe halduse eesmärk on tagada organisatsiooni salastatud teabe, andmete ja IT-teenuste konfidentsiaalsus, terviklus ja käideldavus. Lisaks tehnilistele komponentidele, sealhulgas nende kavandamisele ja testimisele (vt ühenduse tehnilised standardid), on alalise registriühenduse turvanõuete täitmiseks vaja järgmisi ühiseid töömenetlusi.

10.1. Tundliku teabe identifitseerimine

Konkreetse teabeüksuse tundlikkuse hindamiseks tehakse kindlaks selle teabega seotud turvarikkumise võimalik mõju ettevõttele (nt rahaline kahju, mainekahju, seaduse rikkumine jne).

Tundlik teabevara tehakse kindlaks selle põhjal, milline on asjaomase vara mõju registritevahelisele ühendusele.

Kõnealuse teabe tundlikkuse taset hinnatakse vastavalt kõnealuse ühenduse suhtes kohaldatavale tundlikkusskaalale, mida on kirjeldatud käesoleva dokumendi punktis „Turvaintsidendi käsitlemine“.

10.2. Teabevarade tundlikkustasemed

Teabevara liigitamisel kohaldatakse järgmisi reegleid:

- vähemalt ühe KÕRGE konfidentsiaalsus-, terviklus- või käideldavustaseme kindlakstegemise korral on vara märgistus „SPECIAL HANDLING: *ETS Critical*“;
- vähemalt ühe KESKMISE konfidentsiaalsus-, terviklus- või käideldavustaseme kindlakstegemise korral on vara märgistus „SENSITIVE: *ETS*“;
- üksnes MADALA konfidentsiaalsus-, terviklus- või käideldavustaseme kindlakstegemise korral on vara ELi märgistus „ SENSITIVE: *ETS Joint Procurement.“* CH märgistus: „LIMITED: ETS“.

10.3. Teabevara omaniku määramine

Kõigil teabevaradel peaks olema määratud omanik. HKSi teabevarad, mis kuuluvad ELi tehingulogi ja Šveitsi täiendava tehingulogi vahelisele ühendusele või on sellega seotud, tuleks lisada ühisesse varaloendisse, mida peavad mõlemad lepinguosalised. HKSi teabevarad, mis ei ole seotud ELi tehingulogi ja Šveitsi täiendava tehingulogi vahelise ühendusega, tuleks lisada varaloendisse, mida peab vastav lepinguosaline.

ELi tehingulogi ja Šveitsi täiendava tehingulogi vahelisele ühendusele kuuluva või sellega seotud teabevara omanik määratakse lepinguosaliste kokkuleppel. Teabevara omanik vastutab selle tundlikkuse hindamise eest.

Omanikul peaks olema piisavalt kõrge ametikoht, mis on vastavuses määratud vara(de) väärtusega. Tuleks kokku leppida ja ametlikult vormistada omaniku vastutus vara(de) eest ning tema kohustus säilitada nõutav konfidentsiaalsuse, tervikluse ja käideldavuse tase.

10.4. Tundliku teabe registreerimine

Kogu tundlik teave registreeritakse tundliku teabe loetelus.

Vajaduse korral võetakse arvesse tundliku teabe koondamist, millel võib olla suurem mõju kui ühel konkreetsel teabeüksusel eraldi, ning see registreeritakse tundliku teabe loetelus (nt süsteemi andmebaasis säilitatava teabe kogum).

Tundliku teabe loetelu ei ole muutumatu. Varadega seotud ohud, haavatavus, turvaintsidentide tõenäosus või tagajärjed võivad muutuda ootamatult ning registrisüsteemidesse võidakse lisada uusi varasid.

Seetõttu vaadatakse tundliku teabe loetelu korrapäraselt läbi ja kõik tundlikuks tunnistatud uued andmed registreeritakse selles viivitamata.

Tundliku teabe loetelu sisaldab iga kirje kohta vähemalt järgmist teavet:

- teabe kirjeldus;
- teabe omanik;
- tundlikkustase;
- märge selle kohta, kas teave sisaldab isikuandmeid;
- vajaduse korral lisateave.

10.5. Tundliku teabe käitlemine

Kui tundlikku teavet töödeldakse väljaspool liidu registri ja Šveitsi registri vahelist ühendust, käideldakse seda vastavalt käitlemisjuhistele.

Liidu registri ja Šveitsi registri vahelise ühenduse kaudu töödeldavat tundlikku teavet käideldakse vastavalt lepinguosaliste turvanõuetele.

10.6. Juurdepääsu haldamine

Juurdepääsuhalduse eesmärk on anda volitatud kasutajatele õigus teenust kasutada, vältides samal ajal volitamata kasutajate juurdepääsu. Juurdepääsuhaldust nimetatakse mõnikord ka „õiguste halduseks“ või „identiteedihalduseks“.

Alalise registriühenduse ja selle toimimise jaoks on mõlemal lepinguosalisel vaja juurdepääsu järgmistele komponentidele:

- Viki: koostöökeskkond ühise teabe vahetamiseks, näiteks väljalaske planeerimise kohta;
- IT-teenuste haldusvahend intsidendi- ja probleemihalduseks (vt peatükk 3 „Lähenemisviis ja standardid“);
- sõnumivahetussüsteem: kumbki lepinguosaline tagab tehinguandmeid sisaldavate sõnumite edastamiseks turvalise sõnumivahetussüsteemi.

Šveitsi registri haldaja ja liidu registri põhihaldaja tagavad, et juurdepääsuõigused on ajakohased, ning nad on oma osalistele kontaktpunktiks juurdepääsuhaldusega seotud küsimustes. Juurdepääsutaotlusi käsitletakse vastavalt teenindussoovi täitmise menetlustele.

10.7. Sertifikaadi-/võtmehaldus

Kumbki lepinguosaline vastutab oma sertifikaadi-/võtmehalduse eest (sertifikaatide/võtmete genereerimine, registreerimine, talletamine, paigaldamine, kasutamine, uuendamine, tühistamine, varundamine ja taastamine). Nagu on kirjeldatud ühenduse tehnilistes standardites (ÜTS), kasutatakse ainult selliseid digitaalseid sertifikaate, mille on väljastanud mõlema lepinguosalise poolt usaldusväärseks peetav sertifitseerimisasutus. Sertifikaatide/võtmete käitlemisel ja talletamisel tuleb järgida käitlemisjuhiseid.

Sertifikaatide ja võtmete tühistamist ja/või uuendamist koordineerivad mõlemad lepinguosalised. Seda tehakse vastavalt teenindussoovi täitmise menetlustele.

Šveitsi registri haldaja ja liidu registri põhihaldaja vahetavad sertifikaate/võtmeid turvaliste sidevahendite kaudu vastavalt käitlemisjuhistele.

Igasugune sertifikaatide/võtmete kontrollimine lepinguosaliste vahel toimub ribaväliselt.

III LISA

ÜHENDUSE TEHNILISED STANDARDID

vastavalt Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingu artikli 3 lõikele 7

Alalise registriühenduse standard

Sisukord

1. Sõnastik....26
2. Sissejuhatus....29
2.1. Kohaldamisala....29
2.2. Adressaadid....29
3. Üldsätted....30
3.1. Sideühenduse arhitektuur....30
3.1.1. Sõnumivahetus....30
3.1.2. XML-sõnum – üldkirjeldus....30
3.1.3. Valmendusaknad....30
3.1.4. Tehinguga seotud sõnumivood....31
3.2. Andmeedastuse turvalisus....33
3.2.1. Tulemüür ja võrguühendus....33
3.2.2. Virtuaalne privaatvõrk (VPN)....33
3.2.3. IPseci rakendamine....34
3.2.4. Turvaline sõnumivahetuse edastusprotokoll....34
3.2.5. XML-sisu krüptimine ja allkirjastamine....34
3.2.6. Krüptovõtmed....34
3.3. Registritevahelise ühendusega hõlmatud funktsioonide loetelu....34
3.3.1. Äritehingud....35
3.3.2. Kooskõlastava võrdlemise protokoll....35
3.3.3. Testsõnum....35
3.4. Andmesalvestusnõuded....36
3.5. Käitusnõuded....37
4. Käideldavusega seotud sätted....38
4.1. Andmeside käideldavuse projekteerimine....38
4.2. Initsialiseerimise ja side taasaktiveerimise testimisplaan....38
4.2.1. IKT-taristu sisetestid....39

4.2.2. Sidetestid....39
4.2.3. Kogu süsteemi testid (läbivtestimine) 39
4.2.4. Turvatestid 39
4.3. Heakskiitmis-/testimiskeskkond 40
5. Konfidentsiaalsuse ja terviklusega seotud sätted....40
5.1. Turvatestimistaristu 40
5.2. Ühenduse peatamise ja taasaktiveerimisega seotud sätted 41
5.3. Turvarikkumist käsitlevad sätted....41
5.4. Turvatestimise suunised....42
5.4.1. Tarkvara....42
5.4.2. Taristu....42
5.5. Riskihindamisega seotud sätted....42

1. SÕNASTIK

Tabel 1-1. Äritehingutega seotud akronüümid ja mõisted

Akronüüm/termin	Määratlus
Lubatud heitkoguse ühik (LHÜ)	kindlaksmääratud aja jooksul atmosfääri ühe tonni süsinikdioksiidi ekvivalentkoguse paiskamise õigus, mis kehtib üksnes mõlema lepingupoole nõuete täitmisel
CH	Šveitsi Konföderatsioon
CH-LHÜ	alalised saastekvoodid, mida nimetatakse ka CH-LHÜ2ks (vastavalt Kyoto protokolli 2. kohustusperioodile), mille on välja andnud Šveits
CH-LLHÜ	Šveitsi lennunduse LHÜ
ÜTM	ühised töömenetlused ühiselt välja töötatud menetlused ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks
HKR	heitkogustega kauplemise register
HKS	heitkogustega kauplemise süsteem
EL	Euroopa Liit
EL-LHÜ	ELi üldine LHÜ

Akronüüm/termin	Määratlus
EL-LLHÜ	ELi lennunduse LHÜ
ELKR	Euroopa Liidu konsolideeritud register
ELTL	Euroopa Liidu tehingulogi
Register	HKSi raames välja antud lubatud heitkoguse ühikute (LHÜd) arvestussüsteem, mille abil jälgitakse seda, kellele kuuluvad elektroonilistel kontodel hoitavad LHÜd
ŠTTL	Šveitsi täiendav tehingulogi
Tehing	registris aset leidev protsess, mille käigus kantakse LHÜ üle ühelt kontolt teisele
Tehingulogi süsteem	tehingulogi sisaldab andmeid iga ühelt registrilt teisele saadetud kavandatava tehingu kohta

Tabel 1-2. Tehnilised akronüümid ja mõisted

Akronüüm	Määratlus
Asümmeetriline krüptograafia	kasutab andmete krüptimiseks ja dekrüptimiseks avalikke ja privaatvõtmeid
Sertifitseerimisasutus	elektroonilisi sertifikaate väljastav üksus
Krüptovõti	teave, millega määratakse krüptoalgoritmi funktsionaalne väljund
Dekrüptimine	krüptimise pöördprotsess
Digiallkiri	matemaatiline meetod, mida kasutatakse sõnumi, tarkvara või digitaaldokumendi autentsuse ja tervikluse valideerimiseks
Krüpteerimine	teabe või andmete muundamine koodiks, eelkõige volitamata juurdepääsu vältimiseks
Faili valmendus	faili lugemise protsess
Tulemüür	võrguturbeseade või -tarkvara, mis jälgib ja kontrollib sissetulevat ja väljaminevat võrguliiklust eelnevalt kindlaksmääratud reeglite alusel
Südamelöökide seire	riist- või tarkvara poolt genereeritud ja jälgitav perioodiline signaal, mis annab märku tavapärasest tööst või sünkroniseerib arvutisüsteemi muud osad
IPSEC	IP SECurity, IP turve. Võrguprotokollistik, mis autendib ja krüptib andmepakette, et tagada turvaline krüptitud side kahe arvuti vahel IP-võrgu kaudu
Läbistustestimine	arvutisüsteemi, võrgu või veebirakenduse testimine, et leida turvanõrkused, mida ründaja võiks ära kasutada
Kooskõlastav võrdlemine	protsess, millega tagatakse kahe eri andmestiku kooskõla
VPN	virtuaalne privaatvõrk
XML	laiendatav märgistuskeel. See võimaldab projekteerijatel luua oma kohandatud sildid, millega saab määratleda, edastada, valideerida ja tõlgendada andmeid rakenduste ja organisatsioonide vahel.

2. SISSEJUHATUS

Euroopa Liidu ja Šveitsi Konföderatsiooni vahel 23. novembril 2017 sõlmitud kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepinguga (edaspidi „leping“) nähakse ette selliste lubatud heitkoguse ühikute (edaspidi „LHÜd“) vastastikune tunnustamine, mida saab kasutada kohustuste täitmiseks Euroopa Liidu heitkogustega kauplemise süsteemis (edaspidi „ELi HKS“) või Šveitsi heitkogustega kauplemise süsteemis (edaspidi „Šveitsi HKS“). ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks luuakse otseside liidu registri ELi tehingulogi ja Šveitsi registri täiendava tehingulogi vahel, mis võimaldab kummaski HKSis välja antud LHÜde ülekandmist ühest registrist teise (lepingu artikli 3 lõige 2). Selleks et rakendada tööle ELi HKSi ja Šveitsi HKSi vaheline ühendus, võeti 2020. aastal kasutusele ajutine lahendus. Alates 2023. aastast muutub kõnealuse kahe heitkogustega kauplemise süsteemi vaheline registriühendus järk-järgult alaliseks registriühenduseks, mis eelduste kohaselt rakendatakse tööle hiljemalt 2024. aastal ning mis võimaldab ühendatud turgude toimimist ja saada kasu turu likviidsusest ning teha tehinguid kahe ühendatud süsteemi vahel viisil, mis on samaväärne kahest süsteemist koosneva turuga ja mis võimaldab turuosalistel tegutseda nii, nagu nad oleksid ühel turul, tingimusel et poolte üksikud õigusnormid on täidetud (lepingu II lisa).

Lepingu artikli 3 lõike 7 kohaselt peavad Šveitsi registri haldaja ja liidu registri põhihaldaja (lepingus „keskregistrihaldaja“) koostama ühenduse tehnilised standardid, mille aluseks on lepingu II lisas sätestatud põhimõtted ning milles kirjeldatakse üksikasjalikke nõudeid töökindla ja turvalise ühenduse loomiseks Šveitsi täiendava tehingulogi ja Euroopa Liidu tehingulogi vahel. Haldajate koostatud ühenduse tehnilised standardid jõustuvad ühiskomitee otsuse alusel.

Ühiskomitee võttis ühenduse tehnilised standardid vastu oma otsusega nr 2/2020. Käesolevas dokumendis esitatud ühenduse ajakohastatud tehnilised standardid võtab ühiskomitee vastu oma otsusega nr 1/2024. Kooskõlas käesoleva otsusega ja ühiskomitee taotlusel on Šveitsi registri haldaja ja liidu registri põhihaldaja välja töötanud registritevahelise ühenduse töölerakendamise edasised tehnilised suunised, mida ajakohastatakse veelgi, et tagada nende pidev kohandamine tehnika arenguga ja/või ühenduse ohutuse ja turvalisuse ning selle tõhusa ja tulemusliku toimimisega seotud uute nõuetega.

2.1. Kohaldamisala

Käesolev dokument kujutab endast lepinguosaliste ühist arusaama ELi HKSi registri ja Šveitsi HKSi registri vahelise ühenduse tehniliste aluste loomisest. Selles esitatakse tehnilise kirjelduse üldised lähtealused arhitektuuri, teenuste ja turvalisusega seotud nõuete osas, kuid ühenduse töölerakendamiseks on vaja täiendavaid üksikasjalikke suuniseid.

Ühenduse nõuetekohaseks toimimiseks on vaja protsesse ja menetlusi, et ühenduse töölerakendamisega edasi liikuda. Lepingu artikli 3 lõike 6 kohaselt käsitletakse neid küsimusi üksikasjalikult ühistes töömenetlustes (lepingus „ühine tegevuskord“), mille ühiskomitee oma otsusega vastu võtab.

2.2. Adressaadid

Käesolev dokument on adresseeritud Šveitsi registri haldajale ja liidu registri põhihaldajale.

3. ÜLDSÄTTED

3.1. Sideühenduse arhitektuur

Selles punktis kirjeldatakse ELi HKSi ja Šveitsi HKSi vahelise ühenduse toimimise ning sellega seotud eri komponentide üldist arhitektuuri.

Kuna turvalisusel on arhitektuuri määratlemisel oluline osa, on võetud kõik meetmed töökindla arhitektuuri tagamiseks. Alaline registriühendus kasutab failivahetusmehhanismi turvalise õhkeraldatud ühenduse raames.

Tehniline lahendus kasutab

- turvalist sõnumivahetuse edastusprotokolli;
- XML-sõnumeid;
- XMLi-põhist digiallkirja ja krüptimist;
- VPNi.

Järgmisel joonisel on esitatud üldine ülevaade alalise registriühenduse arhitektuurist:

3.1.1. Sõnumivahetus

Liidu registri ja Šveitsi registri vaheline andmeside põhineb turvaliste kanalite kaudu toimival sõnumivahetusmehhanismil. Kumbki otspunkt toetub oma saadud sõnumite hoidlale.

Mõlemad lepinguosalised peavad saadud sõnumite logi koos töötlemise üksikasjadega.

Vigadest või ootamatust seisust tuleb teatada hoiatusega, ning tugirühmade vahel peaks toimuma inimsuhtlus.

Vigade ja ootamatute sündmuste käsitlemisel järgitakse ühistes töömenetlustes kirjeldatud intsidendihaldusprotsessi.

3.1.2. XML-sõnum – üldkirjeldus

XML-sõnum sisaldab ühte järgmistest:

- üks või mitu tehingutaotlust ja/või üks või mitu tehinguvastust;
- üks kooskõlastava võrdlemisega seotud toiming/vastus;
- üks testsõnum.

Igal sõnumil on päis, mis sisaldab järgmist teavet:

- lähte-HKS;
- järjekorranumber.

3.1.3. Valmendusaknad

Alaline registriühendus põhineb eeldefineeritud valmendusakendel, millele järgneb hulk nimega sündmusi. Ühenduse kaudu saadud tehingutaotlused valmendatakse ainult eelnevalt kindlaksmääratud ajavahemike järel ning see hõlmab väljaminevate ja sissetulevate tehingute tehnilist valideerimist. Lisaks võivad kooskõlastavad võrdlemised toimuda iga päev ja neid saab käivitada käsitsi.

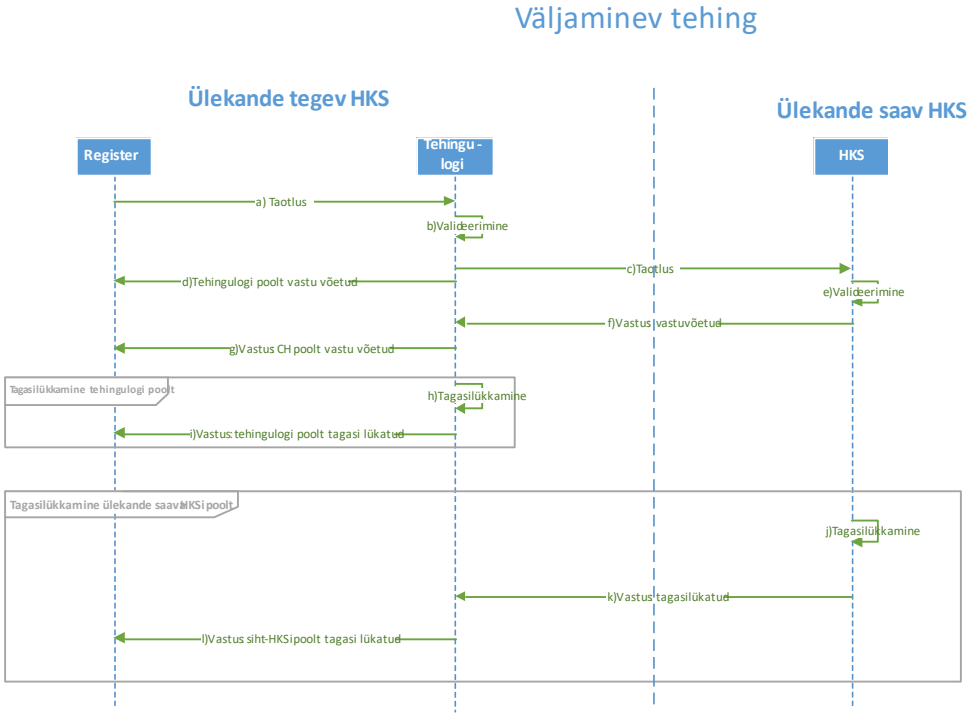
Nende sündmuste sageduse ja/või ajastuse muudatuste käsitlemisel järgitakse ühistes

töömenetlustes kirjeldatud teenindussoovi täitmise protsessi.

3.1.4. Tehinguga seotud sõnumivood

Väljaminevad tehingud

Siin kajastatakse sõnumivoogu ülekande tegeva HKSi vaatepunktist. Konkreetne voog on esitatud järgmisel järgnevusskeemil



Põhivoog näitab järgmisi etappe (nagu eespool esitatud joonisel):

(a) ülekande tegevas HKSis saadetakse tehingutaotlus registrist tehingulogile, kui kõik viivitused on möödas (24-tunnine viivitus, kui kohaldatakse);
(b) tehingulogi valideerib tehingutaotluse;
(c) tehingutaotlus saadetakse siht-HKSile;
(d) lähte-HKSi registrile saadetakse vastuvõtusõnum;
(e) siht-HKS valideerib tehingutaotluse;
(f) siht-HKS saadab vastuvõtusõnumi lähte-HKSi tehingulogile;
(g) tehingulogi saadab vastuvõtusõnumi registrile.

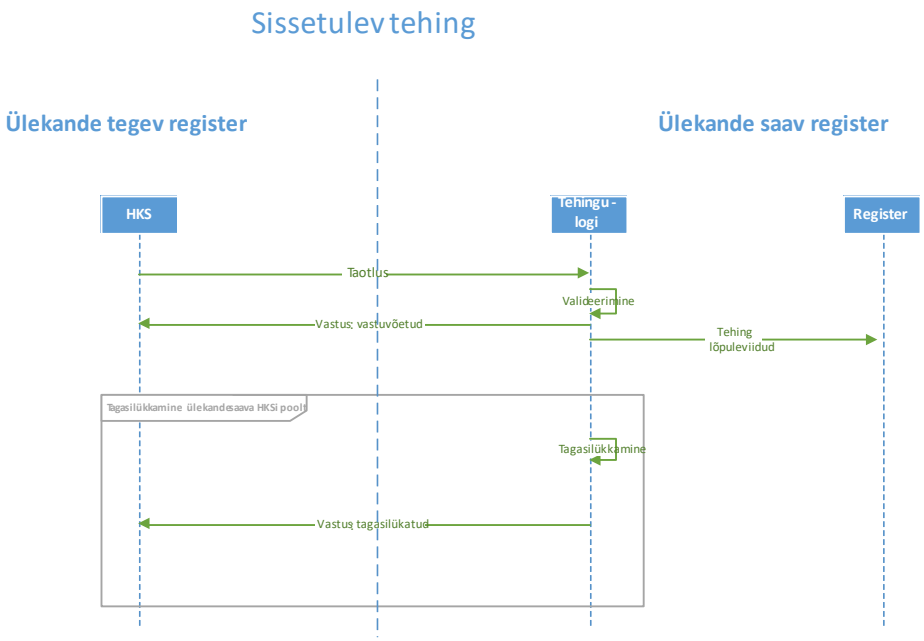
Alternatiivne voog „tagasilükkamine tehingulogi poolt“ (nagu eespool esitatud joonisel, algab punktist a põhivoos):

(a) lähtesüsteemis saadetakse tehingutaotlus registrist tehingulogile, kui kõik viivitused on möödas (24-tunnine viivitus, kui kohaldatakse);
(b) tehingulogi ei valideeri taotlust;
(c) lähteregistrile saadetakse tagasilükkamissõnum.

Alternatiivne voog „tagasilükkamine HKSi poolt“ (nagu eespool esitatud joonisel, algab punktist b põhivoos):

(a) lähte-HKSis saadetakse tehingutaotlus registrist tehingulogile, kui kõik viivitused on möödas (24-tunnine viivitus, kui kohaldatakse);
(b) tehingulogi valideerib tehingu;
(c) tehingutaotlus saadetakse siht-HKSile;
(d) lähte-HKSi registrile saadetakse vastuvõtusõnum;
(e) ülekande saava HKSi tehingulogi ei valideeri tehingut;
(f) ülekande saav HKS saadab tagasilükkamissõnumi ülekannet tegeva HKSi tehingulogile;
(g) tehingulogi saadab tagasilükkamissõnumi registrile.

Sissetulevad tehingud



Siin kajastatakse sõnumivoogu ülekande saava HKSi vaatepunktist. Konkreetne voog on esitatud järgmisel järgnevusskeemil.

Skeemil on kujutatud järgmist:

(1) kui ülekande saava HKSi tehingulogi valideerib taotluse, saadab ta ülekande tegevale HKSile vastuvõtusõnumi ja ülekande saava HKSi registrile sõnumi „tehing lõpuleviidud“;

(2) kui sissetulev taotlus lükatakse ülekande saava tehingulogi poolt tagasi, ei saadeta tehingutaotlust ülekande saava HKSi registrile.

Protokoll

Tehinguga seotud sõnumitsükkel hõlmab ainult kahte sõnumit:

- ülekande tegeva HKSi tehinguettepanek→ ülekande saav HKS;
- ülekande saava HKSi tehinguvastus→ ülekande tegev HKS: kas vastuvõetud või tagasilükatud (sealhulgas tagasilükkamise põhjus).

- Vastuvõetud: tehing viiakse lõpule.
- Tagasilükatud: tehing lõpetatakse.

Tehingu seis

- Kui tehingutaotlus on saadetud, määratakse ülekande tegeva HKSi tehingu seisuks „esitatud“.
- Ülekande saava HKSi tehingu seisuks määratakse „esitatud“, kui taotlus on kätte saadud ja seda menetletakse.
- Ülekande saava HKSi tehingu seisuks määratakse „lõpule viidud“/„lõpetatud“, kui ettepanek on töödeldud. Seejärel saadab ülekande saav HKS vastava vastuvõtu-/tagasilükkamissõnumi.
- Ülekande tegeva HKSi tehingu seisuks määratakse „lõpule viidud“/„lõpetatud“, kui vastuvõtu-/tagasilükkamissõnum on kätte saadud ja töödeldud.
- Kui vastust ei saada, jääb ülekande tegevas HKSis tehingu seisuks „esitatud“.
- Ülekande saavas HKSis määratakse kõigi tehingute, mis jäävad „esitatuks“ kauemaks kui 30 minutiks, seisuks „lõpetatud“.

Tehingutega seotud intsidentide käsitlemisel järgitakse ühistes töömenetlustes kirjeldatud intsidendihaldusprotsessi.

3.2. Andmeedastuse turvalisus

Edastusel olevate andmete suhtes kohaldatakse nelja turvataset:

(1) võrkupääsu reguleerimine: tulemüüri ja võrkude ühenduse kiht;

(2) transporditasandil krüptimine: VPN.

(3) seansitasandil krüptimine: turvaline sõnumivahetuse edastusprotokoll;

(4) rakendustasandil krüptimine: XML-sisu krüptimine ja allkirjastamine.

3.2.1. Tulemüür ja võrguühendus

Registritevaheline ühendus luuakse sellise võrgu kaudu, mis on kaitstud riistvaralise tulemüüriga. Tulemüür peab olema konfigureeritud selliste reeglitega, et VPN-serveriga saavad ühendust ainult „registreeritud“ kliendid.

3.2.2. Virtuaalne privaatvõrk (VPN)

Kogu lepinguosaliste vahelist suhtlust kaitstakse turvalise virtuaalse privaatvõrgu (VPN) abil. VPN-tehnoloogia võimaldab „tunneldada“ läbi sellise võrgu nagu internet ühest punktist teise, kaitstes samal ajal kogu andmesidet. Enne VPN-tunneli loomist väljastatakse võimalikule klientotspunktile elektrooniline sertifikaat, mis võimaldab kliendil ühenduse kooskõlastuse käigus oma isikut tõendada. Kumbki lepinguosaline vastutab sertifikaadi paigaldamise eest oma VPNi otspunkti. Elektroonilise sertifikaadi abil pääseb iga VPN-server ligi keskasutusele, et kooskõlastada autentimismandaat. Tunneli loomise käigus kooskõlastatakse krüptimine, millega tagatakse kogu tunneli kaudu toimuva andmeside kaitse.

Kliendi VPNi otspunktid konfigureeritakse selliselt, et VPN-tunnel oleks püsiv. See võimaldab usaldusväärset kahesuunalist reaalajas sidet lepinguosaliste vahel igal ajal.

Üldiselt kasutab Euroopa Liit turvalist üleeuroopalist valitsusasutuste telemaatiliste teenuste võrku (STESTA) IP-l põhineva eravõrguna. Seetõttu sobib see võrk ka alalise registriühenduse jaoks.

3.2.3. IPseci rakendamine

Kinnis-VPNi taristu loomiseks protokolli IPsec kasutamine tagab asukohtadevahelise autentimise, andmete tervikluse ja krüptimise. IPsec-VPNi konfiguratsioonid tagavad nõuetekohase autentimise VPN-ühenduse kahe otspunkti vahel. Lepinguosalised identivad ja autendivad kaugkliendi IPsec-ühenduse kaudu, kasutades elektroonilisi sertifikaate, mille on välja andnud teise otspunkti poolt tunnustatud sertifitseerimisasutus.

Samuti tagab IPsec VPN-tunneli kaudu toimuva kogu andmeside tervikluse. Andmepaketid räsitakse ja allkirjastatakse, kasutades VPNi loodud autentimisteavet. Samuti tagatakse andmete konfidentsiaalsus, võimaldades IPsec-krüptimist.

3.2.4. Turvaline sõnumivahetuse edastusprotokoll

Turvaliseks andmevahetuseks lepinguosaliste vahel kasutatakse alalise registriühenduse puhul mitut krüptimiskihti. Mõlemad süsteemid ja nende erinevad keskkonnad on võrgu tasandil ühendatud VPN-tunnelite abil. Rakendustasandil kasutatakse failide edastamiseks turvalist sõnumivahetuse edastusprotokolli seansi tasandil.

3.2.5. XML-sisu krüptimine ja allkirjastamine

XML-failides toimub allkirjastamine ja krüptimine kahel tasandil. Iga tehingutaotlus, tehinguvastus ja kooskõlastava võrdlemise sõnum allkirjastatakse digitaalselt eraldi.

Teise sammuna krüptitakse elemendi „sõnum“ kõik alamelemendid eraldi.

Kolmanda sammuna ning kogu sõnumi tervikluse ja salgamatuse tagamiseks allkirjastatakse digitaalselt ka juurelemendi sõnum. Selle tulemusena on XML-vormingus andmed hästi kaitstud. Tehnilisel rakendamisel järgitakse Veebikonsortsiumi standardeid.

Sõnumi dekrüptimiseks ja kontrollimiseks järgitakse protsessi vastupidises järjekorras.

3.2.6. Krüptovõtmed

Krüptimiseks ja allkirjastamiseks kasutatakse avaliku võtme krüptograafiat.

Konkreetselt IPseci puhul kasutatakse sellist elektroonilist sertifikaati, mille on väljastanud mõlema lepinguosalise poolt usaldusväärseks peetav sertifitseerimisasutus. Kõnealune asutus kontrollib isikusamasust ja väljastab sertifikaate, mida kasutatakse organisatsiooni identimiseks ja lepinguosaliste vahel turvaliste andmesidekanalite loomiseks.

Krüptovõtmeid kasutatakse sidekanalite ja andmefailide allkirjastamiseks ja krüptimiseks. Lepinguosalised vahetavad avalikke sertifikaate elektrooniliselt turvaliste kanalite kaudu ja kontrollivad neid ribaväliselt. See on ühistes töömenetlustes kirjeldatud infoturbe halduse lahutamatu osa.

3.3. Registritevahelise ühendusega hõlmatud funktsioonide loetelu

Ühendus määrab kindlaks edastussüsteemi mitme funktsiooni jaoks, millega rakendatakse lepingust tulenevaid äriprotsesse. Ühendus hõlmab ka spetsifikatsiooni kooskõlastava võrdlemise protsessi ja testsõnumite jaoks, mis võimaldavad südamelöögi seiret.

3.3.1. Äritehingud

Äritegevuse seisukohast on ühendusega ette nähtud nelja (4) liiki tehingutaotlused.

- Väline ülekanne
    - Pärast heitkogustega kauplemise süsteemide sidumise jõustumist on ELi ja Šveitsi LHÜd lepinguosaliste vahel asendatavad ja seega täielikult ülekantavad.
    - Registritevahelise ühenduse kaudu tehtav ülekanne hõlmab ülekande tegevat kontot ühes HKSis ja ülekande saavat kontot teises HKSis.
    - Üle saab kanda järgmist nelja (4) liiki LHÜsid mistahes koguses:
        - Šveitsi üldised LHÜd (CH-LHÜd);
        - Šveitsi lennunduse LHÜd (CH-LLHÜd);
        - ELi üldised LHdÜ (EL-LHÜd);
        - ELi lennunduse LHdÜ (EL-LLHÜd).
- Rahvusvaheline eraldamine

Ühe HKSi hallatav õhusõidukikäitaja, kellel on kohustused teises HKSis ning õigus saada kõnealusest teisest HKSist tasuta LHÜsid, saab lennunduse tasuta LHÜd teisest HKSist rahvusvahelise LHÜde eraldamise tehinguga.

- Rahvusvahelise eraldamise tagasipööramine

See tehing tehakse juhul, kui LHÜde tasuta eraldamine õhusõidukikäitaja arvelduskontole teise HKSi poolt tuleb täies mahus tagasi pöörata.

- Ülemääraselt eraldatud LHÜde tagasikandmine

Tagasipööramisega sarnane tehing, kuid tehakse juhul, kui LHÜde eraldamist ei ole vaja täielikult tagasi pöörata, vaid ainult ülemäärased LHÜd need eraldanud HKSile tagasi kanda.

3.3.2. Kooskõlastava võrdlemise protokoll

Kooskõlastav võrdlemine toimub alles pärast seda, kui sõnumite valmendus-, valideerimis- ja töötlemisaknad on suletud.

Kooskõlastav võrdlemine on registritevahelise ühenduse turva- ja kooskõlastusmeetmete lahutamatu osa. Mõlemad lepinguosalised lepivad enne mis tahes ajakava koostamist kokku kooskõlastava võrdlemise täpses ajastuses. Võimalik on igapäevane plaaniline võrdlemine, kui lepinguosalised selles kokku lepivad. Siiski tehakse plaaniline võrdlemine vähemalt pärast valmendust.

Kumbki lepinguosaline võib aga kooskõlastava võrdlemise ka igal ajal käsitsi algatada.

Plaanilise kooskõlastava võrdlemise ajastuse ja sageduse muudatuste käsitlemisel järgitakse ühistes töömenetlustes kirjeldatud teenindussoovi täitmise protsessi.

3.3.3. Testsõnum

Otspunktidevahelise andmeside testimiseks on ette nähtud testsõnum. Sõnum sisaldab andmeid, mis näitavad, et tegemist on testiga, ning sellele vastatakse kohe, kui teine otspunkt on selle kätte saanud.

3.4. Andmesalvestusnõuded

Selleks et toetada mõlema lepinguosalise vajadust säilitada täpne ja kooskõlaline teave ning et tagada vahendid kooskõlastava võrdlemise käigus ebakõlade kõrvaldamiseks, peavad mõlemad lepinguosalised nelja (4) liiki logisid:

- tehingulogid;
- kooskõlastava võrdlemise logid;
- sõnumite arhiiv;
- siseauditi logid.

Kõiki kõnealustes logides sisalduvaid andmeid säilitatakse veaotsingu eesmärgil vähemalt kolm (3) kuud ning nende edasine säilitamine sõltub kummagi lepinguosalise kohaldatavast auditeerimisalasest õigusest. Üle kolme (3) kuu vanad logifailid võib arhiveerida turvalises asukohas sõltumatus IT-süsteemis, kuid neid peab olema võimalik mõistliku aja jooksul välja otsida või neile juurde pääseda.

Tehingulogid

Nii ELi tehingulogi kui ka Šveitsi tehingulogi allsüsteemid on tehingulogi rakendused. Nad on seotud mõlema heitkogustega kauplemise süsteemiga.

Täpsemalt öeldes peavad tehingulogid arvestust iga teisele HKSile saadetud tehinguettepaneku kohta. Iga kirje sisaldab tehingu sisu kõiki välju ja tehingu tulemust (vastuvõtva HKSi vastus). Samuti peetakse tehingulogides arvestust sissetulevate tehingute ja lähte-HKSile saadetud vastuste kohta.

Kooskõlastava võrdlemise logid

Kooskõlastava võrdlemise logi sisaldab iga lepinguosaliste vahel vahetatud kooskõlastava võrdlemise sõnumit, sealhulgas kooskõlastava võrdlemise tunnuskoodi, ajatemplit ja kooskõlastava võrdlemise tulemust: kooskõlastava võrdlemise seis „kooskõlas“ või „lahknevused“. Alalise registriühenduse kooskõlastamissõnumid on vahetatavate sõnumite lahutamatu osa ja neid säilitatakse vastavalt punktis „Sõnumite arhiiv“ kirjeldatule.

Mõlemad lepinguosalised salvestavad iga taotluse ja sellele saadud vastuse kooskõlastava võrdlemise logis. Kuigi kõnealuses logis sisalduvat teavet ei jagata otse kooskõlastava võrdlemise osana, võib ebakõlade kõrvaldamiseks olla vajalik juurdepääs sellele teabele.

Sõnumite arhiiv

Mõlemad lepinguosalised peavad arhiveerima koopia vahetatud andmetest (XML-failid) – nii saadetud kui ka saadud – ning selle, kas need või XML-sõnumid olid õiges vormingus või mitte.

Arhiiv on eelkõige mõeldud auditeerimiseks, et saaks tõendada, mida teisele lepinguosalisele saadeti ja teiselt lepinguosaliselt saadi. Selleks tuleb koos failidega arhiveerida ka nendega seotud sertifikaadid.

Samuti annavad need failid lisateavet veaotsingul.

Siseauditi logid

Nende logide sisu ja kasutuse määrab kindlaks kumbki lepinguosaline iseseisvalt.

3.5. Käitusnõuded

Andmevahetus kahe süsteemi vahel ei ole alalise registriühenduse puhul täielikult autonoomne, see tähendab, et ühenduse töölerakendamiseks on vaja operaatoreid ja menetlusi. Selleks on selles protsessis üksikasjalikult kirjeldatud mitmeid rolle ja vahendeid.

4. KÄIDELDAVUSEGA SEOTUD SÄTTED

4.1. Andmeside käideldavuse projekteerimine

Alalise registriühenduse arhitektuur koosneb põhimõtteliselt info- ja kommunikatsioonitehnoloogia (IKT) taristust ja tarkvarast, mis võimaldab Šveitsi HKSi ja ELi HKSi vahelist andmesidet. Selle andmevoo käideldavuse, tervikluse ja konfidentsiaalsuse kõrge taseme tagamine on seega oluline aspekt, mida tuleb alalise registriühenduse projektis arvesse võtta. Kuna tegemist on projektiga, milles IKT-taristul, tellimustarkvaral ja protsessidel on keskne roll, tuleb paindliku süsteemi projekteerimiseks arvesse võtta kõiki kolme elementi.

IKT-taristu paindlikkus

Käesoleva dokumendi üldsätete peatükis kirjeldatakse üksikasjalikult arhitektuuri komponente. IKT-taristu osas rajatakse alalise registriühendusega paindlik VPN-võrk. Sellega luuakse turvalised sidetunnelid, mille kaudu saab toimuda turvaline sõnumivahetus. Muud taristuelemendid on konfigureeritud kõrgkäideldavaks ja/või need sõltuvad varumehhanismidest.

Tellimustarkvara paindlikkus

Tellimustarkvaramoodulid suurendavad paindlikkust, proovides teatava aja jooksul luua uuesti sidet teise otspunktiga, kui see ei ole mingil põhjusel kättesaadav.

Teenuse paindlikkus

Alalise registriühenduse korral toimub lepinguosalistevaheline andmevahetus eelnevalt kindlaksmääratud ajavahemike järel. Plaanitud andmevahetuse mõne nõutava etapi puhul on vajalik süsteemioperaatorite ja/või registrihaldajate käsitsi sekkumine. Seda arvesse võttes ning selleks, et suurendada käideldavust ja andmevahetuse edukust:

- näevad töömenetlused iga etapi teostamiseks ette ajavahemiku;
- kasutavad alalise registriühenduse tarkvaramoodulid asünkroonset andmesidet;
- tehakse automaatse kooskõlastava võrdlemise käigus kindlaks, kas andmefailide valmendusel esines kummaski otspunktis probleeme;
- käsitatakse seireprotsesse (IKT-taristu ja tellimustarkvaramoodulid) intsidendihaldusmenetluste osana ning need käivitavad intsidendihaldusmenetlused (nagu on määratletud ühistes töömenetlustes). Need menetlused, mille eesmärk on vähendada aega, mis kulub tavapärase töö taastamiseks pärast intsidente, on olulised kõrge käideldavusmäära tagamiseks.

4.2. Initsialiseerimise ja side taasaktiveerimise testimisplaan

Kõik alalise registriühenduse arhitektuuri eri elemendid läbivad hulga individuaal- ja kollektiivteste, et kinnitada platvormi valmisolekut IKT-taristu ja infosüsteemi tasandil. Need toimivustestid on kohustuslik eeltingimus iga kord, kui platvorm viib alalise registriühenduse peatatud olekust tööolekusse.

Ühenduse tööoleku aktiveerimine eeldab eelnevalt kindlaks määratud testimisplaani edukat täitmist. Sellega kinnitatakse, et kumbki register on teinud kõigepealt sisetestid, millele järgneb otspunktühenduvuse valideerimine, enne kui alustatakse tegelike tehingute taotluste esitamist lepinguosaliste vahel.

Testimisplaanis tuleks käsitleda üldist testimisstrateegiat ja testimistaristu üksikasju. Eelkõige peaks see sisaldama iga testiploki iga elemendi kohta järgmist teavet:

- testikriteeriumid ja testimisvahendid;
- testi tegemiseks määratud rollid;
- eeldatavad tulemused (positiivsed ja negatiivsed);
- testi ajakava;
- testi tulemuste registreerimise nõuded;
- veaotsingu dokumentatsioon;
- eskaleerimistingimused.

Protsessina võib tööoleku aktiveerimise testid jagada järgmiseks neljaks (4) mõtteliseks plokiks või etapiks.

4.2.1. IKT-taristu sisetestid

Neid teste peavad tegema ja/või kontrollima registrihaldajad eraldi kummaski otspunktis.

Kummagi otspunkti IKT-taristu iga elementi testitakse eraldi. See hõlmab kõiki taristu komponente. Neid teste võib sooritada automaatselt või käsitsi, kuid nendega tuleb kontrollida, et iga taristuelement on töökorras.

4.2.2. Sidetestid

Neid teste alustavad mõlemad lepinguosalised eraldi, kuid need lõpetatakse omavahelises koostöös.

Kui üksikud elemendid toimivad, tuleb testida registritevahelisi sidekanaleid. Selleks kontrollib kumbki lepinguosaline, et internetiühendus toimib, VPN-tunnelid on loodud ning on olemas asukohtadevaheline IP-ühenduvus. Seejärel tuleks teisele otspunktile kinnitada kohalike ja kaugtaristuelementide juurdepääsetavust ning IP-ühenduvust.

4.2.3. Kogu süsteemi testid (läbivtestimine)

Need testid tuleb sooritada mõlemas otspunktis ja tulemusi jagatakse teise lepinguosalisega.

Kui sidekanaleid ja mõlema registri iga üksikut komponenti on testitud, valmistavad mõlemad otspunktid ette hulga simuleeritud tehinguid ja kooskõlastava võrdlemise, mis esindavad kõiki ühenduse kaudu rakendatavaid funktsioone.

4.2.4. Turvatestid

Neid teste peavad tegema ja/või käivitama registrihaldajad mõlemas otspunktis vastavalt punktides „Turvatestimise suunised“ ja „Riskihindamisega seotud sätted“ kirjeldatule.

Alles pärast seda, kui kõik neli etappi/plokki on lõppenud prognoositavate tulemustega, võib alalist registriühendust pidada töökorras olevaks.

Testimisvahendid

Kumbki lepinguosaline kasutab spetsiaalseid testimisvahendeid (spetsiaalne IKT-taristu tark- ja riistvara) ning töötab välja testimisfunktsioonid oma vastavas süsteemis, et toetada platvormi käsitsi ja pidevat valideerimist. Registrihaldajad võivad igal ajal käsitsi läbi viia individuaalseid või koostööpõhiseid testiprotseduure. Ka tööoleku aktiveerimine toimub käsitsi.

Samuti on ette nähtud, et platvorm teeb korrapäraste ajavahemike järel automaatseid kontrolle. Nende kontrollide eesmärk on suurendada platvormi käideldavust võimalike taristu- või tarkvaraprobleemide varajase avastamise teel. Kõnealune platvormi seirekava koosneb kahest osast.

- IKT-taristu seire: mõlemas otspunktis jälgivad taristut IKT-taristu teenuse osutajad. Automaatsed testid hõlmavad taristu eri elemente ja sidekanalite käideldavust.
- Rakenduse seire: alalise registriühenduse tarkvaramoodulid teostavad süsteemi andmeside seiret rakenduse tasandil (kas käsitsi ja/või korrapäraste ajavahemike järel), et testida ühenduse käideldavust otspunktides, simuleerides ühenduse kaudu teatavaid tehinguid.

4.3. Heakskiitmis-/testimiskeskkond

Liidu registri ja Šveitsi registri arhitektuur koosneb järgmisest kolmest keskkonnast.

- Tootmiskeskkond (PROD): selles keskkonnas hoitakse tegelikke andmeid ja teostatakse tegelikke tehinguid.
- Heakskiitmiskeskkond (ACC): see keskkond sisaldab mittetegelikke või anonüümseks muudetud representatiivseid andmeid. See on keskkond, kus mõlema lepinguosalise süsteemioperaatorid valideerivad uusi väljalaskeid.
- Testimiskeskkond (TEST): see keskkond sisaldab mittetegelikke või anonüümseks muudetud representatiivseid andmeid. Seda keskkonda saavad kasutada üksnes registrihaldajad ja see on mõeldud mõlema lepinguosalise tehtavate integratsioonitestide jaoks.

Kui VPN välja arvata, on need kolm keskkonda üksteisest täiesti sõltumatud, mis tähendab, et riistvara, tarkvara, andmebaasid, virtuaalkeskkonnad, IP-aadressid ja pordid võetakse kasutusele ning need toimivad üksteisest sõltumatult.

Mis puutub VPNi ülesehitusse, siis peab side kolme keskkonna vahel olema täiesti sõltumatu, mis tagatakse STESTA kasutamisega.

5. KONFIDENTSIAALSUSE JA TERVIKLUSEGA SEOTUD SÄTTED

Turvamehhanismide ja -menetlustega nähakse liidu registri ja Šveitsi registri vahelises ühenduses toimuvate toimingute jaoks ette kahe isiku roll (nelja silma põhimõte). Kahe isiku rolli kohaldatakse alati, kui see on vajalik, kuid see ei pruugi olla nõutav kõigi toimingute puhul, mida registrihaldajad teevad.

Turvanõudeid käsitletakse turbekavas, mis hõlmab ka protsesse turvaintsidentide käsitlemiseks pärast turvanõuete võimalikku rikkumist. Nende protsesside seda osa, mis on seotud käitusega, kirjeldatakse ühistes töömenetlustes.

5.1. Turvatestimistaristu

Kumbki lepinguosaline kohustub looma turvatestimistaristu (kasutades ühist tark- ja riistvara, mida kasutatakse nõrkade kohtade tuvastamiseks arendus- ja käitusetapis),

- mis on tootmiskeskkonnast eraldatud;
- kus turvalisust analüüsib süsteemi arendusest ja käitusest sõltumatu rühm.

Kumbki lepinguosaline kohustub tegema nii staatilisi kui ka dünaamilisi analüüse.

Dünaamilise analüüsi puhul (nagu läbistustestimine) kohustuvad mõlemad lepinguosalised piirduma hindamisel üldiselt heakskiitmis-/testimiskeskkonnaga (mis on määratletud punktis „Heakskiitmis-/testimiskeskkond“). Sellest reeglist tehtavad erandid peavad heaks kiitma mõlemad lepinguosalised.

Registriühenduse (mis on määratletud punktis „Sideühenduse arhitektuur“) iga tarkvaramooduli turvalisust testitakse enne selle juurutamist tootmiskeskkonnas.

Testimistaristu peab olema tootmistaristust eraldatud nii võrgu kui ka taristu tasandil ning võimaldama teostada turvateste, mis on vajalikud turvanõuetele vastavuse kontrollimiseks.

5.2. Ühenduse peatamise ja taasaktiveerimisega seotud sätted

Kui tekib kahtlus, et Šveitsi registri, Šveitsi tehingulogi, liidu registri ja ELi tehingulogi turvalisus on ohus, teavitavad lepinguosalised viivitamata teineteist ning peatavad Šveitsi tehingulogi ja ELi tehingulogi vahelise ühenduse.

Teabe jagamise ning ühenduse peatamise otsuse ja selle taasaktiveerimise otsuse tegemisega seotud menetlused on ühistes töömenetlustes kirjeldatud teenindussoovi täitmise protsessi osa.

Ühenduse peatamine

Registriühenduse peatamine vastavalt lepingu II lisale võib toimuda

- halduslikel põhjustel (hooldus, ...) ja seega plaanitult;
- turvalisusega seotud põhjustel (või IT-taristu rikke tõttu) ja seega plaaniväliselt.

Hädaolukorras teavitab lepinguosaline teist lepinguosalist ja peatab ühepoolselt registriühenduse.

Kui registriühendus otsustatakse peatada, tagab kumbki lepinguosaline, et ühendus katkestatakse võrgu tasandil (blokeerides kõik sissetulevad ja väljaminevad ühendused või osa neist).

Otsus registriühendus peatada, olenemata sellest, kas see on plaanitud või plaaniväline, tehakse vastavalt ühistes töömenetlustes kirjeldatud muudatusehalduse või turvaintsidendi halduse menetlusele.

Andmeside taasaktiveerimine

Taasaktiveerimise otsus tehakse vastavalt ühistes töömenetlustes kirjeldatule ja igal juhul mitte enne punktides „Initsialiseerimise ja side taasaktiveerimise testimisplaan“ kirjeldatud turvatestimise edukat lõpuleviimist.

5.3. Turvarikkumist käsitlevad sätted

Turvarikkumist käsitatakse turvaintsidendina, mis mõjutab mis tahes tundliku teabe konfidentsiaalsust ja terviklust ja/või seda käitleva süsteemi käideldavust.

Tundlik teave on kindlaks määratud tundliku teabe loetelus ja seda võidakse käidelda süsteemis või mis tahes sellega seotud osas.

Turvarikkumisega otseselt seotud teavet käsitatakse tundliku teabena märkega „SPECIAL HANDLING: *ETS Critical*“ ja seda käsitletakse vastavalt käitlemisjuhistele, kui ei ole sätestatud teisiti.

Iga turvarikkumist käsitletakse vastavalt ühiste töömenetluste punktile „Turvaintsidentide haldus“.

5.4. Turvatestimise suunised

5.4.1. Tarkvara

Turvatestimine, sealhulgas vajaduse korral läbistustestimine, tehakse vähemalt tarkvara kõigi uute suuremate väljalasete puhul kooskõlas ühenduse tehnilistes standardites sätestatud turvanõuetega, et hinnata ühenduse turvalisust ja sellega seotud riske.

Kui viimase 12 kuu jooksul ei ole toodetud ühtegi suuremat väljalaset, tehakse turvatestimine kasutusel oleva süsteemiga, võttes arvesse küberohtude arengut viimase 12 kuu jooksul.

Registriühenduse turvatestimine toimub heakskiitmiskeskkonnas ja vajaduse korral tootmiskeskkonnas. Seda tehakse kooskõlastatult ja mõlema lepinguosalise kokkuleppel.

Veebirakenduse testimisel järgitakse rahvusvahelisi avatud standardeid, näiteks neid, mis on välja töötatud avatud veebirakenduste turbe projekti (*Open Web Application Security Project* – OWASP) raames.

5.4.2. Taristu

Tootmissüsteemi toetavas taristus tuleb korrapäraselt teha nõrkuseotsing (vähemalt kord kuus) ja leitud nõrkused kõrvaldada eelmises punktis määratletud põhimõtte alusel, kasutades ajakohast nõrkuste andmebaasi.

5.5. Riskihindamisega seotud sätted

Kui tuleb teha läbistustestimine, peab see olema osa turvatestimisest.

Kumbki lepinguosaline võib turvatestimise tegemiseks sõlmida lepingu sellele spetsialiseerunud äriühinguga, tingimusel et

- sellel äriühingul on sellise turvatestimise tegemiseks vajalikud oskused ja kogemused;
- see äriühing ei anna aru otse arendajale ja/või tema töövõtjale ning ei ole seotud registritevahelise ühenduse tarkvara arendamisega ega ole arendaja alltöövõtja;
- see äriühing on allkirjastanud konfidentsiaalsuslepingu, et hoida tulemused konfidentsiaalsena ja käsitleda neid vastavalt tundlikkustasemele „SPECIAL HANDLING: ETS Critical“ kooskõlas käsitlemisjuhistega.