# EUROOPA LIIDU JA ŠVEITSI KONFÖDERATSIOONI VAHELISE KASVUHOONEGAASIDE HEITKOGUSTEGA KAUPLEMISE SÜSTEEMIDE SIDUMISE LEPINGUGA ASUTATUD ÜHISKOMITEE OTSUS nr 2/2020,

**5. november 2020,**

**lepingu I ja II lisa muutmise ning ühenduse tehnilise standardi vastuvõtmise kohta [2021/1034]**

ÜHISKOMITEE,

võttes arvesse Euroopa Liidu ja Šveitsi Konföderatsiooni vahelist kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingut, ([1]) (edaspidi „leping“), eriti selle artikli 3 lõiget 7 ja artikli 13 lõiget 2,

ning arvestades järgmist:

(1) Ühiskomitee 5. detsembri 2019. aasta otsusega nr 2/2019 ([2]) muudeti lepingu I ja II lisa, millega täideti lepingus sätestatud sidumise tingimused.

(2) Pärast ühiskomitee otsuse nr 2/2019 vastuvõtmist ja vastavalt lepingu artikli 21 lõikele 3 vahetasid lepinguosalised oma ratifitseerimis- või heakskiitmiskirju, kuna nad loevad kõiki lepingus sätestatud sidumise tingimusi täidetuks.

(3) Kooskõlas lepingu artikli 21 lõikega 4 jõustus leping 1. jaanuaril 2020.

(4) Lepingu I lisa tuleks muuta kooskõlas lepingu artikli 13 lõikega 2, et registritevahelise ühenduse loomisel tehtud edusammude arvessevõtmisega tagada nende õhusõidukikäitajate haldamise sujuv üleminek, kelle haldamine omistatakse esimest korda Šveitsile.

(5) Selleks et võtta arvesse hiljutisi suundumusi ja tagada suurem paindlikkus lepinguga nõutava registritevahelise ühenduse loomiseks, tuleks lepingu II lisa muuta vastavalt lepingu artikli 13 lõikele 2, et näha ühenduse loomiseks ette suurem, kuid samaväärne tehniliste lahenduste valik.

(6) Lepingu artikli 3 lõike 7 kohaselt peaksid Šveitsi registri haldaja ja liidu põhihaldaja (lepingus „keskregistrihaldaja“) koostama ühenduse tehnilise standardi, mille aluseks on lepingu II lisas sätestatud põhimõtted. Ühenduse tehnilises standardis tuleks kirjeldada üksikasjalikke nõudeid töökindla ja turvalise ühenduse loomiseks Šveitsi täiendava tehingulogi ja Euroopa Liidu tehingulogi vahel. Ühenduse tehniline standard peaks jõustuma ühiskomitee otsuse alusel.

(7) Kooskõlas lepingu artikli 13 lõikega 1 peaks ühiskomitee leppima kokku tehnilistes suunistes, sealhulgas töökindla ja turvalise ühenduse loomises Šveitsi täiendava tehingulogi ja ELi tehingulogi vahel, et tagada lepingu nõuetekohane rakendamine. Tehnilised suunised võib välja töötada lepingu artikli 12 lõike 5 kohaselt moodustatud töörühm. Töörühma peaksid kuuluma vähemalt Šveitsi registri haldaja ja liidu põhihaldaja ning töörühm peaks abistama ühiskomiteed lepingu artikli 13 kohaste ülesannete täitmisel.

(8) Arvestades suuniste tehnilist laadi ja vajadust kohandada neid toimuva arenguga, tuleks Šveitsi registri haldaja ja liidu põhihaldaja välja töötatud tehnilised suunised esitada ühiskomiteele teadmiseks või vajaduse korral heakskiitmiseks,

([1]) ELT L 322, 7.12.2017, lk 3.

([2]) Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepinguga asutatud ühiskomitee 5. detsembri 2019. aasta otsus nr 2/2019, millega muudetakse Euroopa Liidu ja Šveitsi Konföderatsiooni vahelise kasvuhoonegaaside heitkogustega kauplemise süsteemide sidumise lepingu I ja II lisa (ELT L 314, 29.9.2020, lk 68).

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

*Artikkel 1*

Lepingu I lisa B osa punkti 17 teine lõik asendatakse järgmisega:

„Õhusõidukikäitajaid, kelle haldamine omistatakse Šveitsile esimest korda pärast käesoleva lepingu jõustumist, hakkab Šveits haldama pärast omistamisaasta 30. aprilli ja niipea kui ajutine ühendus toimib.“

*Artikkel 2*

Lepingu II lisa neljas lõik asendatakse järgmisega:

„Ühenduse tehnilises standardis nähakse ette, et side Šveitsi tehingulogi ja ELi tehingulogi vahel toimub veebiteenuste sõnumite turvalise vahetusena, mille aluseks on järgmised või samaväärsed tehnilised lahendused (*):

— veebiteenused, mis kasutavad lihtsat objektipöörduse protokolli (Simple Object Access Protocol, SOAP);

— riistvarapõhine VPN (virtuaalne privaatvõrk);

— laiendatav märgistuskeel XML;

— digiallkiri ning

— võrguaja protokollid.

_____

(*) Praegu kasutatakse selliseid tehnilisi lahendusi sidepidamiseks liidu registri ja rahvusvahelise tehingulogi vahel ning ka Šveitsi registri ja rahvusvahelise tehingulogi vahel.“

*Artikkel 3*

Võetakse vastu ühenduse tehniline standard, mis on lisatud käesolevale otsusele.

*Artikkel 4*

Käesolevaga moodustatakse töörühm vastavalt lepingu artikli 12 lõikele 5. Töörühm abistab ühiskomiteed lepingu nõuetekohase rakendamise tagamisel, sealhulgas ühenduse tehnilise standardi rakendamiseks vajalike tehniliste suuniste väljatöötamisel.

Töörühma kuuluvad vähemalt Šveitsi registri haldaja ja liidu põhihaldaja.

*Artikkel 5*

Käesolev otsus jõustub selle vastuvõtmise päeval.

Brüssel, 5. november 2020.

| *Ühiskomitee nimel* | eesistuja | Šveitsi määratud sekretär |
|---|---|---|
| *Euroopa Liidu määratud sekretär* | Beatriz YORDI | Caroline BAUMANN |
| Maja-Alexandra DITTEL | | |

*LISA*

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

STANDARD AJUTISE LAHENDUSE JAOKS

1. **Mõisted**

*Tabel 1-1*

**Äritehingutega seotud akronüümid ja mõisted**

| Akronüüm/termin | Mõiste |
|---|---|
| Lubatud heitkoguse ühik (LHÜ) | Kindlaksmääratud aja jooksul atmosfääri ühe tonni süsinikdioksiidi ekvivalentkoguse paiskamise õigus, mis kehtib üksnes ELi HKSi või Šveitsi HKSi nõuete täitmisel. |
| Šveits | Šveitsi Konföderatsioon |
| CH-LHÜ | Šveitsi üldine LHÜ (teise kohustusperioodi Šveitsi LHÜde puhul kasutatakse lühendit „CH-LHÜ2“) |
| CH-LLHÜ | Šveitsi lennunduse LHÜ |
| ÜTM | Lepinguosaliste poolt ühiselt välja töötatud ühised töömenetlused ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks. |
| HKR | Heitkogustega kauplemise register |
| HKS | Heitkogustega kauplemise süsteem |
| EL | Euroopa Liit |
| EL-LHÜ | ELi üldine LHÜ |
| 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** | Mõiste |
|---|---|
| Asümmeetriline krüptograafia | Kasutab andmete krüptimiseks ja dekrüptimiseks avalikke ja privaatvõtmeid. |
| Sertifitseerimisasutus | Elektroonilisi sertifikaate väljastav üksus. |

| Akronüüm | Mõiste |
|---|---|
| Krüptovõti | Teave, millega määratakse krüptoalgoritmi funktsionaalne väljund. |
| Dekrüptimine | Krüptimise pöördprotsess. |
| Digiallkiri | Matemaatiline meetod, mida kasutatakse sõnumi, tarkvara või digitaaldokumendi autentsuse ja tervikluse valideerimiseks. |
| Krüptimine | 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). ELi HKSi ja Šveitsi HKSi vahelise ühenduse töölerakendamiseks tuleb 2020. aasta maiks või esimesel võimalusel võtta kasutusele ajutine lahendus. Lepinguosalised teevad koostööd, et asendada ajutine registriühenduse lahendus alalisega niipea kui võimalik (lepingu II lisa).

Lepingu artikli 3 lõike 7 kohaselt peavad Šveitsi registri haldaja ja liidu põhihaldaja (lepingus „keskregistrihaldaja“) koostama ühenduse tehnilise standardi, 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 tehniline standard jõustub ühiskomitee otsuse alusel.

Käesolevas dokumendis esitatud ühenduse tehniline standard on ühiskomiteel kavas vastu võtta otsusega nr 2/2020. Kooskõlas käesoleva otsusega palub ühiskomitee Šveitsi registri haldajal ja liidu põhihaldajal töötada välja edasised tehnilised suunised registritevahelise ühenduse töölerakendamiseks ning 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 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 eraldi otsusega vastu võtab.

2.2. *Adressaadid*

Käesolev dokument on adresseeritud Šveitsi registri haldajale ja liidu 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 registriühenduse arhitektuuri määratlemisel oluline osa, on võetud kõik meetmed töökindla arhitektuuri tagamiseks. Kuigi ettenähtud alaline registriühendus põhineb veebiteenustel, kasutatakse ajutise lahenduse puhul selle asemel failivahetusmehhanismi.

Tehniline lahendus kasutab

— turvalist sõnumivahetuse edastusprotokolli;

— XML-sõnumeid;

— XMLi-põhist digiallkirja ja krüptimist;

— VPN-seadet või samaväärset turvalist andmetranspordivõrku.

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.

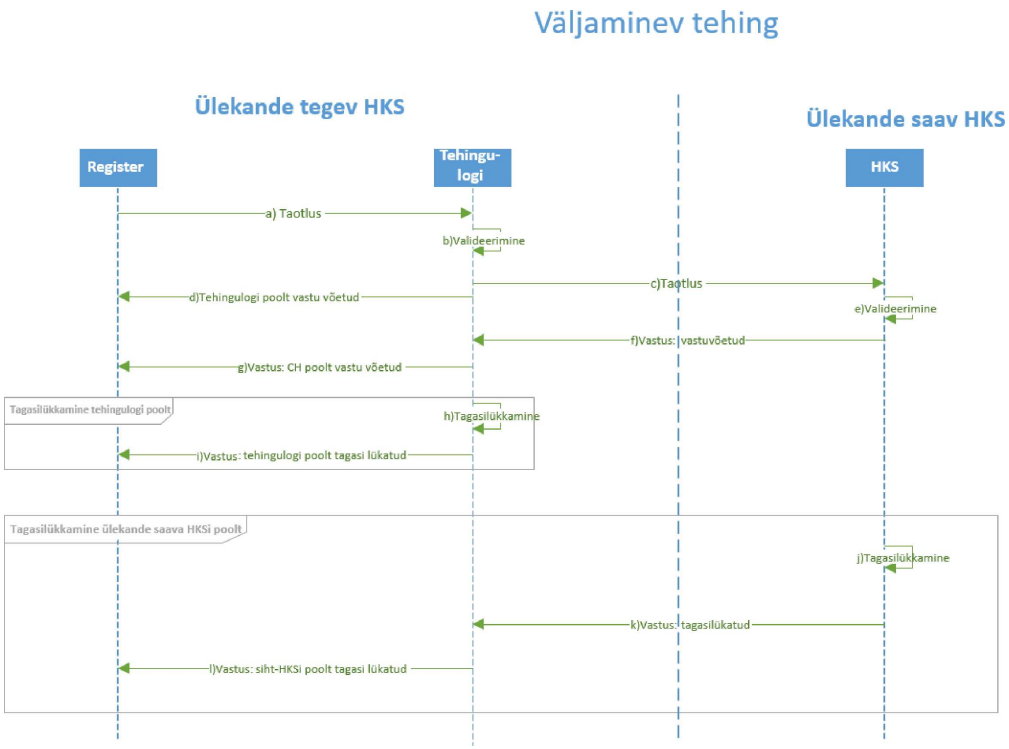
### 3.1.3. Valmendusaknad

Ajutine lahendus põhineb eeldefineeritud valmendusakendel, millele järgneb hulk nimega sündmusi. Ühenduse kaudu saadud tehingutaotlused valmendatakse ainult eelnevalt kindlaksmääratud ajavahemike järel. Valmendusaknad hõlmavad 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. Ülaltoodud järgnevusskeemil on kujutatud kõik konkreetsed väljamineva tehinguga seotud vood.

Põhivoog „tavaline tehing“ (ülaltoodud joonisel kujutatud etappidega):

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“ (ülaltoodud joonisel kujutatud etappidega, mis algavad samuti punktist a):

a) lähte-HKSis saadetakse tehingutaotlus registrist tehingulogile, kui kõik viivitused on möödas (24-tunnine viivitus, kui kohaldatakse);

sellele järgneb:

b) tehingulogi ei valideeri taotlust;

c) lähteregistrile saadetakse tagasilükkamissõnum.

Alternatiivne voog „tagasilükkamine HKSi poolt“ (ülaltoodud joonisel kujutatud etappidega, mis algavad punktist a):

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;

sellele järgneb:

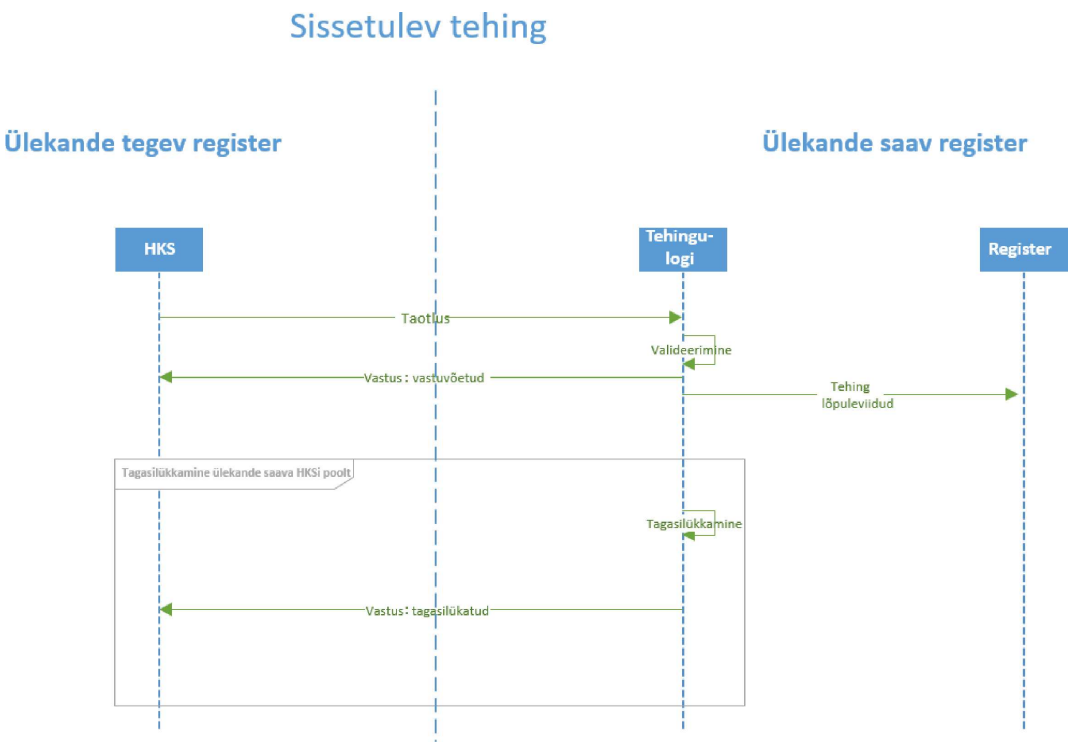
e) ülekande saava HKSi tehingulogi ei valideeri tehingut;

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 saava HKSi tehingu seisuks määratakse „lõpetatud“, kui tehing jääb „esitatuks“ kauemaks kui 30 minutiks.

| |
|---|
| 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 või samaväärne turvaline andmetranspordivõrk;

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 andmesidet kaitstakse turvalise andmetransporditehnoloogia abil. Virtuaalse privaatvõrgu puhul peaks taristu põhinema riistvaral või virtuaalsetel seadmetel. 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.

Mis tahes muu samaväärne lahendus peab vastama eespool nimetatud põhimõtetele.

3.2.3. IPseci rakendamine

VPN-lahenduse kasutamise korral tagab kinnis-VPNi taristu loomiseks protokolli IPsec kasutamine asukohtadevahelise autentimise, andmete tervikluse ja krüptimise. IPsec-VPNi konfiguratsioonid tagavad nõuetekohase autentimise VPN-ühenduse kahe otspunkti vahel. Lepinguosalised idendivad 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 ajutise lahenduse puhul mitut krüptimiskihti. Mõlemad süsteemid ja nende erinevad keskkonnad on võrgu tasandil ühendatud VPN-tunnelite või samaväärsete turvaliste andmetranspordivõrkude 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 sertifikaadi omaniku 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. Vähemalt üks plaaniline võrdlemine tehakse vähemalt pärast iga valmendust.

Kumbki lepinguosaline võib kooskõlastava võrdlemise igal ajal ka 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 sõnumile vastatakse kohe, kui teine otspunkt on selle kätte saanud.

3.4. *Veebiteenuste standardid*

Ajutise lahenduse puhul veebiteenuseid ei kasutata. Väärib siiski märkimist, et XML-sõnumite kuju ja vorming jäävad suures osas samaks. Kui tulevikus võetakse kasutusele alaline registriühendus, peaksid veebiteenused võimaldama XML-sõnumite vahetamist reaalajas.

3.5. *Veebiteenuste erimääratlus*

See punkt ei ole ajutise lahenduse puhul asjakohane. Nagu eelmises punktis märgitud, hakatakse veebiteenuseid kasutama üksnes tulevase alalise registriühenduse puhul.

3.6. *Andmete salvestamise nõuded*

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 sisaldavad tehingulogi rakendusi.

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“. Ajutises lahenduses on kooskõlastava võrdlemise sõnumid vahetatavate sõnumite lahutamatu osa.

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.

3.7. *Käitusnõuded*

Andmevahetus kahe süsteemi vahel ei ole ajutise lahenduse puhul täielikult autonoomne, see tähendab, et ühenduse töölerakendamiseks on vaja operaatoreid ja menetlusi.

## 4. **Käideldavusega seotud sätted**

4.1. *Andmeside käideldavuse projekteerimine*

Ajutise lahenduse 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 ajutise lahenduse ja 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 ajutise ühendusega paindlik VPN-võrk (või samaväärne 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

Ajutise lahenduse puhul toimub lepinguosaliste vaheline andmevahetus eelmääratud ajapiludes kogu aasta vältel. 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 arvestatava ajavahemiku;

— kasutavad ajutise lahenduse tarkvaramoodulid asünkroonset andmesidet;

— tehakse automaatse kooskõlastava võrdlemise käigus kindlaks, kas andmefailide valmendusel esines kummaski otspunktis probleeme;

— käsitatakse seireprotsesse (IKT-taristu ja tellimustarkvaramoodulid) intsidendihaldusmenetlustes 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 ajutise lahenduse 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 ajutise lahenduse 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 mõlemad lepinguosalised 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

Need testid käivitab kumbki lepinguosaline eraldi ning testi lõpetamine eeldab koostööd teise otspunktiga.

Kui üksikud elemendid toimivad, tuleb testida registritevahelisi sidekanaleid. Selleks kontrollib kumbki lepinguosaline, et internetiühendus toimib, VPN-tunnelid (või samaväärne turvaline transpordivõrk) on loodud ning on olemas asukohtadevaheline IP-ühenduvus. Seejärel tuleks teises otspunktis 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 mõlemad lepinguosalised mõlemas otspunktis vastavalt punktides „5.4. Turvatestimise suunised“ ja „5.5. Riskihindamisega seotud sätted“ kirjeldatule.

Alles pärast seda, kui kõik neli etappi/plokki on lõppenud prognoositavate tulemustega, võib ajutist ühendust 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. Registrite haldajad 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: ajutise ühenduse 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 registrite haldajad ja see on mõeldud mõlema lepinguosalise tehtavate integratsioonitestide jaoks.

Kui VPN (või samaväärne võrk) 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.

VPN luuakse kahes erinevas keskkonnas: üks tootmiskeskkonna ja teine, sõltumatu heakskiitmis- ja testimiskeskkonna jaoks.

5. **Konfidentsiaalsuse ja terviklusega seotud sätted**

Turvamehhanismide ja -menetlustega nähakse liidu registri ja Šveitsi registri vahelises ühenduses toimuvate toimingute jaoks ette kahe isiku meetod (nelja silma põhimõte). Kahe isiku meetodit kohaldatakse alati, kui see on vajalik. See ei pruugi aga olla nõutav kõigi toimingute puhul, mida registrite haldajad 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. *Turvatestimise taristu*

Kumbki lepinguosaline kohustub looma turvatestimise taristu (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 „4.3. Heakskiitmis-/testimiskeskkond“). Sellest reeglist tehtavad erandid peavad heaks kiitma mõlemad lepinguosalised.

Registriühenduse (mis on määratletud punktis „3.1. Sideühenduse arhitektuur“) iga tarkvaramooduli turvalisust testitakse enne selle juurutamist tootmiskeskkonnas.

Testimistaristu peab olema tootmistaristust eraldatud nii võrgu kui ka taristu tasandil. Turvateste, mis on vajalikud turvanõuetele vastavuse kontrollimiseks, teostatakse testimistaristus.

5.2. *Ühenduse peatamise ja taasaktiveerimisega seotud sätted*

Kui tekib kahtlus, et Šveitsi registri, Šveitsi täiendava tehingulogi, liidu registri või ELi tehingulogi turvalisus on ohus, teavitab kumbki lepinguosaline viivitamata teist lepinguosalist ning peatab Šveitsi täiendava 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 (nt hooldus), mis on plaanitud;

— turvalisusega seotud põhjustel (või IT-taristu rikke tõttu), mis ei ole plaantitud.

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 mitte, tehakse vastavalt ühistes töömenetlustes kirjeldatud muudatusehalduse või turvaintsidendi halduse menetlusele. |

Andmeside taasaktiveerimine

Registriühenduse taasaktiveerimise otsus tehakse ühistes töömenetlustes kirjeldatud viisil ja igal juhul mitte enne punktides „5.4. Turvatestimise suunised“ ja „4.2. 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 süsteemi mis tahes seotud osas.

Turvarikkumisega otseselt seotud teavet loetakse tundlikuks, sellele määratakse tundlikkustase „KRIITILINE HKS“ ja seda käideldakse vastavalt käitlemisjuhistele, kui ei ole sätestatud teisiti.

| |
|---|
| Iga turvarikkumist käsitletakse kooskõlas ühiste töömenetluste punktiga „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 tehnilises standardis 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. Testimine toimub vastavalt punktis 5.4.1. kirjeldatud meetodile, 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 käidelda neid vastavalt tundlikkustasemele „KRIITILINE HKS“ kooskõlas käitlemisjuhistega.