ROZHODNUTIE č. 2/2020 SPOLOČNÉHO VÝBORU ZRIADENÉHO DOHODOU MEDZI EURÓPSKOU ÚNIOU A ŠVAJČIARSKOU KONFEDERÁCIOU O PREPOJENÍ ICH SYSTÉMOV OBCHODOVANIA S EMISIAMI SKLENÍKOVÝCH PLYNOV

z 5. novembra 2020

o zmene príloh I a II k Dohode a o prijatí prepájacích technických noriem [2021/1034]

SPOLOČNÝ VÝBOR,

so zreteľom na Dohodu medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov ([1]) (ďalej len „dohoda“), a najmä na jej článok 3 ods. 7 a článok 13 ods. 2,

keďže:

(1) Rozhodnutím spoločného výboru č. 2/2019 z 5. decembra 2019 ([2]) sa zmenili prílohy I a II k dohode, čím sa splnili podmienky na prepojenie stanovené v dohode.

(2) Po prijatí rozhodnutia spoločného výboru č. 2/2019 a podľa článku 21 ods. 3 dohody si zmluvné strany vymenili svoje listiny o ratifikácii alebo schválení, pretože sa domnievajú, že všetky podmienky na prepojenie uvedené v dohode boli splnené.

(3) V súlade s článkom 21 ods. 4 dohody nadobudla dohoda platnosť 1. januára 2020.

(4) Príloha I k dohode by sa mala zmeniť v súlade s článkom 13 ods. 2 dohody, aby sa zabezpečil bezproblémový prechod v rámci riadenia prevádzkovateľov lietadiel pridelených Švajčiarsku po prvýkrát, zohľadňujúc pokrok dosiahnutý pri vytváraní prepojenia registrov.

(5) Aby sa zohľadnil najnovší vývoj a zabezpečila sa vyššia úroveň flexibility na vytvorenie prepojenia registrov, ako to vyžaduje dohoda, mala by sa príloha II k dohode zmeniť v súlade s článkom 13 ods. 2 dohody, aby sa umožnilo zriadenie prepojenia registrov s väčším, ale rovnocenným súborom technológií.

(6) Podľa článku 3 ods. 7 dohody švajčiarsky správca registra a ústredný správca registra Únie by mali vypracovať prepájacie technické normy (LTS) na základe zásad stanovených v prílohe II k dohode. V prepájacích technických normách by sa mali opísať podrobné požiadavky na vytvorenie spoľahlivého (robust) a bezpečného spojenia medzi dodatkovým protokolom transakcií Švajčiarska (Swiss Supplementary Transaction Log – SSTL) a protokolom transakcií Európskej únie (European Union Transaction Log – EUTL). Prepájacie technické normy by mali začať platiť po prijatí rozhodnutia spoločného výboru.

(7) V súlade s článkom 13 ods. 1 dohody by mal spoločný výbor odsúhlasiť technické usmernenia s cieľom zabezpečiť riadne vykonávanie dohody vrátane vytvorenia spoľahlivého a bezpečného spojenia medzi SSTL a EUTL. Technické usmernenia môže vypracovať pracovná skupina zriadená podľa článku 12 ods. 5 dohody. Pracovná skupina by mala zahŕňať minimálne švajčiarskeho správcu registra a ústredného správcu registra Únie a mala by pomáhať spoločnému výboru pri výkone jeho funkcií podľa článku 13 dohody.

(8) Vzhľadom na technickú povahu usmernení a potrebu prispôsobiť ich aktuálnemu vývoju by sa technické usmernenia vypracované švajčiarskym správcom registra a ústredným správcom registra Únie mali predložiť spoločnému výboru na účely informovania alebo v prípade potreby na účely schválenia,

([1]) Ú. v. EÚ L 322, 7.12.2017, s. 3.

([2]) Rozhodnutie č. 2/2019 Spoločného výboru zriadeného Dohodou medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov z 5. decembra 2019, ktorým sa menia prílohy I a II k Dohode medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov (Ú. v. EÚ L 314, 29.9.2020, s. 68).

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Časť B bod 17 druhý odsek prílohy I k dohode sa nahrádza takto:

„Švajčiarsko prevezme riadenie prevádzkovateľov lietadiel, ktorí mu boli prvý raz pridelení po nadobudnutí platnosti tejto dohody, po 30. apríli roka pridelenia a po uvedení predbežného prepojenia registrov do prevádzky.“

Článok 2

Štvrtý pododsek prílohy II k dohode sa nahrádza takto:

„V prepájacích technických normách sa uvedie, že komunikácia medzi SSTL a EUTL spočíva v zabezpečenej výmene webových správ pomocou týchto technológií (*) alebo rovnocenných technológií:

— webových služieb, ktoré využívajú protokol na jednoduchý prístup k objektom (Simple Object Access Protocol, SOAP),

— hardvérovej virtuálnej privátnej siete (Virtual Private Network, VPN),

— XML (Extensible Markup Language, rozšíriteľný značkový jazyk),

— digitálneho podpisu a

— časových protokolov siete (Network Time Protocol).

_____

(*) Tieto technológie sa v súčasnosti používajú na vytvorenie prepojenia medzi registrom Únie a medzinárodným protokolom transakcií, ako aj medzi švajčiarskym registrom a medzinárodným protokolom transakcií.“

Článok 3

Týmto sa prijímajú prepájacie technické normy (LTS), ktoré tvoria prílohu k tomuto rozhodnutiu.

Článok 4

Týmto sa zriaďuje pracovná skupina podľa článku 12 ods. 5 dohody. Spoločnému výboru bude pomáhať pri zabezpečovaní riadneho vykonávania dohody vrátane vypracovania technických usmernení na vykonávanie prepájacích technických noriem.

Členmi pracovnej skupina musia byť minimálne švajčiarsky správca registra a ústredný správca registra Únie.

Článok 5

Toto rozhodnutie nadobúda účinnosť dňom jeho prijatia.

V Bruseli 5. novembra 2020

Za spoločný výbor	Predsedníčka	Tajomníčka za Švajčiarsko
Tajomníčka za Európsku úniu	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

PRÍLOHA

Prepájacie technické normy (LTS) podľa článku 3 ods. 7 Dohody medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov

NORMY PRE PREDBEŽNÉ RIEŠENIE

1. **Glosár**

Tabuľka 1-1

Všeobecné skratky a definície

Skratka/Termín	Definícia
Kvóta	Kvóta oprávňujúca vypustiť jednu tonu ekvivalentu oxidu uhličitého počas určitého obdobia, pričom táto kvóta je platná len na účely splnenia požiadaviek EU ETS alebo ETS Švajčiarska.
CH	Švajčiarska konfederácia
CHU	Švajčiarske všeobecné kvóty (termín „CHU2“ sa používa ako skratka pre záväzné obdobie 2 kvót CHU)
CHUA	Švajčiarska kvóta pre leteckú dopravu
COP	Spoločné operačné postupy, ktoré spoločne vypracovali zmluvné strany dohody s cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska.
ETR	Register na obchodovanie s emisnými kvótami
ETS	Systém obchodovania s emisiami
EÚ	Európska únia
EUA	Všeobecná kvóta EÚ
EUAA	Kvóta EÚ pre leteckú dopravu
EUCR	Konsolidovaný register Európskej únie
EUTL	Protokol transakcií Európskej únie
Register	Systém účtovania kvót vydaných v rámci ETS, ktorý sleduje vlastníctvo kvót vedených na elektronických účtoch.
SSTL	Dodatkový protokol transakcií Švajčiarska
Transakcia	Proces v registri, ktorý zahŕňa prevod kvóty z jedného účtu na iný.
Systém protokolov transakcií	Protokoly transakcií obsahujú záznam o každej navrhovanej transakcii zaslanej z jedného registra do druhého.

Tabuľka 1-2

Technické skratky a definície

Skratka	Definícia
Asymetrická kryptografia	Používa verejné a súkromné kľúče na šifrovanie a dešifrovanie dát.
Certifikačný orgán (CA)	Subjekt, ktorý vydáva digitálne certifikáty.

Skratka	Definícia
Šifrovací kľúč	Informácia, ktorá určuje funkčný výstup šifrovacieho algoritmu.
Dešifrovanie	Opačný proces k šifrovaniu.
Digitálny podpis	Matematická technika používaná na validáciu autentickosti a integrity správy, softvéru alebo digitálneho dokumentu.
Šifrovanie	Proces premeny informácií alebo dát na kód, najmä s cieľom zabrániť neoprávnenému prístupu.
Príjem súboru	Proces čítania súboru.
Firewall	Zariadenie alebo softvér sieťovej bezpečnosti, ktorý monitoruje a kontroluje prichádzajúcu a odchádzajúcu sieťovú prevádzku na základe vopred stanovených pravidiel.
Monitorovanie pravidelného signálu	Pravidelný signál generovaný a monitorovaný hardvérom alebo softvérom s cieľom indikovať bežnú prevádzku alebo synchronizovať iné časti počítačového systému.
IPSec	IP SECurity. Súbor sieťových protokolov, ktorý autentifikuje a šifruje dátové pakety s cieľom poskytnúť zabezpečenú šifrovanú komunikáciu medzi dvoma počítačmi cez sieť internetového protokolu.
Penetračné testovanie	Spôsob testovania počítačového systému, siete alebo webovej aplikácie, ktorého cieľom je nájsť zraniteľné miesta v oblasti zabezpečenia, ktoré by útočník mohol využiť.
Proces zosúhlasenia	Proces zabezpečenia zhody dvoch súborov záznamov.
VPN	Virtuálna privátna sieť
XML	Rozšíriteľný značkový jazyk. Umožňuje programátorom vytvoriť si vlastné prispôsobené značky, ktoré umožňujú definovať, prenášať, validovať a interpretovať dáta medzi aplikáciami a medzi organizáciami.

2. **Úvod**

V dohode medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov z 23. novembra 2017 (ďalej len „dohoda“) sa stanovuje vzájomné uznávanie emisných kvót, ktoré možno použiť na dosiahnutie súladu v rámci systému obchodovania s emisiami Európskej únie (ďalej len „EU ETS“) alebo systému obchodovania s emisiami Švajčiarska (ďalej len „ETS Švajčiarska“). S cieľom realizovať prepojenie medzi EU ETS a ETS Švajčiarska sa zriadi priame prepojenie medzi protokolom transakcií Európskej únie (European Union Transaction Log – EUTL) registra Únie a dodatkovým protokolom transakcií Švajčiarska (Swiss Supplementary Transaction Log – SSTL) švajčiarskeho registra, čím sa umožní prenos emisných kvót vydaných v rámci ktoréhokoľvek z týchto dvoch ETS medzi registrami (článok 3 ods. 2 dohody). S cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska sa bude od mája 2020 alebo čo najskôr po uvedenom mesiaci uplatňovať predbežné riešenie. Zmluvné strany sú povinné spolupracovať na čo možno najvčasnejšom nahradení predbežného riešenia trvalým prepojením registrov (príloha II k dohode).

Podľa článku 3 ods. 7 dohody švajčiarsky správca registra a ústredný správca registra Únie vypracujú prepájacie technické normy (LTS) na základe zásad stanovených v prílohe II k dohode s opisom podrobných požiadaviek na vytvorenie stabilného a bezpečného spojenia medzi SSTL a EUTL. Prepájacie technické normy vypracované správcami nadobudnú účinnosť, keď sa prijmú vo forme rozhodnutia spoločného výboru.

Prepájacie technické normy uvedené v tomto dokumente má prijať spoločný výbor rozhodnutím č. 2/2020. V súlade s týmto rozhodnutím spoločný výbor požiada švajčiarskeho správcu registra a ústredného správcu registra Únie, aby vypracovali ďalšie technické usmernenia s cieľom sfunkčniť prepojenie a aby zabezpečili, aby sa tieto usmernenia neustále prispôsobovali technickému pokroku a novým požiadavkám týkajúcim sa bezpečnosti a zabezpečenia prepojenia, ako aj jeho účinného a efektívneho fungovania.

2.1. *Rozsah pôsobnosti*

Tento dokument predstavuje všeobecnú zhodu zmluvných strán dohody týkajúcu sa vytvorenia technických základov prepojenia medzi registrami EU ETS a ETS Švajčiarska. Aj keď uvádza základnú líniu pre technické špecifikácie z hľadiska požiadaviek na štruktúru, služby a zabezpečenie, na sfunkčnenie prepojenia budú potrebné aj niektoré ďalšie podrobné usmernenia.

Na správne fungovanie si prepojenie bude vyžadovať procesy a postupy slúžiace na zabezpečenie jeho ďalšieho sfunkčnenia. Podľa článku 3 ods. 6 dohody sa tieto záležitosti podrobne uvádzajú v dokumente týkajúcom sa spoločných operačných postupov, ktorý sa má prijať samostatne, a to rozhodnutím spoločného výboru.

2.2. *Adresáti*

Tento dokument je určený švajčiarskemu správcovi registra a ústrednému správcovi registra Únie.

3. **Všeobecné ustanovenia**

3.1. *Štruktúra komunikačného prepojenia*

Účelom tohto oddielu je poskytnúť opis všeobecnej štruktúry sfunkčnenia prepojenia medzi EU ETS a ETS Švajčiarska a jej jednotlivých zložiek.

Pretože kľúčovou časťou definície štruktúry je zabezpečenie prepojenia registrov, boli prijaté všetky opatrenia, aby sa vytvorila spoľahlivá štruktúra. Hoci predpokladané trvalé prepojenie registrov bude založené na webových službách, predbežné riešenie bude namiesto toho používať mechanizmus výmeny súborov.

Technické riešenie používa:

— prenosový protokol zabezpečenej výmeny správ,

— správy XML,

— digitálny podpis a šifrovanie založené na XML,

— zariadenie VPN alebo rovnocennú sieť na zabezpečený prenos dát.

3.1.1. Výmena správ

Komunikácia medzi registrom Únie a švajčiarskym registrom bude založená na mechanizme výmeny správ prostredníctvom zabezpečených kanálov. Každý koniec bude využívať vlastné úložisko prijatých správ.

Obidve zmluvné strany si vedú záznamy prijatých správ spolu s podrobnosťami o spracovaní.

Chyby alebo neočakávaný stav sa budú oznamovať ako upozornenia a medzi podpornými tímami by sa mal by sa udržiavať ľudský kontakt.

Chyby a neočakávané udalosti sa budú riešiť v súlade s prevádzkovými postupmi stanovenými v procese riadenia incidentov v rámci spoločných operačných postupov.

3.1.2. Správa XML – Všeobecný opis

Správa XML obsahuje jeden z týchto prvkov:

— jednu alebo viacero transakčných žiadostí a/alebo jednu alebo viacero transakčných odpovedí,

— jednu operáciu/odpoveď na zosúhlasenie,

— jednu testovaciu správu.

Každá správa obsahuje záhlavie s týmito údajmi:

— východiskový systém ETS,

— poradové číslo.

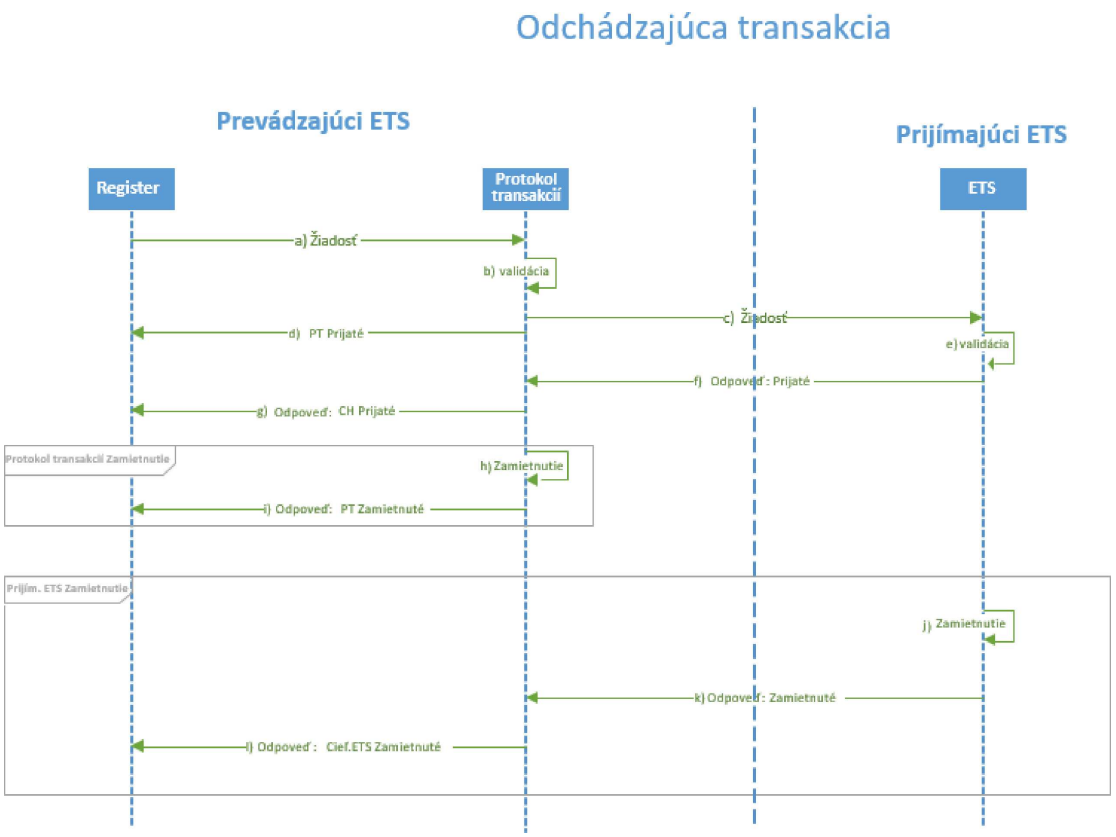
3.1.3. Okná pre príjem

Predbežné riešenie je založené na vopred určených oknách pre príjem, po ktorých nasleduje súbor pomenovaných udalostí. Transakčné žiadosti prijaté cez prepojenie budú prijaté len vo vopred stanovených intervaloch. Okná pre príjem zahŕňajú technickú validáciu odchádzajúcich a prichádzajúcich transakcií. Okrem toho môže zosúhlasenie prebiehať denne a môže sa spustiť manuálne.

Zmeny frekvencie a/alebo načasovania ktorejkoľvek z týchto udalostí sa budú spracovávať v súlade s prevádzkovými postupmi stanovenými v procese plnenia požiadaviek spoločných operačných postupov.

3.1.4. Toky správ o transakciách

Odchádzajúce transakcie



Vyjadrené je hľadisko prevádzajúceho ETS. Vo vyššie uvedenom sekvenčnom diagrame sú zobrazené všetky špecifické toky odchádzajúcich transakcií.

Hlavný tok „Normálna transakcia“ (s krokmi uvedenými na obrázku vyššie):

a) pokiaľ ide o prevádzajúci ETS, transakčná žiadosť sa odošle z registra do protokolu transakcií hneď po uplynutí všetkých obchodných oneskorení (24 hodinového oneskorenia v príslušných prípadoch);

b) protokol transakcií transakčnú žiadosť validuje;

c) transakčná žiadosť sa odošle do cieľového ETS;

d) do registra východiskového ETS sa zašle odpoveď o akceptácii;

e) cieľový ETS transakčnú žiadosť validuje;

f) cieľový ETS zašle odpoveď o akceptácii späť do protokolu transakcií východiskového ETS;

g) protokol transakcií zašle odpoveď o akceptácii do registra.

Alternatívny tok „Zamietnutie v protokole transakcií“ [s krokmi uvedenými na obrázku vyššie, začína sa narovnako od bodu a)]:

a) Vo východiskovom ETS sa transakčná žiadosť zašle z registra do protokolu transakcií po uplynutí všetkých obchodných oneskorení (24 hodinového oneskorenia v príslušných prípadoch).

Potom nasleduje:

b) protokol transakcií žiadosť nevaliduje;

c) správa o zamietnutí sa zašle do východiskového registra.

Alternatívny tok „Zamietnutie v ETS“ [s krokmi uvedenými na obrázku vyššie, začína sa od bodu a)]:

a) vo východiskovom ETS sa transakčná žiadosť zašle z registra do protokolu transakcií po uplynutí všetkých obchodných oneskorení (24 hodinového oneskorenia v príslušných prípadoch);

b) protokol transakcií transakciu validuje;

c) transakčná žiadosť sa odošle do cieľového ETS;

d) do registra východiskového ETS sa zašle odpoveď o akceptácii.

Potom nasleduje:

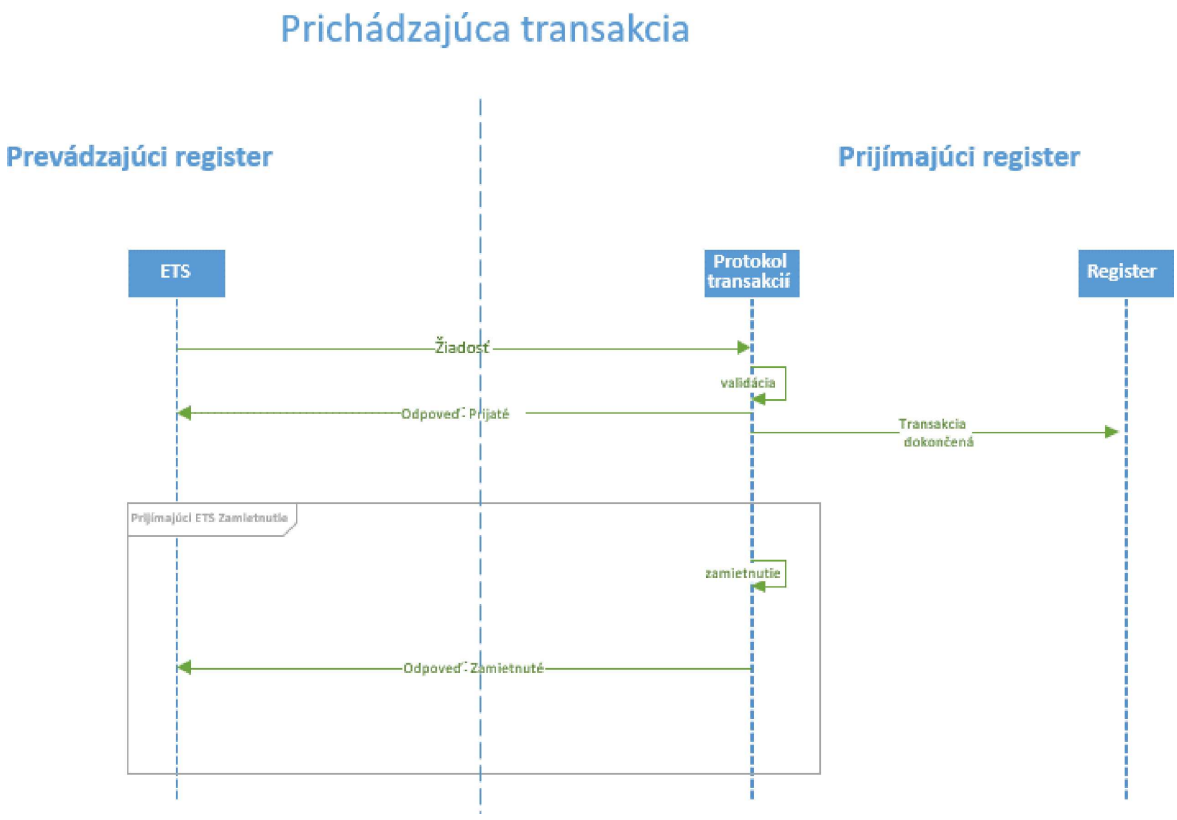
e) protokol transakcií prijímajúceho ETS transakciu nevaliduje;

f) prijímajúci ETS odošle odpoveď o zamietnutí do protokolu transakcií prevádzajúceho ETS;

g) protokol transakcií zašle zamietnutie do registra.

Prichádzajúce transakcie

Vyjadrené je hľadisko prijímajúceho ETS. Špecifický tok je znázornený na tomto sekvenčnom diagrame:



Tento diagram znázorňuje:

1. Keď protokol transakcií prijímajúceho ETS validuje žiadosť, zašle správu o akceptácii do prevádzajúceho ETS a správu „transakcia dokončená“ do registra prijímajúceho ETS.

2. Ak je v prijímajúcom protokole transakcií prichádzajúca žiadosť zamietnutá a zamietne sa, transakčná žiadosť sa do registra prijímajúceho ETS neodošle.

Protokol

Cyklus správ o transakciách zahŕňa len dve správy:

— Prevádzajúci ETS Návrh na transakciu v prijímajúcom ETS.

— Prijímajúci ETS Transakčná odpoveď v prevádzajúcom ETS: Prijaté alebo zamietnuté (vrátane dôvodu zamietnutia):

  — Prijaté: Transakcia je dokončená.

  — Zamietnuté: Transakcia je zrušená.

Stav transakcie

— Stav transakcie v rámci prevádzajúceho ETS sa pri odoslaní žiadosti nastaví na „navrhovaná“.

— Stav transakcie v rámci prijímajúceho ETS sa pri prijatí žiadosti nastaví na „navrhovaná“, kým sa nespracuje.

— Stav transakcie v rámci prijímajúceho ETS sa po spracovaní návrhu nastaví na „dokončená“/„zrušená“. Prijímajúci ETS potom odošle príslušnú správu o akceptácii/zamietnutí.

— Stav transakcie prevádzajúceho ETS sa po prijatí a spracovaní správy o akceptácii/zamietnutí nastaví na „dokončená“/„zrušená“.

— Ak nebola prijatá žiadna odpoveď, zostane stav transakcie v prevádzajúcom ETS taký, aký bol navrhnutý.

— Prijímajúci ETS nastaví každú transakciu, ktorá zostane v takom stave, ako bola navrhnutá, dlhšie ako 30 minút, na „zrušenú“.

Incidenty súvisiace s transakciami sa budú riešiť v súlade s prevádzkovými postupmi stanovenými v procese riadenia incidentov v rámci spoločných operačných postupov.

3.2. *Zabezpečenie prenosu dát*

V priebehu prenosu budú údaje podliehať štyrom stupňom zabezpečenia:

1. Riadenie prístupu do siete: firewall a vrstva sieťového prepojenia.

2. Šifrovanie na úrovni prenosu: VPN alebo rovnocenná sieť pre zabezpečený prenos dát.

3. Šifrovanie na úrovni relácie: prenosový protokol zabezpečenej výmeny správ.

4. Šifrovanie na úrovni aplikácie: šifrovanie a podpis obsahu XML.

3.2.1. Firewall a sieťové prepojenie

Prepojenie sa vytvorí cez sieť chránenú hardvérovým firewallom. Firewall sa konfiguruje pomocou pravidiel tak, aby sa na server VPN mohli pripojiť len „registrovaní“ klienti.

3.2.2. Virtuálna privátna sieť (VPN)

Všetka komunikácia medzi zmluvnými stranami sa musí chrániť pomocou zabezpečenej technológie prenosu dát. V prípade virtuálnej privátnej siete by infraštruktúra mala byť založená na hardvérových alebo virtuálnych zariadeniach. Technológie VPN poskytujú možnosť „tunelovania“ cez sieť, ako je internet, z jedného bodu do druhého, pričom všetka komunikácia je chránená. Pred vytvorením tunela VPN sa budúcemu koncovému bodu klienta vydáva digitálny certifikát, ktorý umožňuje klientovi pri vyjednávaní pripojenia preukázať svoju totožnosť. Každá strana je zodpovedná za inštaláciu certifikátu do svojho koncového bodu VPN. Pomocou digitálnych certifikátov sa každý koncový server VPN pripojí k centrálnej autorite na vyjednanie autentifikačných prihlasovacích údajov. Pri vytváraní tunela sa vyjedná šifrovanie, čím sa zabezpečí, že všetka komunikácia cez tunel bude chránená.

Klientské koncové body VPN sa nakonfigurujú tak, aby udržovali tunel VPN natrvalo s cieľom vždy umožniť spoľahlivú, obojsmernú komunikáciu v reálnom čase medzi zmluvnými stranami.

Akékoľvek iné rovnocenné riešenie musí byť v súlade s uvedenými zásadami.

3.2.3. Implementácia IPSec

V prípade použitia riešenia VPN zabezpečí používanie protokolu IPSec na vytvorenie infraštruktúry VPN typu site-to-site autentifikáciu, integritu dát a šifrovanie dát. Konfigurácie IPSec VPN zabezpečujú riadnu autentifikáciu medzi dvoma koncovými bodmi v spojení VPN. Zmluvné strany identifikujú a autentifikujú vzdialeného klienta prostredníctvom pripojenia IPSec pomocou digitálnych certifikátov, ktoré poskytla certifikačná autorita uznaná druhým koncovým bodom.

IPSec zabezpečuje aj integritu dát pri všetkej komunikácií prechádzajúcej cez tunel VPN. Dátové pakety sa hašujú a podpisujú pomocou autentifikačných informácií vytvorených VPN. Dôvernosť dát je zaručená podobne umožnením šifrovania IPSec.

3.2.4. Prenosový protokol zabezpečenej výmeny správ

Dočasné riešenie používa na zabezpečenú výmenu dát medzi zmluvnými stranami niekoľko šifrovacích vrstiev. Obidva systémy a ich rôzne prostredia sú vzájomne prepojené na úrovni siete prostredníctvom tunelov VPN alebo rovnocenných sietí na zabezpečený prenos dát. Na úrovni aplikácie sa súbory prenášajú pomocou prenosového protokolu zabezpečenej výmeny správ na úrovni relácie.

3.2.5. Šifrovanie a podpis XML

V rámci XML súborov prebieha podpísanie a šifrovanie na dvoch úrovniach. Každá transakčná žiadosť, transakčná odpoveď a správa o zosúhlasení sa elektronicky podpisujú individuálne.

V druhom kroku sa individuálne šifruje každý čiastkový prvok prvku „správy“.

Okrem toho, ako tretí krok a s cieľom zabezpečiť integritu a nespochybniteľnosť celej správy, sa elektronicky podpisuje koreňový prvok správy. Výsledkom je vysoká úroveň ochrany dátového obsahu XML. V rámci technickej realizácie sa dodržiavajú normy Konzorcia World Wide Web.

Na dešifrovanie a overenie správy sa tento proces realizuje v opačnom poradí.

3.2.6. Šifrovacie kľúče

Na šifrovanie a podpisovanie sa bude používať kryptografia s verejným kľúčom.

V konkrétnom prípade IPSec sa musí používať digitálny certifikát vydaný certifikačnou autoritou (CA), ktorej obidve zmluvné strany dôverujú. Táto certifikačná autorita overuje totožnosť držiteľa certifikátu a vydáva certifikáty, ktoré sa použijú na pozitívnu identifikáciu organizácie a nastavenie zabezpečených dátových komunikačných kanálov medzi zmluvnými stranami.

Šifrovacie kľúče sa používajú na podpisovanie a šifrovanie komunikačných kanálov a dátových súborov. Verejné certifikáty si zmluvné strany digitálne vymieňajú pomocou zabezpečených kanálov a overujú sa mimopásmovo (out-of-band). Tento postup je neoddeliteľnou súčasťou procesu riadenia informačnej bezpečnosti v rámci spoločných operačných postupov.

3.3. *Zoznam funkcií v rámci prepojenia*

Prepojenie špecifikuje prenosový systém pre sériu funkcií, ktorými sa vykonávajú obchodné postupy vychádzajúce z dohody. Prepojenie zahŕňa aj špecifikáciu procesu zosúhlasenia a testovacích správ, ktoré umožnia monitorovanie pravidelného signálu.

3.3.1. Obchodné transakcie

Z obchodného hľadiska má prepojenie štyri (4) typy transakčných žiadostí:

— Externý prevod:

  — Po nadobudnutí platnosti prepojenia ETS sú kvóty EÚ a Švajčiarska medzi zmluvnými stranami zameniteľné, a teda plne prevoditeľné.

— Prevod odoslaný cez prepojenie bude zahŕňať prevádzajúci účet v jednom ETS a prijímajúci účet v druhom ETS.

— Prevod môže zahŕňať akékoľvek množstvo štyroch (4) druhov kvót:

  — švajčiarske všeobecné kvóty (CHU),

  — švajčiarske kvóty pre leteckú dopravu (CHUA),

  — všeobecné kvóty EÚ (EUA),

  — kvóty EÚ pre leteckú dopravu (EUAA).

— Medzinárodné pridelenie:

  Prevádzkovatelia lietadiel, ktorých spravuje jeden ETS s povinnosťami v druhom ETS a ktorí majú nárok na bezplatné kvóty z toho druhého ETS, dostanú z druhého systému bezplatné kvóty pre leteckú dopravu prostredníctvom transakcie medzinárodného prideľovania.

— Zrušenie medzinárodného pridelenia:

  Táto transakcia sa uskutoční v prípade, keď sa všetky bezplatné kvóty pridelené na holdingový účet prevádzkovateľa lietadla iným ETS musia zrušiť.

— Vrátenie nadmerného pridelenia:

  Podobne ako v prípade zrušenia, ale tomto prípade nie je potrebné zrušiť celý prídel, a do prideľujúceho ETS sa musia vrátiť len nadmerne pridelené kvóty.

3.3.2. Protokol zosúhlasenia

Zosúhlasenia sa uskutočnia až potom, ako sa zatvoria okná pre príjem správ, ich validáciu a spracovanie.

Zosúhlasenia sú neoddeliteľnou súčasťou opatrení na zaistenie bezpečnosti a konzistentnosti prepojenia. Obidve zmluvné strany sa pred vytvorením akéhokoľvek harmonogramu dohodnú na presnom načasovaní zosúhlasenia. Plánované denné zosúhlasenie sa môže uskutočniť, ak s tým súhlasia obidve zmluvné strany. Po každom prijatí sa vykoná aspoň jedno plánované zosúhlasenie.

Každá zmluvná strana však môže kedykoľvek začať manuálne zosúhlasenia.

Zmeny načasovania a frekvencie plánovaného zosúhlasenia sa budú spracovávať v súlade s prevádzkovými postupmi stanovenými v procese plnenia spoločných operačných postupov.

3.3.3. Testovacia správa

Testovacia správa sa poskytuje na testovanie komunikácie medzi koncovými bodmi. Správa bude obsahovať dáta, ktoré túto správu identifikujú ako test, a bude zodpovedaná po prijatí druhým koncovým bodom.

3.4. *Normy pre webové služby*

Webové služby nebudú v predbežnom riešení použité. Je však potrebné poznamenať, že forma a formát správ XML zostanú sa do veľkej miery nezmenené. So zavedením trvalého prepojenia registrov v budúcnosti by webové služby mali umožňovať výmenu správ XML v reálnom čase.

3.5. *Osobitná definícia webových služieb*

Tento oddiel sa neuplatňuje na predbežné riešenie. Ako sa uvádza v predchádzajúcom oddiele, webové služby sa budú používať len v rámci budúceho trvalého prepojenia registrov.

3.6. *Požiadavky na evidenciu údajov*

S cieľom podporiť potrebu obidvoch zmluvných strán, aby si zachovali presné a konzistentné informácie, a poskytnúť nástroje na použitie v procese zosúhlasenia, aby sa vyriešili nezrovnalosti, musia obidve zmluvné strany viesť štyri (4) typy protokolov údajov:

— protokoly transakcií,

— protokoly zosúhlasenia,

— archív správ,

— protokoly vnútorného auditu.

Všetky dáta v týchto protokoloch sa uchovávajú aspoň počas troch (3) mesiacov na účely odstraňovania porúch a ich ďalšie uchovávanie bude závisieť od platných právnych predpisov v každom koncovom bode na účely auditu. Súbory protokolov staršie ako tri (3) mesiace sa môžu archivovať na zabezpečenom mieste v nezávislom IT systéme, pokiaľ bude možné ich stiahnuť alebo k nim získať prístup v primeranej lehote.

Protokoly transakcií

Subsystémy EUTL aj SSTL obsahujú implementácie protokolov transakcií.

Konkrétnejšie, v protokoloch transakcií sa uchová záznam o každej navrhovanej transakcii odoslanej do druhého ETS. Každý záznam obsahuje všetky polia s obsahom transakcie a následný výsledok danej transakcie (odpoveď prijímajúceho ETS). Protokoly transakcií budú viesť aj záznamy o prichádzajúcich transakciách, ako aj o odpovediach zaslaných východiskovému ETS.

Protokoly zosúhlasenia

Protokol zosúhlasenia obsahuje záznam o každej správe o zosúhlasení medzi obidvoma zmluvnými stranami vrátane identifikácie zosúhlasenia, časovej pečiatky a výsledku zosúhlasenia: Stav zosúhlasenia „Schválené“ alebo „Nezrovnalosti“. V predbežnom riešení sú správy o zosúhlasení neoddeliteľnou súčasťou vymieňaných správ.

Obidve zmluvné strany zaznamenajú každú žiadosť a odpoveď na ňu v protokole zosúhlasenia. Aj keď sa informácie z protokolu zosúhlasenia nezdieľajú priamo v rámci samotného zosúhlasenia, prístup k tejto informácii môže byť potrebný na vyriešenie nezrovnalostí.

Archív správ

Obidve zmluvné strany sú povinné archivovať kópiu vymieňaných dát (súbory XML), odoslaných a prijatých, a informáciu o tom, či boli tieto dáta alebo správy XML v správnom formáte alebo nie.

Hlavným účelom archivácie je audit s cieľom získať dôkazy o tom, čo bolo druhej strane odoslané a z jej strany prijaté. V tomto zmysle je spolu so súbormi potrebné archivovať aj súvisiace certifikáty.

Tieto súbory budú takisto poskytovať dodatočné informácie na odstraňovanie porúch.

Protokol vnútorného auditu

Tieto protokoly si každá strana definuje a používa sama.

3.7. *Prevádzkové požiadavky*

Výmena dát medzi obidvoma systémami nie je v predbežnom riešení úplne autonómna, čo znamená, že na fungovanie prepojenia sú potrební operátori a postupy.

4. **Ustanovenia o dostupnosti**

4.1. *Návrh dostupnosti komunikácie*

Štruktúra predbežného riešenia je v podstate infraštruktúra IKT a softvér, ktorý umožňuje komunikáciu medzi ETS Švajčiarska a EU ETS. Zabezpečenie vysokej úrovne dostupnosti, integrity a dôvernosti tohto toku dát sa preto stáva základným aspektom, ktorý treba zvažovať pri návrhu predbežného riešenia a trvalého prepojenia registrov. Keďže ide o projekt, v ktorom hlavnú úlohu zohrávajú infraštruktúra IKT, softvér na zákazku a procesy, musia sa zohľadniť všetky tri prvky, aby bolo možné navrhnúť odolný systém.

Odolnosť infraštruktúry IKT

Štrukturálne stavebné prvky sú opísané v kapitole o všeobecných ustanoveniach tohto dokumentu. Na strane infraštruktúry IKT zriaďuje dočasné prepojenie odolnú sieť VPN (alebo rovnocennú sieť), ktorá vytvára zabezpečené komunikačné tunely, cez ktoré sa môže uskutočňovať zabezpečená výmena správ. Ostatné prvky infraštruktúry sú konfigurované na vysokú dostupnosť a/alebo sa spoliehajú na záložné mechanizmy.

Odolnosť softvéru na zákazku

Softvérové moduly vyvinuté na zákazku zvyšujú odolnosť opakovanými pokusmi o komunikáciu s druhým koncovým bodom po určitý čas, pokiaľ nie je z nejakého dôvodu dostupný.

Odolnosť služieb

V dočasnom riešení sa výmena dát medzi zmluvnými stranami uskutočňuje počas vopred stanovených časových úsekov počas celého roka. Niektoré z krokov požadovaných v stanovenom harmonograme výmeny dát si vyžadujú manuálny zásah zo strany systémových operátorov a/alebo správcov registrov. Vzhľadom na to a s cieľom zvýšiť dostupnosť a úspešnosť výmen:

— prevádzkové postupy predpokladajú značné časové lehoty na vykonanie každého kroku,

— softvérové moduly predbežného riešenia implementujú asynchrónnu komunikáciu,

— automatický proces zosúhlasenia bude detegovať, či sa pri prijímaní súborov údajov na ktoromkoľvek konci vyskytli problémy,

— zohľadňujú sa monitorovacie procesy (infraštruktúra IKT a softvérové moduly na zákazku), ktoré spúšťajú postupy riadenia incidentov (podľa definície v dokumente o spoločných operačných postupoch). Tieto postupy, ktorých cieľom je skrátiť čas na obnovenie bežnej prevádzky po incidentoch, sú nevyhnutné na zabezpečenie vysokej miery dostupnosti.

4.2. *Inicializácia, komunikácia, reaktivácia a plán testovania*

Všetky rôzne prvky, ktoré sa týkajú štruktúry predbežného riešenia, prejdú sériou individuálnych a kolektívnych testov s cieľom potvrdiť, že platforma je na úrovni infraštruktúry IKT a informačného systému pripravená. Tieto prevádzkové testy sú povinným predpokladom vždy, keď sa v platforme predbežné riešenie zmení z pozastavenia na prevádzkový stav.

Aktivácia prepojenia do prevádzkového stavu si potom vyžaduje úspešnú realizáciu vopred vymedzeného testovacieho plánu. Ten musí potvrdiť, že každý register najprv vykonal súbor interných testov, po ktorých nasleduje validácia spojenia medzi koncovými bodmi predtým, než sa začne predkladanie produkčných transakcií medzi obidvoma zmluvnými stranami.

V testovacom pláne by sa mala uvádzať celková testovacia stratégia a podrobnosti o testovacej infraštruktúre. Každý prvok v každom testovacom bloku by mal konkrétne zahŕňať:

— kritériá a nástroje na testovanie,

— úlohy pridelené na vykonanie testu,

— očakávané výsledky (pozitívne a negatívne),

— časový rozvrh testu,

— zaznamenávanie požiadaviek na výsledky testu,

— dokumentáciu o riešení problémov,

— ustanovenia o postúpení.

Ako proces by sa aktivačné testy prevádzkového stavu mohli rozdeliť do štyroch (4) koncepčných blokov alebo fáz:

4.2.1. Interné testy infraštruktúry IKT

Tieto testy majú byť vykonávané a/alebo jednotlivo kontrolované obidvoma zmluvnými stranami na každom konci.

Každý prvok infraštruktúry IKT na každom konci sa testuje individuálne. Patrí sem každý jednotlivý komponent infraštruktúry. Tieto testy sa môžu vykonať automaticky alebo manuálne, musia však overiť, či je každý prvok infraštruktúry funkčný.

4.2.2. Testy komunikácie

Tieto testy začne každá strana individuálne a dokončia sa v spolupráci s druhým koncom.

Keď budú jednotlivé prvky funkčné, musia sa otestovať komunikačné kanály medzi obidvoma registrami. Na tento účel každá strana overí, že funguje prístup na internet, tunely VPN (alebo rovnocenná sieť pre zabezpečený prenos dát) sú zriadené a že existuje IP prepojiteľnosť site-to-site. Potom by na druhom konci mala potvrdiť dosiahnuteľnosť miestnych a vzdialených prvkov infraštruktúry a IP prepojiteľnosť.

4.2.3. Testy celého systému (medzi koncovými bodmi)

Tieto testy sa majú vykonať na každom konci a výsledky sa poskytnú druhej strane.

Po otestovaní komunikačných kanálov a každého jednotlivého komponentu obidvoch registrov pripraví každý koniec sériu simulovaných transakcií a zosúhlasení, v ktorých sú zastúpené všetky funkcie, ktoré sa majú v rámci prepojenia vykonávať.

4.2.4. Testy zabezpečenia

Tieto testy majú byť vykonávané a/alebo spustené obidvoma zmluvnými stranami na každom konci, ako je podrobne opísané v oddieloch 5.4 „Usmernenia pre testy zabezpečenia“ a 5.5 „Ustanovenia o posudzovaní rizika“.

Až po ukončení každej zo štyroch fáz/blokov s predvídateľnými výsledkami možno považovať predbežné prepojenie za sfunkčnené.

Testovacie zdroje

Každá strana musí využívať špecifické testovacie zdroje (špecifický softvér a hardvér infraštruktúry IKT) a vytvorí si vo svojom príslušnom systéme testovacie funkcie s cieľom podporiť manuálnu a priebežnú validáciu platformy. Správcovia registrov môžu kedykoľvek realizovať manuálne individuálne alebo kooperatívne testovacie postupy. Aktivácia prevádzkového stavu je sama osebe manuálny proces.

Podobne sa tiež stanovuje, že platforma v pravidelných intervaloch vykonáva automatické kontroly. Cieľom týchto kontrol je zvýšiť dostupnosť platformy včasnou detekciou potenciálnych problémov v oblasti infraštruktúry alebo softvéru. Tento plán monitorovania platformy tvoria dva prvky:

— Monitorovanie infraštruktúr IKT: na obidvoch koncoch budú infraštruktúru monitorovať poskytovatelia služieb infraštruktúry IKT. Automatické testy budú zahŕňať rôzne prvky infraštruktúry a dostupnosť komunikačných kanálov.

— Monitorovanie aplikácií: v softvérových moduloch predbežného prepojenia sa bude vykonávať monitorovanie systémovej komunikácie na úrovni aplikácie (buď manuálne a/alebo v pravidelných intervaloch), ktoré bude testovať dostupnosť prepojenia medzi koncovými bodmi simulovaním niektorých transakcií cez prepojenie.

4.3. *Akceptačné/testovacie prostredie*

Štruktúra registra Únie a registra Švajčiarska pozostáva z týchto troch prostredí:

— Produkcia (PROD): V tomto prostredí sú skutočné údaje a spracúvajú sa v ňom skutočné transakcie.

— Schvaľovanie (ACC): Toto prostredie obsahuje dáta, ktoré nie sú skutočné alebo sú anonymizované a reprezentatívne. Ide o prostredie, v ktorom systémoví operátori obidvoch zmluvných strán validujú nové verzie.

— Testovanie (TEST): Toto prostredie obsahuje dáta, ktoré nie sú skutočné alebo sú anonymizované a reprezentatívne. Toto prostredie sa obmedzuje na správcov registrov a má sa používať na vykonávanie integračných testov obidvoma zmluvnými stranami.

S výnimkou VPN (alebo rovnocennej siete) sú tieto tri prostredia vzájomne úplne nezávislé, čo znamená, že hardvér, softvér, databázy, virtuálne prostredia, IP adresy a porty sa nastavujú a prevádzkujú sa nezávisle od seba.

Pokiaľ ide o štruktúru VPN, zriaďuje sa v dvoch rôznych prostrediach, v jednom pre PROD, v druhom nezávislom pre ACC a TEST.

5. **Ustanovenia o dôvernosti a integrite**

Mechanizmy a postupy zabezpečenia stanovujú v prípade operácií prebiehajúcich v prepojení medzi registrom Únie a švajčiarskym registrom metódu dvoch osôb (zásada 4 očí). Metóda dvoch osôb sa uplatňuje vždy, keď je to potrebné. Nemusí sa však uplatňovať na všetky kroky, ktoré správcovia registrov vykonajú.

Požiadavky na zabezpečenie sa posudzujú a riešia v pláne riadenia zabezpečenia, ktorý zahŕňa aj procesy týkajúce sa riešenia kybernetickobezpečnostných incidentov po prípadnom narušení zabezpečenia. Prevádzková časť týchto procesov je opísaná v spoločných operačných postupoch.

5.1. *Infraštruktúra na testovanie zabezpečenia*

Každá zmluvná strana sa zaväzuje vytvoriť infraštruktúru na testovanie zabezpečenia (použitím spoločného súboru softvéru a hardvéru používaného pri zisťovaní zraniteľných miest vo vývojovej a prevádzkovej fáze):

— oddelené od produkčného prostredia,

— kde zabezpečenie analyzuje tím nezávislý od vývoja a prevádzky systému.

Každá strana sa zaväzuje vykonávať statickú aj dynamickú analýzu.

V prípade dynamickej analýzy (ako pri penetračnom testovaní) sa obidve zmluvné strany zaväzujú, že obmedzia hodnotenia na testovacie a akceptačné prostredia (ako sú vymedzené v oddiele 4.3 „Akceptačné/testovacie prostredie“). Výnimky z tejto politiky podliehajú schváleniu obidvoch zmluvných strán.

Pred zavedením do produkčného prostredia sa každý softvérový modul na prepojenie (ako sa vymedzuje v oddiele 3.1 „Štruktúra komunikačného prepojenia“) otestuje z hľadiska zabezpečenia.

Testovacia infraštruktúra musí byť od produkčnej infraštruktúry oddelená na úrovni siete, ako aj na úrovni infraštruktúry. V testovacej infraštruktúre sa vykonávajú testy zabezpečenia potrebné na kontrolu súladu s požiadavkami na zabezpečenie.

5.2. *Ustanovenia o pozastavení prepojenia a jeho reaktivácii*

Ak existuje podozrenie, že bolo narušené zabezpečenie registra Švajčiarska, SSTL, registra Únie alebo EUTL, obidve zmluvné strany sa okamžite navzájom informujú a prerušia prepojenie medzi SSTL a EUTL.

Postupy týkajúce sa výmeny informácií, rozhodnutia pozastavení a rozhodnutia o reaktivácii sú súčasťou procesu plnenia žiadostí v rámci spoločných operačných postupov.

Pozastavenie

Pozastavenie prepojenia registrov v súlade s prílohou II k dohode sa môže uskutočniť z:

— administratívnych dôvodov (napr. údržba), a teda dôvodov plánovaných,

— dôvodov súvisiacich so zabezpečením (alebo s poruchami IT infraštruktúry), a teda dôvodov neplánovaných.

V naliehavom prípade jedna strana informuje druhú a jednostranne pozastaví prepojenie registrov.

Ak sa prijme rozhodnutie o pozastavení prepojenia registrov, každá strana zabezpečí, aby bolo prepojenie prerušené na úrovni siete (blokovaním častí alebo všetkých prichádzajúcich a odchádzajúcich spojení).

Rozhodnutie o pozastavení prepojenia registrov, či už plánované alebo neplánované, sa prijme v súlade s postupom riadenia zmien a kybernetickobezpečnostných incidentov spoločných operačných postupov.

Reaktivácia komunikácie

Rozhodnutie o reaktivácii prepojenia registrov sa prijme spôsobom opísaným v spoločných operačných postupoch a v každom prípade až po úspešnom ukončení postupov testovania zabezpečenia, ako sa podrobne uvádza v oddieloch 5.4 „Usmernenia pre testy zabezpečenia“ a 4.2 „Inicializácia, komunikácia, reaktivácia a plán testovania“.

5.3. *Ustanovenia o narušení bezpečnosti*

Narušenie bezpečnosti sa považuje za kybernetickobezpečnostný incident, ktorý má vplyv na dôvernosť a integritu všetkých citlivých informácií a/alebo dostupnosť systému, ktorý ich spracúva.

Citlivé informácie sú uvedené v zozname citlivých informácií a môžu sa spracúvať v systéme alebo v akejkoľvek súvisiacej časti systému.

Informácie, ktoré sa priamo týkajú narušenia bezpečnosti, sa budú považovať za citlivé, označia sa „ETS CRITICAL“ a budú sa spracúvať v súlade s pokynmi na spracúvanie, pokiaľ nie je stanovené inak.

S každým narušením bezpečnosti sa bude zaobchádzať podľa kapitoly spoločných operačných postupov o riadení kybernetickobezpečnostných incidentov.

5.4. *Usmernenia pre testy zabezpečenia*

5.4.1. Softvér

Aspoň v rámci všetkých dôležitých nových aktualizácií softvéru sa vykoná testovanie zabezpečenia, v prípade potreby vrátane penetračného testovania, a to v súlade s požiadavkami na zabezpečenie stanovenými v prepájacích technických normách, aby bolo možné posúdiť zabezpečenie prepojenia a súvisiace riziká.

Ak za posledných 12 mesiacov nedošlo k žiadnej dôležitej aktualizácii softvéru, vykoná sa testovanie zabezpečenia súčasného systému vzhľadom na vývoj kybernetických hrozieb, ku ktorému za posledných 12 mesiacov došlo.

Testovanie zabezpečenia prepojenia registrov sa vykoná v akceptačnom prostredí a v prípade potreby v produkčnom prostredí a v koordinácii a po vzájomnej dohode obidvoch zmluvných strán.

Pri testovaní webových aplikácií sa budú dodržiavať medzinárodné otvorené normy, napríklad normy vypracované v rámci projektu Open Web Application Security Project (OWASP).

5.4.2. Infraštruktúra

Infraštruktúra podporujúca produkčný systém sa musí pravidelne skenovať s cieľom nájsť zraniteľné miesta (aspoň raz za mesiac) a zistené zraniteľné miesta sa musia opraviť. Testovanie sa vykonáva podľa metódy uvedenej v oddiele 5.4.1 s využitím aktualizovanej databázy zraniteľných miest.

5.5. *Ustanovenia o posudzovaní rizika*

Ak je penetračné testovanie použiteľné, musí sa zahrnúť do testovania zabezpečenia.

Každá zmluvná strana môže uzavrieť zmluvu so špecializovanou spoločnosťou na testovanie zabezpečenia za predpokladu, že táto spoločnosť:

— má zručnosti a skúsenosti v oblasti takéhoto testovania zabezpečenia,

— nie je priamo podriadená vývojárovi a/alebo jeho dodávateľovi, nie je ani zapojená do vývoja softvéru prepojenia ani nie je subdodávateľom vývojára,

— podpísala dohodu o nezverejňovaní informácií s cieľom zachovať dôvernosť výsledkov a zaobchádzať s nimi na úrovni „ETS CRITICAL“ v súlade s pokynmi na spracúvanie.