ROZHODNUTÍ SMÍŠENÉHO VÝBORU ZŘÍZENÉHO DOHODOU MEZI EVROPSKOU UNIÍ A ŠVÝCARSKOU KONFEDERACÍ O PROPOJENÍ JEJICH SYSTÉMŮ OBCHODOVÁNÍ S EMISEMI SKLENÍKOVÝCH PLYNŮ č. 2/2020

ze dne 5. listopadu 2020

o změně příloh I a II dohody a o přijetí technických norem pro propojování [2021/1034]

SMÍŠENÝ VÝBOR,

s ohledem na Dohodu mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů ([1]) (dále jen „dohoda“), a zejména na čl. 3 odst. 7 a čl. 13 odst. 2 této dohody,

vzhledem k těmto důvodům:

(1) Rozhodnutím č. 2/2019 smíšeného výboru ze dne 5. prosince 2019 ([2]) byly změněny přílohy I a II dohody, čímž byly splněny podmínky pro propojení stanovené v této dohodě.

(2) Po přijetí rozhodnutí č. 2/2019 smíšeného výboru a podle čl. 21 odst. 3 dohody si strany vyměnily své listiny o ratifikaci nebo schválení, neboť došly k závěru, že jsou splněny veškeré podmínky pro propojení stanovené v dohodě.

(3) V souladu s čl. 21 odst. 4 dohody vstoupila dohoda v platnost dne 1. ledna 2020.

(4) Příloha I dohody by měla být změněna v souladu s čl. 13 odst. 2 dohody, aby byl zajištěn bezproblémový přechod ve správě provozovatelů letadel poprvé přidělených Švýcarsku, přičemž se zohlední pokrok dosažený při zřizování propojení registrů.

(5) Aby byl zohledněn poslední vývoj a aby byla zajištěna vyšší úroveň flexibility pro zřízení propojení registrů, jak to vyžaduje dohoda, měla by být příloha II dohody změněna v souladu s čl. 13 odst. 2 dohody, aby bylo umožněno nastavení propojení registrů s větší, ale rovnocennou skupinou technologií.

(6) Podle čl. 3 odst. 7 dohody by správce švýcarského registru a ústřední správce Unie měli vypracovat technické normy pro propojování podle zásad uvedených v příloze II dohody. V technických normách pro propojování by měly být popsány podrobné požadavky na zřízení stabilního a zabezpečeného spojení mezi švýcarským doplňkovým protokolem transakcí (SSTL) a protokolem transakcí Evropské unie (EUTL). Technické normy pro propojování by měly nabýt účinnosti poté, co byly přijaty rozhodnutím smíšeného výboru.

(7) V souladu s čl. 13 odst. 1 dohody by se smíšený výbor měl dohodnout na technických pokynech, aby bylo zajištěno řádné provádění dohody včetně zřízení stabilního a zabezpečeného spojení mezi SSTL a EUTL. Technické pokyny mohou být vypracovány pracovní skupinou zřízenou podle čl. 12 odst. 5 dohody. Pracovní skupina by měla zahrnovat alespoň správce švýcarského registru a ústředního správce Unie a měla by smíšenému výboru pomáhat ve výkonu jeho funkcí podle článku 13 dohody.

(8) S ohledem na technickou povahu pokynů a nutnost přizpůsobit je dalšímu vývoji by technické pokyny vypracované správcem švýcarského registru a ústředním správcem Unie měly být předloženy smíšenému výboru pro informaci nebo v příslušných případech ke schválení,

([1]) Úř. věst. L 322, 7.12.2017, s. 3.

([2]) Rozhodnutí č. 2/2019 smíšeného výboru zřízeného Dohodou mezi Evropskou unií a švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů ze dne 5. prosince 2019, kterým se mění přílohy I a II Dohody mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů (Úř. věst. L 314, 29.9.2020, s. 68).

PŘIJAL TOTO ROZHODNUTÍ:

Článek 1

V příloze I části B dohody se druhý odstavec bodu 17 nahrazuje tímto:

„Provozovatelé letadel, kteří jsou Švýcarsku poprvé přiděleni po vstupu této dohody v platnost, jsou spravováni Švýcarskem po 30. dubnu roku přidělení a po zprovoznění prozatímního propojení registrů.“

Článek 2

V příloze II dohody se čtvrtý pododstavec nahrazuje tímto:

„Technické normy pro propojování stanoví, že komunikace mezi SSTL a EUTL spočívá v zabezpečených výměnách vzkazů založených na následujících technologiích (*) nebo na rovnocenných technologiích:

— internetové služby využívající protokol „Simple Object Access Protocol“ (SOAP),

— technické vybavení založené virtuální soukromé sítě (VPN),

— XML (rozšiřitelný značkovací jazyk, „Extensible Markup Language“),

— digitální podpis a

— síťové protokoly pro synchronizaci času.

_____

(*) Tyto technologie se v současné době používají pro navázání spojení mezi registrem Unie a mezinárodní evidencí transakcí, jakož i mezi švýcarským registrem a mezinárodní evidencí transakcí.“

Článek 3

Tímto se přijímají technické normy pro propojování, které tvoří přílohu tohoto rozhodnutí.

Článek 4

Tímto se zřizuje pracovní skupina podle čl. 12 odst. 5 dohody. Pracovní skupina pomáhá smíšenému výboru při zajišťování řádného provádění dohody včetně vypracování technických pokynů pro zavedení technických norem pro propojování.

Pracovní skupina zahrnuje alespoň správce švýcarského registru a ústředního správce Unie.

Článek 5

Toto rozhodnutí vstupuje v platnost dnem přijetí.

V Bruselu dne 5. listopadu 2020.

Za smíšený výbor	předsedkyně	tajemnice pro Švýcarsko
tajemnice pro Evropskou unii	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

PŘÍLOHA

Technické normy pro propojování podle čl. 3 odst. 7 Dohody mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů

NORMY PRO PROZATÍMNÍ ŘEŠENÍ

1. **Glosář**

Tabulka 1-1

Obchodní zkratky a definice

Zkratka/výraz	Definice
Povolenka	Povolení vypouštět jednu tunu ekvivalentu oxidu uhličitého po specifikované období, přičemž toto povolení je platné pouze pro účely splnění požadavků podle systému EU pro obchodování s emisemi nebo systému Švýcarska pro obchodování s emisemi.
CH	Švýcarská konfederace
CHU	Švýcarské všeobecné povolenky (Výraz „CHU2“ se používá jako zkratka pro závazkové období 2 povolenek CHU)
CHUA	Švýcarská povolenka pro letectví
COP	Společné provozní postupy společně vypracované stranami dohody s cílem zprovoznit propojení mezi unijním systémem ETS a švýcarským ETS.
ETR	Registr systému pro obchodování s emisemi
ETS	Systém obchodování s emisemi
EU	Evropská unie
EUA	Všeobecná povolenka EU
EUAA	Povolenka EU pro letectví
EUCR	Konsolidovaný registr Evropské unie
EUTL	Protokol transakcí Evropské unie
Registr	Účetní systém pro povolenky vydané v rámci systému obchodování s emisemi, který sleduje vlastnictví povolenek vedených na elektronických účtech.
SSTL	Švýcarský doplňkový protokol transakcí
Transakce	Proces v registru, který zahrnuje převod povolenky z jednoho účtu na jiný účet.
Protokol transakcí systému	Protokol transakcí obsahuje záznam o každé navržené transakci zaslané z jednoho registru do jiného.

Tabulka 1-2

Technické zkratky a definice

Zkratka	Definice
Asymetrická kryptografie	Používá veřejné a soukromé klíče k šifrování a dešifrování dat.
Certifikační orgán	Subjekt, který vydává digitální certifikáty.

Zkratka	Definice
Kryptografický klíč	Informace, která určuje funkční výstup kryptografického algoritmu.
Dešifrování	Opačný proces šifrování
Digitální podpis	Matematická technika používaná k ověření pravosti a neporušenosti zprávy, softwaru nebo digitálního dokumentu.
Šifrování	Proces přeměny informace nebo údaje na kód, zejména za účelem zabránění neoprávněnému přístupu.
Příjem souboru	Proces čtení souborů
Firewall	Zařízení nebo software pro bezpečnost sítě, které monitoruje a řídí příchozí a odchozí provoz v síti podle předem stanovených pravidel.
Monitorování prezenčního signálu (Heartbeat monitoring)	Pravidelný signál generovaný a monitorovaný hardwarem nebo softwarem za účelem označení normálního provozu nebo synchronizace jiných částí výpočetního systému.
IPSec	IP SECurity. Bezpečnostní rozšíření IP protokolu, které autentizuje a šifruje pakety dat za účelem bezpečné šifrované komunikace mezi dvěma počítači přes síť internetového protokolu.
Penetrační testování	Způsob testování výpočetního systému, sítě nebo webové aplikace, jehož cílem je nalézt slabá místa v zabezpečení, která by mohl využít útočník.
Proces sesouhlasení	Proces zajištění, že dva soubory záznamů spolu souhlasí.
VPN	Virtuální soukromá síť
XML	Rozšiřitelný značkovací jazyk. Umožňuje návrhářům vytvářet vlastní přizpůsobené značky, jež umožňují definovat, přenášet, validovat a interpretovat data mezi aplikacemi a mezi organizacemi.

2. **Úvod**

Dohoda mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů ze dne 23. listopadu 2017 (dále jen „dohoda“) stanoví vzájemné uznávání emisních povolenek, které mohou být použity za účelem zajištění souladu v rámci systému obchodování s emisemi Evropské unie (dále jen „unijní ETS“) nebo v rámci systému obchodování s emisemi Švýcarska (dále jen „švýcarský ETS“). Za účelem operacionalizace propojení mezi unijním ETS a švýcarským ETS bude zřízeno přímé propojení mezi protokolem transakcí Evropské unie (EUTL) registru Unie a švýcarským doplňkovým protokolem transakcí (SSTL) švýcarského registru, které umožní převádět mezi registry povolenky na emise vydané v rámci obou ETS (čl. 3 odst. 2 dohody). Aby bylo možné zprovoznit propojení mezi unijním ETS a švýcarským ETS, zavede se do května 2020, nebo co nejdříve po tomto datu, prozatímní řešení. Strany spolupracují na tom, aby prozatímní řešení co nejdříve nahradily trvalým propojením registrů (příloha II dohody).

Podle čl. 3 odst. 7 dohody správce švýcarského registru a ústřední správce Unie vypracují technické normy pro propojování podle zásad uvedených v příloze II dohody, v nichž budou popsány podrobné požadavky na zřízení stabilního a zabezpečeného spojení mezi SSTL a EUTL. Technické normy pro propojování vypracované správci nabývají účinnosti poté, co byly přijaty rozhodnutím smíšeného výboru.

Technické normy pro propojování uvedené v tomto dokumentu přijme smíšený výbor svým rozhodnutím č. 2/2020. V souladu s tímto rozhodnutím požádá smíšený výbor správce švýcarského registru a ústředního správce Unie, aby vypracovali další technické pokyny k operacionalizaci propojení a aby zajistili jejich průběžné přizpůsobování technickému pokroku a novým požadavkům týkajícím se bezpečnosti a zabezpečení propojení a jeho účelného a efektivního fungování.

2.1 *Oblast působnosti*

Tento dokument vyjadřuje společné ujednání stran dohody, pokud jde o vytvoření technických základů propojení mezi registry unijního ETS a švýcarského ETS. Přestože nastiňuje výchozí stav pro technické specifikace z hlediska požadavků na architekturu, služby a zabezpečení, budou nutné i některé další podrobné pokyny, aby bylo možné propojení zprovoznit.

K jeho správnému fungování bude propojení vyžadovat procesy a postupy, aby bylo možné ho dále provozovat. Podle čl. 3 odst. 6 dohody jsou tyto záležitosti podrobně popsány v samostatném dokumentu týkajícím se společných provozních postupů, který bude přijat samostatným rozhodnutím smíšeného výboru.

2.2 *Určení*

Tento dokument je určen správci švýcarského registru a ústřednímu správci Unie.

3. **Obecná ustanovení**

3.1 *Architektura komunikačního propojení*

Účelem tohoto oddílu je poskytnout popis obecné architektury pro provozování propojení mezi unijním ETS a švýcarským ETS a jednotlivých komponentů, které jej tvoří.

Protože klíčovou částí definice architektury propojení registrů je bezpečnost, byla přijata veškerá opatření, aby byla zajištěna stabilní architektura. Přestože předpokládané stálé propojení registrů bude založeno na webových službách, prozatímní řešení bude namísto toho používat mechanismus výměny souborů.

Technické řešení používá:

— protokol pro bezpečný přenos zpráv,

— zprávy XML,

— digitální podpis a šifrování na základě XML,

— zařízení VPN nebo rovnocennou síť pro bezpečný přenos dat.

3.1.1 Výměna zpráv

Komunikace mezi unijním registrem a švýcarským registrem bude založena na mechanismu výměny zpráv prostřednictvím zabezpečených kanálů. Každý konec bude využívat své vlastní úložiště přijatých zpráv.

Obě strany povedou protokol přijatých zpráv společně s údaji o zpracování.

Chyby nebo neočekávaný stav je třeba hlásit jako výstrahy a mělo by dojít k lidskému kontaktu mezi podpůrnými týmy.

Chyby a neočekávané události budou řešeny podle provozních postupů stanovených v procesu řízení incidentů, který je součástí společných provozních postupů.

3.1.2 Zpráva XML – podrobný popis

Zpráva XML obsahuje jeden z těchto prvků:

— jednu nebo několik žádostí o transakci a/nebo jednu nebo několik odpovědí na transakci,

— jednu operaci/odpověď související se sesouhlasením,

— jednu testovací zprávu.

Každá zpráva obsahuje záhlaví s těmito údaji:

— výchozí systém ETS,

— pořadové číslo.

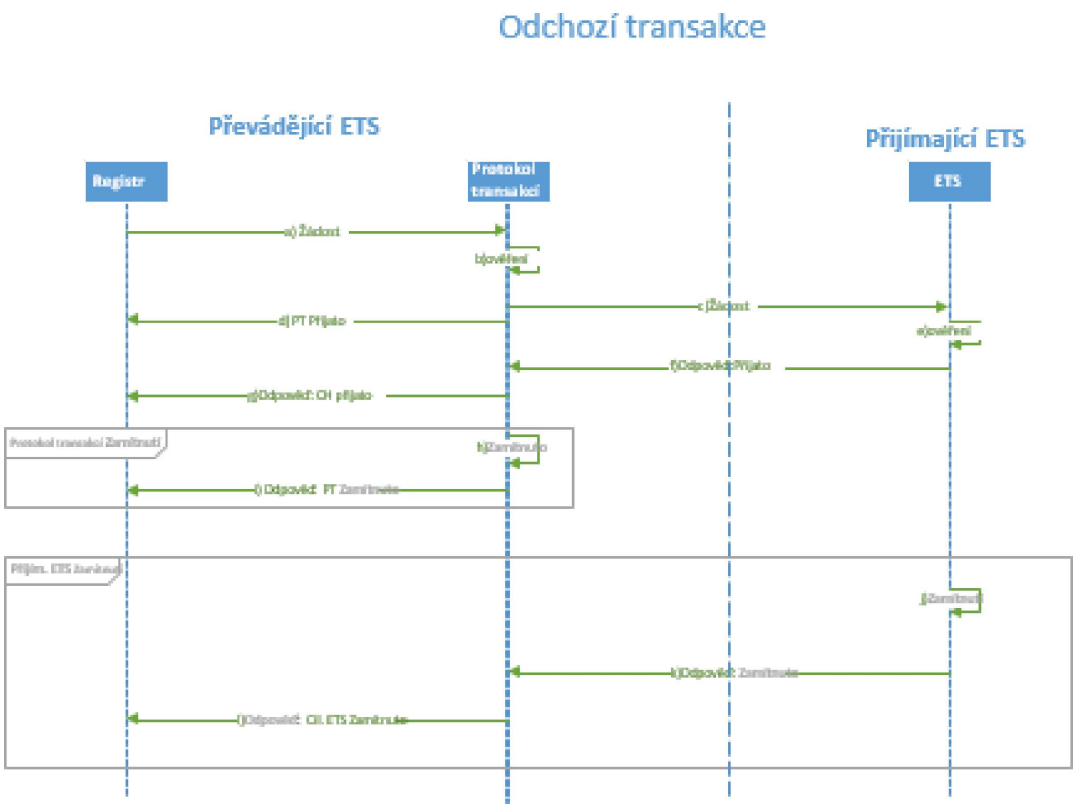
3.1.3 Okna pro příjem

Prozatímní řešení vychází z předem definovaných oken pro příjem, po nichž následuje skupina uvedených událostí. Žádosti o transakci obdržené přes propojení budou přijímány pouze v předem definovaných intervalech. Okna pro příjem zahrnují technické ověření odchozích a příchozích transakcí. Kromě toho může každý den probíhat sesouhlasení, které může být spuštěno manuálně.

Změny četnosti a/nebo načasování kterékoli z těchto událostí budou řešeny podle provozních postupů stanovených v procesu plnění žádostí, který je součástí společných provozních postupů.

3.1.4 Toky zpráv o transakcích

Odchozí transakce



Vyjádřeno je hledisko převádějícího systému ETS. Výše uvedený sekvenční diagram popisuje všechny specifické toky odchozích transakcí.

Hlavní tok „Normální transakce“ (s kroky uvedenými na obrázku výše):

a) v převádějícím systému ETS se žádost o transakci odešle po uplynutí všech obchodních zpoždění (24hodinového zpoždění v příslušných případech) z registru do protokolu transakcí;

b) protokol transakcí ověří žádost o transakci;

c) žádost o transakci se odešle do cílového systému ETS;

d) do registru výchozího systému ETS se zašle odpověď o přijetí;

e) cílový systém ETS ověří žádost o transakci;

f) cílový systém ETS zašle odpověď o přijetí zpět do protokolu transakcí výchozího systému ETS;

g) protokol transakcí zašle odpověď o přijetí do registru.

Alternativní tok „Zamítnutí v protokolu transakcí“ (s kroky uvedenými na obrázku výše, začíná se stejně od bodu a)):

a) ve výchozím systému ETS se žádost o transakci odešle po uplynutí všech obchodních zpoždění (24hodinového zpoždění v příslušných případech) z registru do protokolu transakcí.

Poté následuje:

b) protokol transakcí žádost neověří;

c) do výchozího registru se zašle odpověď o zamítnutí.

Alternativní tok „Zamítnutí v ETS“ (s kroky uvedenými na obrázku výše, začíná se od bodu a)):

a) ve výchozím systému ETS se žádost o transakci odešle po uplynutí všech obchodních zpoždění (24hodinového zpoždění v příslušných případech) z registru do protokolu transakcí;

b) protokol transakcí ověří transakci;

c) žádost o transakci se odešle do cílového systému ETS;

d) do registru výchozího systému ETS se zašle zpráva o přijetí.

Poté následuje:

e) protokol transakcí přijímajícího systému ETS žádost neověří;

f) přijímající systém ETS zašle odpověď o zamítnutí do protokolu transakcí převádějícího systému ETS;

g) protokol transakcí zašle zamítnutí do registru.

Příchozí transakce

Vyjádřeno je hledisko přijímajícího systému ETS. Konkrétní tok je zobrazen na následujícím sekvenčním diagramu:

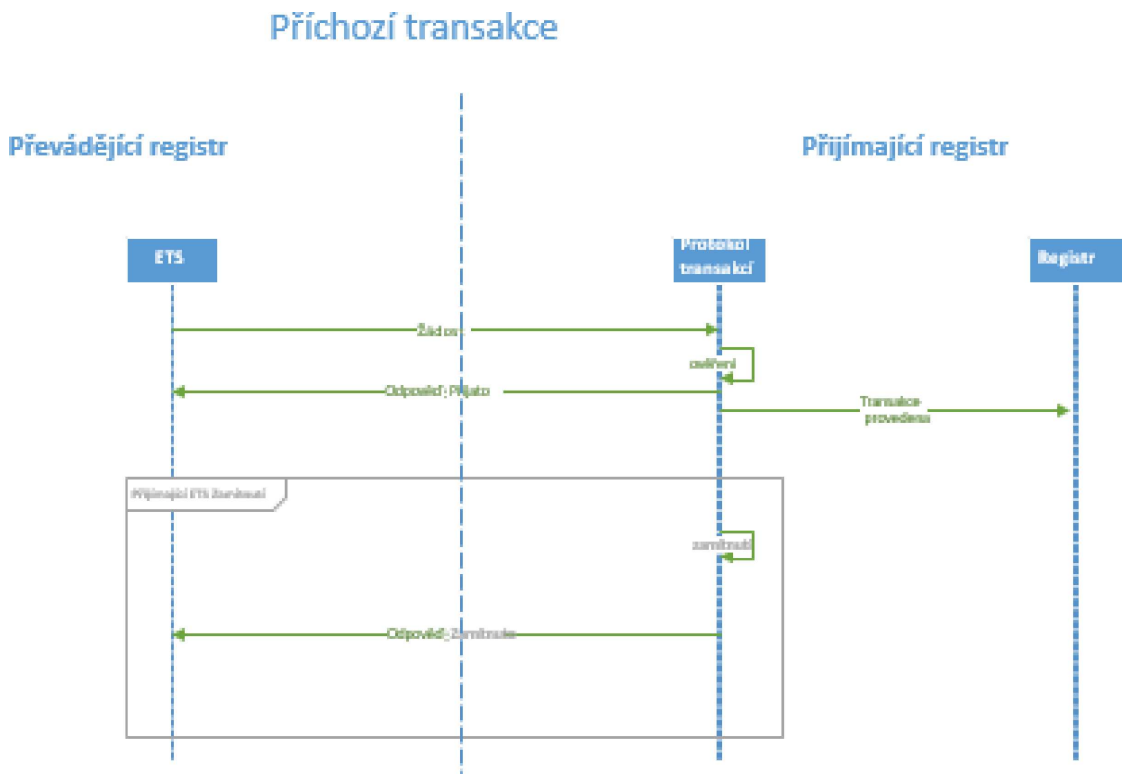


Diagram znázorňuje:

1. Když protokol transakcí přijímajícího systému ETS ověří žádost, zašle zprávu o přijetí do převádějícího systému ETS a zprávu „transakce provedena“ do registru přijímajícího systému ETS.

2. Když je v přijímajícím protokolu transakcí příchozí žádost zamítnuta, žádost o transakci se do registru přijímajícího systému ETS neodešle.

Protokol

Cyklus zpráv o transakci zahrnuje pouze dvě zprávy:

— převádějící systém ETS →návrh na transakci v přijímajícím systému ETS,

— přijímající systém ETS →odpověď na transakci v převádějícím systému ETS: Přijato nebo Zamítnuto (včetně důvodu zamítnutí).

  — datum: transakce je provedena.

  — Zamítnuto: transakce je zastavena.

Stav transakce

— stav transakce v převádějícím systému ETS bude při odeslání žádosti nastaven na „navrženo“,

— stav transakce v přijímajícím systému ETS bude při přijetí žádosti a během jejího zpracování nastaven na „navrženo“,

— stav transakce v přijímajícím systému ETS bude po zpracování žádosti nastaven na „provedeno“/„zastaveno“. Přijímající systém ETS poté odešle odpovídající zprávu o přijetí/zamítnutí,

— stav transakce v převádějícím systému ETS bude při přijetí a zpracování zprávy o přijetí/zamítnutí žádosti nastaven na „provedeno“/„zastaveno“,

— jestliže není přijata žádná odpověď, zůstane stav transakce v převádějícím systému ETS takový, jaký byl navržen,

— přijímající systém ETS nastaví každou transakci, která zůstane v navrženém stavu déle než 30 minut, na „zastaveno“.

Incidenty související s transakcemi budou řešeny podle provozních postupů stanovených v procesu řízení incidentů, který je součástí společných provozních postupů.

3.2 *Zabezpečení přenosu dat*

V průběhu přenosu budou data zabezpečena ve čtyřech úrovních:

1) řízení přístupu do sítě: Firewall a vrstva síťového propojení;

2) šifrování na úrovni přenosu: VPN nebo rovnocenná síť pro bezpečný přenos dat;

3) šifrování na úrovni relace: protokol pro bezpečný přenos zpráv;

4) šifrování na úrovni aplikace: šifrování a podpis obsahu XML.

3.2.1 Firewall a síťové propojení

Propojení se zřídí přes síť chráněnou hardwarovým firewallem. Firewall je konfigurován pomocí pravidel tak, že připojení na server VPN budou moci uskutečnit pouze „registrovaní“ klienti.

3.2.2 Virtuální soukromá síť (VPN)

Veškerá komunikace mezi stranami je chráněna s využitím technologie bezpečného přenosu dat. V případě virtuální soukromé sítě (VPN) by infrastruktura měla být založena na hardwaru nebo virtuálních zařízeních. Technologie VPN poskytují možnost „tunelování“ přes síť, jako je internet, z jednoho místa do druhého, přičemž veškerá komunikace je chráněna. Před vytvořením tunelu VPN je budoucímu koncovému bodu klienta vystaven digitální certifikát, který klientovi umožní prokázat při sjednávání spojení svou identitu. Každá strana je odpovědná za instalaci certifikátu do svého koncového bodu VPN. Digitální certifikáty bude každý koncový server VPN používat pro přístup do ústředního orgánu, aby si sjednal autentizační protokoly. V průběhu procesu vytváření tunelu se sjednává šifrování, což zajišťuje, že veškerá komunikace přes tunel bude chráněna.

Koncové body VPN klienta jsou konfigurovány tak, aby udržovaly tunel VPN trvale, aby byla vždy umožněna spolehlivá a oboustranná komunikace v reálném čase mezi stranami.

Jakékoli jiné rovnocenné řešení musí být v souladu s výše uvedenými zásadami.

3.2.3 Provádění IPSec

V případě použití řešení VPN zajistí používání protokolu IPSec k vytvoření infrastruktury VPN typu Site-to-Site ověření, integritu dat a šifrování dat typu Site-to-Site. Konfigurace IPSec VPN zajišťuje řádné ověření mezi dvěma koncovými body ve spojení VPN. Strany budou vzdáleného klienta identifikovat a ověřovat přes spojení IPSec pomocí digitálních certifikátů vydaných certifikačním orgánem uznávaným druhým koncovým bodem.

IPSec rovněž zajišťuje integritu dat při veškeré komunikaci procházející přes tunel VPN. Datové pakety se transformují a podepisují pomocí ověřovacích údajů vytvořených v síti VPN. Důvěrnost dat je zajištěna podobně umožněním šifrování IPSec.

3.2.4 Protokol pro bezpečný přenos zpráv

Prozatímní řešení používá pro bezpečnou výměnu dat mezi stranami několik šifrovacích vrstev. Oba systémy a jejich různá prostředí jsou propojeny na úrovni sítě pomocí tunelů VPN nebo rovnocenných sítí pro bezpečný přenos dat. Na úrovni aplikací jsou soubory přenášeny s využitím protokolu pro bezpečný přenos zpráv na úrovni relace.

3.2.5 Šifrování a podpis XML

V souborech XML probíhá podepisování a šifrování na dvou úrovních. Každá žádost o transakci, odpověď na transakci a sesouhlasovací zpráva se digitálně podepisuje jednotlivě.

V druhém kroku se jednotlivě šifruje každý dílčí prvek „zprávového“ prvku.

Navíc se digitálně podepisuje kořenový element zprávy jako třetí krok, což zajišťuje integritu a neodmítnutí celé zprávy. Výsledkem je vysoká úroveň ochrany vložených dat XML. Technické provedení je v souladu se standardy konsorcia World Wide Web.

Při dešifrování a ověřování zprávy probíhá tento proces v opačném pořadí.

3.2.6 Kryptografické klíče

Pro šifrování a podepisování se bude používat kryptografie s veřejným klíčem.

Ve zvláštním případě IPSec se používá digitální certifikát vydaný certifikačním orgánem, kterému obě strany důvěřují. Tento certifikační orgán ověřuje identitu držitele certifikátu a vydává certifikáty, které se používají pro pozitivní identifikaci organizace a nastavení komunikačních kanálů mezi stranami pro bezpečný přenos dat.

Kryptografické klíče se používají k podepisování a šifrování komunikačních kanálů a datových souborů. Veřejné certifikáty si strany digitálně vyměňují s využitím bezpečných kanálů a ověřují se mimo IP síť. Tento postup je nedílnou součástí procesu řízení bezpečnosti informačních systémů v rámci společných provozních postupů.

3.3 *Seznam funkcí v rámci propojení*

Propojení určí přenosový systém pro sérii funkcí, které provádějí obchodní procesy vycházející z dohody. Propojení zahrnuje také určení procesu sesouhlasení a zkušebních zpráv, což umožní provádět monitorování prezenčního signálu.

3.3.1 Obchodní transakce

Z obchodního hlediska jsou v propojení uvažovány čtyři (4) druhy žádostí o transakci:

— vnější převod:

  — jakmile vstoupí v platnost propojení systémů ETS, jsou unijní a švýcarské povolenky mezi stranami zaměnitelné, a tedy i plně převoditelné,

— převod odeslaný přes propojení bude zahrnovat převádějící účet v jednom systému ETS a přijímající účet v druhém systému ETS,

— převod může zahrnovat jakékoli množství čtyř (4) druhů povolenek:

— švýcarské všeobecné povolenky (CHU),

— švýcarské povolenky pro letectví (CHUA),

— všeobecné povolenky EU (EUA),

— povolenky EU pro letectví (EUAA),

— mezinárodní přidělování:

provozovatelé letadel spravovaní jedním systémem ETS s povinnostmi v druhém systému ETS, kteří mají nárok na bezplatné povolenky od tohoto druhého systému ETS, obdrží bezplatné povolenky pro letectví od druhého systému ETS prostřednictvím transakce mezinárodního přidělení,

— zrušení mezinárodního přidělení:

k této transakci dojde v případě, že všechny bezplatné povolenky přidělené na vkladní účet provozovatele letadla druhým systémem ETS musí být zrušeny,

— vrácení nadměrného přídělu:

podobně jako u zrušení, ale v případě, že není třeba rušit celý příděl, a do přidělujícího systému ETS je třeba vrátit pouze nadměrně přidělené povolenky.

3.3.2 Protokol sesouhlasení

K sesouhlasení dochází až poté, co jsou uzavřena okna pro příjem zpráv, jejich ověření a zpracování.

Sesouhlasení je nedílnou součástí bezpečnostních opatření a zachování konzistentnosti v rámci propojení. Obě strany se před vytvořením jakéhokoli plánu dohodnou na přesném načasování sesouhlasení. Denní plánované sesouhlasení může probíhat, pokud je dohodnuto oběma stranami. Po každém přijetí bude provedeno alespoň jedno plánované sesouhlasení.

Každá strana může kdykoli zahájit manuální odsouhlasení.

Změny načasování a četnosti plánovaného sesouhlasení budou řešeny podle provozních postupů stanovených v procesu plnění žádostí, který je součástí společných provozních postupů.

3.3.3 Testovací zpráva

Testovací zpráva je určena pro testování komunikace mezi koncovými body. Tato zpráva bude obsahovat údaje, které tuto zprávu identifikují jako testovací, a bude zodpovězena po přijetí druhým koncovým bodem.

3.4 *Standardy pro webové služby*

Webové služby nebudou v prozatímním řešení používány. Je však vhodné poznamenat, že forma a formát zpráv XML zůstanou do značné míry nezměněny. Po zavedení stálého propojení registrů v budoucnosti by webové služby měly umožňovat výměnu zpráv XML v reálném čase.

3.5 *Specifická definice webových služeb*

Tento oddíl neplatí pro prozatímní řešení. Jak již bylo uvedeno v předchozím oddíle, budou webové služby používány až v budoucím trvalém propojení registrů.

3.6 *Požadavky na evidenci údajů*

S cílem podpořit obě strany, aby vedly přesné a konzistentní údaje, a poskytnout nástroje pro použití při procesu sesouhlasení při řešení nesrovnalostí povedou obě strany čtyři (4) druhy datové evidence:

— protokoly transakcí,

— protokoly sesouhlasení,

— archiv zpráv,

— protokoly interního auditu.

Všechny údaje v těchto protokolech se uchovávají alespoň po dobu tří (3) měsíců pro účely řešení problémů, přičemž jejich další uchovávání bude záviset na platných právních předpisech v každém koncovém bodě pro účely kontroly. Soubory protokolů starší tří (3) měsíců mohou být archivovány na bezpečném místě v nezávislém IT systému, pokud je bude možné stáhnout nebo k nim získat přístup v přiměřené lhůtě.

Protokoly transakcí

V subsystémech EUTL a SSTL jsou implementovány protokoly transakcí.

Konkrétně se v protokolech transakcí povede záznam o každé navržené transakci zaslané do druhého systému ETS. Každý záznam obsahuje všechna pole s obsahem transakce a následný výsledek této transakce (odpověď přijímajícího systému ETS). V protokolech transakcí se také povede záznam o příchozích transakcích a odpovědích zaslaných do výchozího systému ETS.

Protokoly sesouhlasení

Protokol sesouhlasení obsahuje záznam každé zprávy o sesouhlasení, kterou si obě strany vyměnily, včetně identifikace sesouhlasení, časového razítka a výsledku sesouhlasení: Stav sesouhlasení „Schváleno“ nebo „Nesrovnalosti“. V prozatímním řešení jsou zprávy o sesouhlasení nedílnou součástí vyměňovaných zpráv.

Obě strany evidují každou žádost a odpověď na ni v protokolu sesouhlasení. Přestože se údaje z protokolu sesouhlasení nesdílejí přímo v rámci sesouhlasení samotného, může být přístup k těmto údajům nezbytný pro účely řešení nesrovnalostí.

Archiv zpráv

Je třeba, aby obě strany archivovaly kopii vyměňovaných dat (soubory XML), zaslaných i přijatých, a to bez ohledu na to, zda tato data nebo zprávy XML byly ve správném formátu.

Hlavním účelem archivace je mít pro kontrolu důkaz o tom, co bylo odesláno druhé straně a přijato od druhé strany. V tomto smyslu je třeba společně se soubory archivovat také příslušné certifikáty.

Tyto soubory budou také poskytovat další informace pro řešení problémů.

Protokol interního auditu

Tyto protokoly si každá strana definuje a používá sama.

3.7 *Provozní požadavky*

Výměna dat mezi oběma systémy není v prozatímním řešení zcela autonomní, což znamená, že zprovoznění propojení vyžaduje operátory a postupy.

4. **Ustanovení o dostupnosti**

4.1 *Návrh dostupnosti komunikace*

Architektura prozatímního řešení je v podstatě IKT infrastruktura a software, který umožňuje komunikaci mezi systémem ETS Švýcarska a systémem EU ETS. Proto se zajištění vysoké úrovně dostupnosti, integrity a důvěrnosti toku těchto dat stává zásadním aspektem, který je třeba zvažovat při návrhu prozatímního řešení i trvalého propojení registrů. Protože jde o projekt, v němž hraje hlavní roli IKT infrastruktura, software a procesy na zakázku, je třeba vzít všechny tyto tři prvky v úvahu, aby bylo možné navrhnout odolný systém.

Odolnost IKT infrastruktury

Stavební bloky architektury jsou popsány v kapitole týkající se obecných ustanovení. Pokud jde o IKT infrastrukturu, prozatímní propojení zřizuje odolnou VPN síť (nebo ekvivalentní síť), která vytváří bezpečné komunikační tunely, jimiž může probíhat bezpečná výměna zpráv. Jiné prvky infrastruktury jsou konfigurovány na vysokou dostupnost a/nebo spoléhají na nouzové mechanismy.

Odolnost softwaru na zakázku

Softwarové moduly vyvinuté na zakázku zvyšují odolnost opakovanými pokusy o komunikaci s druhým koncovým bodem po danou dobu, pokud z nějakého důvodu není dostupný.

Odolnost služeb

V prozatímním řešení dochází k výměně dat mezi stranami v předem definovaných vysílacích časech v průběhu celého roku. Některé z kroků potřebných pro plánované výměny dat vyžadují manuální zásah systémových operátorů a/nebo správců registru. Vzhledem k tomu a za účelem zvýšení dostupnosti a úspěšnosti výměn:

— provozní postupy předpokládají značná časová okna na provedení každého kroku,

— v softwarových modulech pro prozatímní řešení je implementována asynchronní komunikace,

— automatický proces sesouhlasení detekuje, zda při příjmu datových souborů na kterémkoli konci došlo k problémům,

— jsou zapojeny monitorovací procesy (IKT infrastruktura a softwarové moduly na zakázku), které spouštějí postupy řízení incidentů (podle definice v dokumentu o společných provozních postupech). Tyto postupy, jejichž cílem je zkrácení času do obnovení normálního provozu po incidentech, jsou zásadní pro zajištění vysoké míry dostupnosti.

4.2 *Inicializace, komunikace, reaktivace a plán testování*

Všechny různé prvky zapojené do architektury prozatímního řešení procházejí sérií individuálních a kolektivních testů, aby bylo potvrzeno, že platforma je na úrovni IKT infrastruktury a informačního systému připravena. Tyto provozní testy jsou povinnou podmínkou pokaždé, když se v platformě převádí prozatímní řešení z pozastaveného do provozního stavu.

Aktivace propojení do provozního stavu poté vyžaduje úspěšné provedení předem definovaného testovacího plánu. To potvrdí, že každý registr nejprve provedl skupinu interních testů, po nichž následovalo ověření spojení mezi koncovými body předtím, než začne nabídka produkčních transakcí mezi oběma stranami.

V testovacím plánu by měla být uvedena celková strategie testování a podrobnosti o testovací infrastruktuře. Každý prvek v každém testovacím bloku by měl konkrétně zahrnovat:

— kritéria a nástroje pro testování,

— role přiřazené k provedení testu,

— očekávané výsledky (pozitivní i negativní),

— časový rozvrh testu,

— záznam požadavku na výsledky testu,

— dokumentaci pro řešení problémů,

— ustanovení o eskalaci.

Aktivační testy provozního stavu by jako proces mohly být rozděleny do čtyř (4) koncepčních bloků nebo fází:

4.2.1 Interní testy IKT infrastruktury

Tyto testy mají být prováděny a/nebo kontrolovány individuálně oběma stranami na každém konci.

Každý prvek IKT infrastruktury na každém konci se testuje individuálně. Zahrnuje to každý jednotlivý komponent infrastruktury. Tyto testy mohou být prováděny automaticky nebo manuálně, ale musí ověřit, že každý prvek infrastruktury je funkční.

4.2.2 Testy komunikace

Tyto testy zahajuje každá strana individuálně, přičemž jejich dokončení vyžaduje spolupráci s druhým koncem.

Jakmile jsou jednotlivé prvky funkční, je třeba otestovat komunikační kanály mezi oběma registry. Za tímto účelem každá strana ověří, že funguje přístup k internetu, že jsou vytvořeny VPN tunely (nebo rovnocenná bezpečná přenosová síť) a že je mezi oběma místy IP spojení. Poté je třeba na druhém konci potvrdit dosažitelnost lokálních i vzdálených prvků infrastruktury a IP spojení.

4.2.3 Testy celého systému (end-to-end)

Tyto testy mají být provedeny na obou koncích a výsledky sděleny druhé straně.

Po otestování komunikačních kanálů a všech jednotlivých komponentů obou registrů připraví každý konec sérii simulovaných transakcí a sesouhlasení vyjadřujících všechny funkce, jež mají být v propojení implementovány.

4.2.4 Bezpečnostní testy

Tyto testy mají být prováděny a/nebo spouštěny oběma stranami na každém konci, jak je popsáno v oddílech 5.4 „Pokyny pro testování bezpečnosti“ a 5.5 „Ustanovení o posouzení rizik“.

Až když každá ze čtyř fází/bloků skončí s předvídatelnými výsledky, může být prozatímní propojení považováno za zprovozněné.

Zdroje pro testování

Každá strana bude používat zvláštní zdroje pro testování (zvláštní IKT infrastrukturu, software a hardware) a vytvoří si ve svém příslušném systému testovací funkce, které budou podporovat manuální a kontinuální ověřování platformy. Správci registrů mohou kdykoli realizovat manuální individuální nebo společné testovací postupy. Aktivace provozního stavu je sama o sobě manuální proces.

Je rovněž stanoveno, že platforma v pravidelných intervalech provádí automatické kontroly. Cílem těchto kontrol je zvýšit dostupnost platformy včasným detekováním potenciálních problémů v oblasti infrastruktury nebo softwaru. Tento plán monitorování platformy se skládá ze dvou prvků:

— monitorování IKT infrastruktury: infrastruktura bude na obou koncích monitorována poskytovateli služeb pro IKT infrastrukturu. Automatické testy budou zahrnovat různé prvky infrastruktury a dostupnost komunikačních kanálů,

— monitorování aplikací: v softwarových modulech prozatímního propojení bude implementováno monitorování systémové komunikace na úrovni aplikací (manuálně a/nebo v pravidelných intervalech), které bude testovat dostupnost propojení mezi oběma konci simulováním některých transakcí přes propojení.

4.3 *Schvalovací/testovací prostředí*

Architektura registru Unie a registru Švýcarska sestává z těchto tří prostředí:

— produkce (PROD): v tomto prostředí jsou skutečné údaje a zpracovávají se v něm skutečné transakce,

— schvalování (ACC): toto prostředí obsahuje údaje, které nejsou skutečné nebo jsou anonymizované či reprezentativní. Je to prostředí, kde operátoři systémů obou stran ověřují nové verze,

— testování (TEST): toto prostředí obsahuje údaje, které nejsou skutečné nebo jsou anonymizované či reprezentativní. Toto prostředí je omezeno na správce registrů a má být používáno k provádění integračních testů oběma stranami.

S výjimkou VPN (nebo rovnocenné sítě) jsou tato tři prostředí na sobě zcela nezávislá, což znamená, že hardware, software, databáze, virtuální prostředí, IP adresy a porty se nastavují a provozují nezávisle na sobě.

Pokud jde o strukturu VPN, nastavuje se ve dvou různých prostředích, v jednom pro PROD a v dalším nezávislém pro ACC a TEST.

5. **Ustanovení o důvěrnosti a integritě**

Bezpečnostní mechanismy a postupy stanovují u operací probíhajících v propojení mezi registrem Unie a švýcarským registrem metodu dvou osob (zásada čtyř očí). Metoda dvou osob se uplatní vždy, když je to potřebné. Je však možné, že se nepoužije u všech kroků prováděných správci registrů.

Bezpečnostní požadavky jsou rozebrány a řešeny v plánu pro řízení bezpečnosti, který zahrnuje rovněž procesy týkající se řešení bezpečnostních incidentů po případném narušení bezpečnosti. Provozní část těchto procesů je popsána ve společných provozních postupech.

5.1 *Infrastruktura pro testování bezpečnosti*

Každá strana se zavazuje vytvořit infrastrukturu pro testování bezpečnosti (s využitím společné sady softwaru a hardwaru, který se používá pro detekci slabých stránek ve vývojové a provozní fázi):

— odděleně od produkčního prostředí,

— kde bezpečnost analyzuje tým nezávislý na vývoji a provozu systému.

Každá strana provádí statickou a dynamickou analýzu.

V případě dynamické analýzy (jako je penetrační testování) obě strany omezí hodnocení zpravidla na testovací a schvalovací prostředí (podle definice v oddíle 4.3 „Schvalovací/testovací prostředí“). Výjimky z této zásady podléhají schválení oběma stranami.

Před zavedením do produkčního prostředí se každý softwarový modul spojení (podle definice v oddíle 3.1 „Architektura komunikačního propojení“) otestuje na bezpečnost.

Testovací infrastruktura musí být oddělena na úrovni sítě i infrastruktury od produkční infrastruktury. V testovací infrastruktuře se provádějí bezpečnostní testy potřebné ke kontrole souladu s bezpečnostními požadavky.

5.2 *Ustanovení o pozastavení propojení a jeho reaktivaci*

Existuje-li podezření, že zabezpečení registru Švýcarska, SSTL, registru Unie nebo EUTL bylo ohroženo, každá strana neprodleně informuje druhou stranu a propojení mezi SSTL a EUTL pozastaví.

Postupy pro sdílení informací, rozhodnutí o pozastavení a rozhodnutí o reaktivaci jsou součástí procesu plnění žádostí v rámci společných provozních postupů.

Pozastavení

K pozastavení propojení registrů v souladu s přílohou II dohody může dojít v důsledku:

— administrativních důvodů (např. údržby), které jsou plánované,

— bezpečnostních důvodů (nebo poruch IT infrastruktury), které jsou neplánované.

V případě mimořádné situace každá strana informuje druhou stranu a jednostranně pozastaví propojení registrů.

Jestliže je přijato rozhodnutí o pozastavení propojení registrů, každá strana zajistí, aby bylo propojení přerušeno na úrovni sítě (zablokováním částí nebo všech příchozích a odchozích spojení).

Rozhodnutí pozastavit propojení registrů, ať už plánované či neplánované, bude přijato podle postupu řízení změn nebo postupu řízení bezpečnostních incidentů uvedených ve společných provozních postupech.

Reaktivace komunikace

Rozhodnutí o reaktivaci propojení registrů bude přijato způsobem popsaným ve společných provozních postupech a v každém případě až po úspěšném provedení bezpečnostního testování, jak je popsáno v oddílech 5.4 „Pokyny pro testování bezpečnosti“ a 4.2 „Inicializace, komunikace, reaktivace a plán testování“.

5.3 *Ustanovení o narušení bezpečnosti*

Narušení bezpečnosti se považuje za bezpečnostní incident s dopadem na důvěrnost a integritu jakýchkoli citlivých informací a/nebo dostupnost systému pro nakládání s nimi.

Citlivé informace jsou označeny v seznamu citlivých informací a mohou být zpracovávány v systému nebo v jakékoli související části systému.

Informace přímo související s narušením bezpečnosti budou považovány za citlivé, označeny za „ETS KRITICKÉ“ a bude s nimi zacházeno podle pokynů pro nakládání, pokud není uvedeno jinak.

Každé narušení bezpečnosti bude řešeno podle kapitoly o řízení bezpečnostních incidentů ve společných provozních postupech.

5.4 *Pokyny pro testování bezpečnosti*

5.4.1 Software

V rámci veškerých nových vydání důležitého softwaru se provede testování bezpečnosti, v příslušných případech včetně penetračního testování, a to v souladu s bezpečnostními požadavky stanovenými v technických normách pro propojování, aby bylo možné posoudit bezpečnost propojení a související rizika.

Pokud v posledních 12 měsících nedošlo k vydání žádného důležitého softwaru, provede se testování bezpečnosti na stávajícím systému se zohledněním vývoje kybernetických hrozeb, k němuž v posledních 12 měsících došlo.

Testování bezpečnosti propojení registrů se provede ve schvalovacím prostředí a v případě potřeby v produkčním prostředí, a to s koordinací a po vzájemné dohodě obou stran.

Při testování webových aplikací budou dodržovány otevřené mezinárodní normy, jako jsou standardy vyvinuté projektem Bezpečnost otevřených webových aplikací (OWASP).

5.4.2 Infrastruktura

Infrastruktura podporující produkční systém je pravidelně prověřována na slabá místa (alespoň jednou měsíčně) a zjištěná slabá místa se opraví. Testování se provádí metodou uvedenou v oddíle 5.4.1 s využitím aktuální databáze slabých míst.

5.5 *Ustanovení o posouzení rizik*

Je-li použitelné testování penetrace, musí být zařazeno do testování bezpečnosti.

Každá strana si může na provedení testování bezpečnosti sjednat specializovanou společnost, pokud tato společnost:

— má s takovým testováním bezpečnosti dovednosti a zkušenosti,

— není podřízena přímo vývojáři ani jeho dodavateli a není zapojena do vývoje softwaru propojení a není ani dodavatelem vývojáře,

— uzavřela dohodu o mlčenlivosti, aby výsledky zůstaly důvěrné a aby se s nimi v souladu s pokyny pro nakládání zacházelo jako s „ETS KRITICKÝMI“.