EVROPSKÁ
KOMISE

V Bruselu dne 20.3.2024
COM(2024) 125 final

ANNEX

PŘÍLOHA

návrhu rozhodnutí Rady

o postoji, který má být zaujat jménem Evropské unie ve smíšeném výboru zřízeném Dohodou mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů, pokud jde o změnu přílohy II dohody, společných provozních postupů a technických norem pro propojování

ROZHODNUTÍ č. 1/2024 SMÍŠENÉHO VÝBORU ZŘÍZENÉHO DOHODOU MEZI EVROPSKOU UNIÍ A ŠVÝCARSKOU KONFEDERACÍ O PROPOJENÍ JEJICH SYSTÉMŮ OBCHODOVÁNÍ S EMISEMI SKLENÍKOVÝCH PLYNŮ
ze dne ...,
pokud jde o změnu přílohy II dohody, společných provozních postupů a technických norem pro propojování

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 článek 9 a čl. 13 odst. 2 této dohody,

vzhledem k těmto důvodům:

(1) Rozhodnutí smíšeného výboru č. 2/2019[2] stanovilo prozatímní řešení pro zprovoznění propojení mezi systémem EU ETS a ETS Švýcarska.

(2) Smíšený výbor se na svém třetím zasedání dohodl na tom, že je třeba analyzovat nákladovou efektivnost trvalého propojení mezi registrem Unie a registrem Švýcarska.

(3) Smíšený výbor na svém pátém zasedání schválil zprávu předloženou pracovní skupinou zřízenou rozhodnutím smíšeného výboru č. 1/2020[3] a č. 2/2020[4], v níž tato pracovní skupina analyzovala a doporučila přístup k provádění trvalého propojení mezi registrem Unie a registrem Švýcarska.

(4) Aby se zohlednily technické požadavky trvalého propojení mezi registrem Unie a registrem Švýcarska a zefektivnila ustanovení přílohy II dohody s ohledem na technologický vývoj, měla by být příloha II dohody změněna.

(5) Aby byl zajištěn soulad společných provozních postupů a technických norem pro propojování s přílohou II dohody, měly by být uvedené dokumenty rovněž změněny,

PŘIJAL TOTO ROZHODNUTÍ:

Článek 1

1. Příloha II dohody se nahrazuje zněním v příloze I tohoto rozhodnutí.

2. Společné provozní postupy uvedené v čl. 3 odst. 6 dohody jsou stanoveny v příloze II tohoto rozhodnutí.

3. Technické normy pro propojování uvedené v čl. 3 odst. 7 dohody jsou stanoveny v příloze III tohoto rozhodnutí.

Článek 2

Toto rozhodnutí vstupuje v platnost dnem přijetí.

Vyhotoveno v angličtině dne [xx 2024] v [Bruselu][Bernu].

[1] Úř. věst. L 322, 7.12.2017, s. 3.
[2] Úř. věst. L 314, 29.9.2020, s. 68.
[3] Úř. věst. L 226, 25.6.2021, s. 2.
[4] Úř. věst. L 226, 25.6.2021, s. 16.

Za smíšený výbor

tajemník/tajemnice za Evropskou unii	*předseda/předsedkyně*	*tajemník/tajemnice za Švýcarsko*

PŘÍLOHA I

„PŘÍLOHA II

TECHNICKÉ NORMY PRO PROPOJOVÁNÍ

S cílem zprovoznit propojení mezi systémem EU ETS a ETS Švýcarska bylo v roce 2020 zavedeno prozatímní řešení. Od roku 2023 se propojení registrů mezi oběma systémy obchodování s emisemi bude postupně vyvíjet směrem k trvalému propojení registrů, jež by mělo být realizováno nejpozději v roce 2024, což umožní fungování propojených trhů, pokud jde o výhody z tržní likvidity a provádění transakcí mezi oběma propojenými systémy způsobem, který je rovnocenný jednomu trhu tvořenému dvěma systémy a který účastníkům trhu umožňuje jednat, jako by byli na jednom trhu, s výhradou pouze jednotlivých regulačních ustanovení stran. Technické normy pro propojování stanoví:

– architekturu komunikačního propojení,

– komunikaci mezi protokoly transakcí SSTL a EUTL,

– zabezpečení přenosu dat,

– seznam funkcí (transakce, sesouhlasení …),

– definici transportní vrstvy,

– požadavky na vedení protokolů,

– provozní opatření (telefonická linka, podpora),

– plán pro aktivaci komunikace a testovací postup,

– postup pro ověřování bezpečnosti.

Technické normy pro propojování stanoví, že správci přijmou veškerá přiměřená opatření k zajištění toho, že SSTL, EUTL a propojení jsou provozuschopné dvacet čtyři hodin denně sedm dní v týdnu a že přerušení provozu SSTL, EUTL a propojení jsou omezena na minimum.

Technické normy pro propojování stanoví dodatečné bezpečnostní požadavky pro švýcarský registr, SSTL, registr Unie a EUTL a zdokumentuje je v „plánu pro řízení bezpečnosti“. Technické normy pro propojování konkrétně uvedou, že:

– existuje-li podezření, že zabezpečení švýcarského registru, SSTL, registru Unie nebo EUTL bylo ohroženo, obě strany se neprodleně vzájemně informují a pozastaví propojení mezi SSTL a EUTL,

– v případě narušení bezpečnosti se strany zavazují, že budou bezodkladně vzájemně sdílet informace. V rozsahu, v jakém jsou dostupné technické podrobnosti, správce švýcarského registru a ústřední správce Unie vzájemně sdílí zprávu popisující daný incident (datum, příčina, dopad, opravné prostředky), a to do 24 hodin poté, co je bezpečnostní incident identifikován jako narušení bezpečnosti.

Postup pro ověřování bezpečnosti stanovený v technických normách pro propojování musí být dokončen předtím, než je zřízeno komunikační propojení mezi SSTL a EUTL a když je nutná nová verze nebo vydání SSTL nebo EUTL.

Technické normy pro propojování kromě prostředí produkce poskytnou také dvě testovací prostředí: prostředí pro testování vývojářů a prostředí akceptace.

Strany prostřednictvím správce švýcarského registru a ústředního správce Unie poskytnou důkazy, že v předchozích dvanácti měsících bylo provedeno nezávislé hodnocení zabezpečení jejich systémů v souladu s bezpečnostními požadavky stanovenými v technických normách pro propojování. V rámci veškerých nových vydání důležitého softwaru se provede ověřování bezpečnosti a zejména penetrační testování, a to v souladu s bezpečnostními požadavky stanovenými v technických normách pro propojování. Penetrační testování nesmí být prováděno vývojářem softwaru ani subdodavatelem vývojáře softwaru.“

PŘÍLOHA II

SPOLEČNÉ PROVOZNÍ POSTUPY

podle čl. 3 odst. 6 Dohody mezi Evropskou unií a Švýcarskou konfederací o propojení jejich systémů obchodování s emisemi skleníkových plynů

Postupy pro trvalé propojení registrů

Obsah

1. Glosář 10
2. Úvod 11
2.1. Oblast působnosti 11
2.2. Určení 12
3. Přístup a standardy 12
4. Řízení incidentů 13
4.1. Zjištění a záznam incidentu 13
4.2. Klasifikace a počáteční podpora 13
4.3. Šetření a diagnostika 14
4.4. Vyřešení a obnova 14
4.5. Uzavření incidentu 14
5. Řízení problémů 15
5.1. Identifikace a záznam problému 15
5.2. Stanovení priority problému 15
5.3. Šetření a diagnostika problémů 15
5.4. Vyřešení 15
5.5. Uzavření problému 15
6. Plnění žádostí 15
6.1. Iniciování žádosti 16
6.2. Registrování a analýza žádosti 16
6.3. Schválení žádosti 16
6.4. Plnění žádosti 16
6.5. Eskalace žádosti 16
6.6. Kontrola splnění žádosti 16
6.7. Uzavření žádosti 17
7. Řízení změn 18
7.1. Žádost o změnu 18

7.2. Hodnocení a plánování změn 18
7.3. Schválení změny 18
7.4. Provedení změny 18
8. Řízení vydání 18
8.1. Plánování vydání 19
8.2. Vytvoření a otestování balíčku vydání 19
8.3. Příprava na zprovoznění 19
8.4. Návrat do původního stavu 20
8.5. Kontrola a uzavření vydání 20
9. Řízení bezpečnostních incidentů 20
9.1. Kategorizace incidentů v oblasti bezpečnosti informací 20
9.2. Řešení incidentů v oblasti bezpečnosti informací 21
9.3. Identifikace bezpečnostních incidentů 21
9.4. Analýza bezpečnostních incidentů 21
9.5. Posouzení závažnosti bezpečnostního incidentu, eskalace a podávání zpráv 21
9.6. Podávání zpráv o reakcích v oblasti bezpečnosti 21
9.7. Monitorování, budování kapacit a průběžné zdokonalování 22
10. Řízení bezpečnosti informací 22
10.1. Identifikace citlivých informací 22
10.2. Úrovně citlivosti informačních aktiv 22
10.3. Přiřazení vlastníka informačních aktiv 22
10.4. Registrace citlivých informací 23
10.5. Nakládání s citlivými informacemi 23
10.6. Řízení přístupu 23
10.7. Správa certifikátů/klíčů 24
1. Glosář 27
2. Úvod 30
2.1. Oblast působnosti 30
2.2. Určení 31
3. Obecná ustanovení 31
3.1. Architektura komunikačního propojení 31
3.1.1. Výměna zpráv 31
3.1.2. Zpráva XML – podrobný popis 31

3.1.3. Okna pro příjem 31
3.1.4. Toky zpráv o transakcích 32
3.2. Zabezpečení přenosu dat 35
3.2.1. Firewall a síťové propojení 35
3.2.2. Virtuální privátní síť (VPN) 35
3.2.3. Provádění IPSec 35
3.2.4. Protokol pro bezpečný přenos zpráv. 36
3.2.5. Šifrování a podpis XML 36
3.2.6. Kryptografické klíče 36
3.3. Seznam funkcí v rámci propojení 36
3.3.1. Obchodní transakce 36
3.3.2. Protokol sesouhlasení 37
3.3.3. Testovací zpráva 37
3.4. Požadavky na vedení protokolů 37
3.5. Provozní požadavky 38
4. Ustanovení o dostupnosti 39
4.1. Návrh dostupnosti komunikace 39
4.2. Inicializace, reaktivace komunikace a plán testování 39
4.2.1. Interní testy IKT infrastruktury 40
4.2.2. Testy komunikace 40
4.2.3. Testy celého systému (end-to-end) 40
4.2.4. Bezpečnostní testy 40
4.3. Akceptační/testovací prostředí 41
5. Ustanovení o důvěrnosti a integritě 41
5.1. Infrastruktura pro testování bezpečnosti 41
5.2. Ustanovení o pozastavení propojení a jeho reaktivaci 42
5.3. Ustanovení o narušení bezpečnosti 42
5.4. Pokyny pro testování bezpečnosti 43
5.4.1. Software 43
5.4.2. Infrastruktura 43
5.5. Ustanovení o posouzení rizik 43

1. GLOSÁŘ

Tabulka 1-1 Zkratky a definice

Zkratka/výraz	Definice
Certifikační orgán	Subjekt, který vydává digitální certifikáty
CH	Švýcarská konfederace
ETS	Systém obchodování s emisemi
EU	Evropská unie
IMT	Tým pro řízení incidentů
Informační aktivum	Informace, která je cenná pro společnost nebo organizaci
IT	Informační technologie
ITIL	Knihovna infrastruktury informačních technologií (*Information Technology Infrastructure Library*)
ITSM	Řízení IT služeb
LTS	Technické normy pro propojování
Registr	Účetní systém pro povolenky vydané v rámci systému obchodování s emisemi, který sleduje vlastnictví povolenek vedených na elektronických účtech.
RFC	Žádost o změnu
SIL	Seznam citlivých informací
SR	Žádost o službu
Wiki	Webové stránky, které umožňují uživatelům vyměňovat si informace a znalosti přidáváním nebo úpravou obsahu přímo přes webový prohlížeč.

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 „EU ETS“) nebo v rámci systému obchodování s emisemi Švýcarska (dále jen „ETS Švýcarska“). Aby bylo možné zprovoznit propojení mezi EU ETS a ETS Švýcarska, 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). S cílem zprovoznit propojení mezi systémem EU ETS a ETS Švýcarska bylo v roce 2020 zavedeno prozatímní řešení. Od roku 2023 se propojení registrů mezi oběma systémy obchodování s emisemi bude postupně vyvíjet směrem k trvalému propojení registrů, jež by mělo být realizováno nejpozději v roce 2024, což umožní fungování propojených trhů, pokud jde o výhody z tržní likvidity a provádění transakcí mezi oběma propojenými systémy způsobem, který je rovnocenný jednomu trhu tvořenému dvěma systémy a který účastníkům trhu umožňuje jednat, jako by byli na jednom trhu, s výhradou pouze jednotlivých regulačních ustanovení stran. (Příloha II dohody)

Podle čl. 3 odst. 6 dohody správce švýcarského registru a ústřední správce Unie určí společné provozní postupy týkající se technických nebo jiných záležitostí nezbytných pro fungování propojení a zohlední priority vnitrostátních právních předpisů. Společné provozní postupy vypracované správci nabývají účinnosti poté, co byly přijaty rozhodnutím smíšeného výboru.

Společné provozní postupy byly přijaty smíšeným výborem rozhodnutím č. 1/2020. Aktualizované společné provozní postupy zaznamenané v tomto dokumentu přijme smíšený výbor svým rozhodnutím č. 1/2024. V souladu s tímto rozhodnutím a žádostmi smíšeného výboru správce švýcarského registru a ústřední správce Unie vypracovali a budou aktualizovat další technické pokyny, aby mohlo dojít ke zprovoznění propojení a bylo zajištěno průběžné přizpůsobování uvedených pokynů 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 procedurálních základů propojení mezi registry EU ETS a ETS Švýcarska. Přestože nastiňuje celkové procedurální náležitosti z hlediska fungování, budou potřebné i některé další technické pokyny, aby bylo možné propojení zprovoznit.

Ke správnému fungování bude propojení vyžadovat technické specifikace, aby bylo možné zajistit jeho pokračující zprovozňování. Podle čl. 3 odst. 7 dohody jsou tyto záležitosti podrobně popsány v dokumentu obsahujícím technické normy pro propojování, který má být přijat samostatným rozhodnutím smíšeného výboru.

Cílem společných provozních postupů je zajistit, aby byly IT služby související s provozem propojení mezi registry EU ETS a ETS Švýcarska poskytovány účelně a efektivně, zejména při plnění žádostí o službu, řešení selhání služby, odstraňování problémů, jakož i při provádění rutinních provozních úkolů podle mezinárodních standardů pro řízení IT služeb.

Pro trvalé propojení registrů budou potřebné pouze tyto společné provozní postupy, které jsou součástí tohoto dokumentu:

- řízení incidentů,
- řízení problémů,
- plnění žádostí,
- řízení změn,
- řízení vydání,
- řízení bezpečnostních incidentů,
- řízení bezpečnosti informací.

2.2. Určení

Tyto společné provozní postupy jsou určeny pro podpůrné týmy unijního a švýcarského registru.

3. PŘÍSTUP A STANDARDY

Pro všechny společné provozní postupy platí tato zásada:

- EU a Švýcarsko se dohodly na definici společných provozních postupů podle ITIL (Knihovna infrastruktury informačních technologií, verze 4). Použity jsou postupy podle tohoto standardu, které jsou upraveny podle konkrétních potřeb souvisejících s trvalým propojením registrů,
- komunikace a koordinace potřebná pro zpracování společných provozních postupů mezi stranami probíhá přes centra podpory registrů Švýcarska a EU. Úkoly se přidělují vždy v rámci jedné strany,
- jestliže nedojde k dohodě, jak mají být společné provozní postupy zpracovány, bude to analyzováno a řešeno oběma centry podpory. Není-li možné dosáhnout dohody, nalezení společného řešení bude předáno na vyšší úroveň,

Úrovně eskalace	EU	CH
1. úroveň	Centrum podpory EU	Centrum podpory Švýcarska
2. úroveň	Provozní manažer EU	Manažer pro aplikace registru Švýcarska
3. úroveň	Smíšený výbor (který může tuto odpovědnost delegovat podle čl. 12 odst. 5 dohody o propojení)	
4. úroveň	Smíšený výbor, pokud je delegováno na 3. úrovni	

- každá strana může určit postupy pro provoz svého vlastního registračního systému, přičemž zohlední požadavky a rozhraní související s těmito společnými provozními postupy,
- na podporu společných provozních postupů se používá nástroj pro řízení IT služeb (ITSM), zejména řízení incidentů, řízení problémů a plnění žádostí, a komunikace mezi oběma stranami,
- kromě toho je přípustná výměna informací prostřednictvím elektronické pošty,
- obě strany zajistí, aby byly splněny požadavky na bezpečnost informací v souladu s pokyny pro nakládání.

4. ŘÍZENÍ INCIDENTŮ

Cílem procesu řízení incidentů je vrátit IT služby po incidentu na běžnou úroveň služeb co možná nejrychleji a s minimálním narušením provozu.

Při řízení incidentů je také třeba vést záznam o incidentech pro účely vykazování a tento proces by měl být integrován s jinými procesy, aby bylo možné jej průběžně zdokonalovat.

Z celkového pohledu zahrnuje řízení incidentů tyto činnosti:

- zjištění a záznam incidentu,
- klasifikaci a počáteční podporu,
- šetření a diagnostiku,
- vyřešení a obnovu,
- uzavření incidentu.

Po celou dobu trvání incidentu je proces řízení incidentu odpovědný za trvalé zapojení odpovědných osob, monitorování, sledování a komunikaci.

4.1. Zjištění a záznam incidentu

Incident může zjistit podpůrná skupina, automatizované monitorovací nástroje nebo techničtí pracovníci vykonávající rutinní dozor.

Incident musí být po zjištění zaznamenán a musí mu být přiřazen jedinečný identifikátor umožňující jeho řádné sledování a monitorování. Jedinečný identifikátor incidentu je identifikátor, který mu ve společném tiketovacím systému přiřadí centrum podpory té strany (EU nebo Švýcarsko), která incident zjistila, přičemž tento identifikátor musí být použit při každé komunikaci související s tímto incidentem.

U všech incidentů by kontaktním místem mělo být centrum podpory té strany, která tiket zaregistrovala.

4.2. Klasifikace a počáteční podpora

Cílem klasifikace incidentu je zjistit a určit, jaký systém a/nebo služba jsou incidentem postiženy a v jakém rozsahu. Aby byla klasifikace účinná, měla by nasměrovat incident ke správnému zdroji hned napoprvé, aby se urychlilo jeho vyřešení.

Ve fázi klasifikace je třeba incident kategorizovat a určit jeho prioritu podle jeho dopadu a naléhavosti, aby mohl být řešen podle příslušného časového rámce pro danou prioritu.

Pokud má incident potenciální dopad na důvěrnost nebo integritu citlivých údajů a/nebo má dopad na dostupnost systému, je třeba tento incident označit také za bezpečnostní incident a poté jej řídit podle procesu uvedeného v kapitole „Řízení bezpečnostních incidentů“ tohoto dokumentu.

Centrum podpory, které tiket zaregistrovalo, by mělo pokud možno provést první diagnostiku. Centrum podpory přitom zjistí, zda je incident známou chybou. V kladném případě jsou již způsob řešení nebo dočasné řešení známa a zadokumentovaná.

Jestliže centrum podpory incident úspěšně vyřeší, potom jej v tomto okamžiku uzavře, neboť primární účel řízení incidentů byl splněn (a to rychlá obnova služby pro konečného uživatele). V opačném případě centrum podpory předá incident na vyšší úroveň příslušné řešitelské skupině k dalšímu šetření a diagnostice.

4.3. Šetření a diagnostika

Šetření a diagnostika incidentů se používá, když incident nedokáže vyřešit centrum podpory v rámci první diagnostiky, a proto jej předá na vyšší úroveň. Eskalace incidentů je součástí procesu šetření a diagnostiky.

Běžnou praxí ve fázi šetření a diagnostiky je pokus o zopakování incidentu za řízených podmínek. Při šetření a diagnostice incidentů je důležité zjistit správné pořadí událostí, které k incidentu vedly.

Eskalace je uznání toho, že incident nemůže být vyřešen na aktuální úrovni podpory a musí být předán podpůrné skupině vyšší úrovně nebo druhé straně. Eskalace může probíhat dvěma způsoby: horizontálně (funkčně) nebo vertikálně (hierarchicky).

Centrum podpory, které incident zaznamenalo a spustilo jeho řešení, je odpovědné za předání incidentu příslušnému zdroji a za sledování celkového stavu a přiřazení incidentu.

Strana, jíž byl incident přiřazen, je odpovědná za zajištění včasného provedení požadovaných opatření a za poskytnutí zpětné vazby svému vlastnímu centru podpory.

4.4. Vyřešení a obnova

Jakmile je incident zcela prozkoumán, dochází k jeho vyřešení a obnově. Nalezení řešení incidentu znamená, že byl zjištěn způsob nápravy problému. Provedení řešení je obnovovací fáze.

Jakmile příslušné zdroje selhání služby vyřeší, je incident předán zpět do příslušného centra podpory, které jej zaregistrovalo, a toto centrum podpory u iniciátora incidentu potvrdí, že chyba byla opravena a že incident lze uzavřít. Zjištění ze zpracování incidentu je třeba zaznamenat pro budoucí použití.

Obnovu mohou provést pracovníci IT podpory nebo je možné předat konečnému uživateli pokyny, jak má postupovat.

4.5. Uzavření incidentu

Uzavření je posledním krokem v procesu řízení incidentů a probíhá krátce po vyřešení incidentu.

Ze seznamu činností, které musí být v průběhu fáze uzavření incidentu provedeny, je třeba zdůraznit tyto:

- ověření počáteční kategorizace, která byla incidentu přiřazena,
- správné zachycení všech informací souvisejících s incidentem,
- řádnou dokumentaci incidentu a aktualizaci znalostní báze,
- adekvátní komunikaci s každým účastníkem, který byl incidentem přímo nebo nepřímo postižen.

Incident je formálně uzavřen, jakmile centrum podpory provede fázi uzavření a oznámí to druhé straně.

Jakmile je incident uzavřen, znovu se neotevírá. Jestliže se incident v krátké době vyskytne znovu, původní incident se znovu neotevírá, ale je třeba zaregistrovat nový incident.

Jestliže incident sledují centra podpory EU i Švýcarska, je konečné uzavření povinností toho centra podpory, které tiket zaregistrovalo.

5. ŘÍZENÍ PROBLÉMŮ

Tento postup by měl být použit při každém zjištění problému, takže se jím spouští proces řízení problémů. Řízení problémů se zaměřuje na zvýšení kvality a snížení množství vzniklých incidentů. Problém může být příčinou jednoho nebo několika incidentů. Při ohlášení incidentu je cílem řízení incidentů obnovit službu co možná nejrychleji, což může zahrnovat dočasné řešení. Když vznikne problém, je cílem prošetřit základní příčinu tohoto problému, aby bylo možné určit, jaká změna zajistí, aby se tento problém a s ním spojené incidenty již nevyskytly.

5.1. Identifikace a záznam problému

Podle toho, která strana iniciovala tiket, bude kontaktním místem pro záležitosti spojené s problémem buď unijní centrum podpory, nebo švýcarské centrum podpory.

Jedinečný identifikátor problému je identifikátor, který mu přiřadí řízení IT služeb (ITSM). Musí být používán při každé komunikaci týkající se tohoto problému.

Problém může být spuštěn incidentem nebo může být otevřen samostatně za účelem odstranění nedostatků zjištěných v jakémkoli okamžiku v systému.

5.2. Stanovení priority problému

Problémy mohou být kategorizovány podle své závažnosti a priority stejně jako incidenty, aby bylo usnadněno jejich sledování, přičemž se zohlední dopad s nimi souvisejících incidentů a četnost jejich výskytu.

5.3. Šetření a diagnostika problémů

Problém může nadnést každá strana, přičemž centrum podpory iniciující strany je odpovědné za zaregistrování problému, jeho přiřazení příslušnému zdroji a sledování jeho celkového stavu.

Řešitelská skupina, jíž byl problém předán, je odpovědná za včasné řešení problému a komunikaci s centrem podpory.

Obě strany jsou na požádání odpovědné za zajištění provedení přiřazených činností a poskytnutí zpětné vazby svému vlastnímu centru podpory.

5.4. Vyřešení

Řešitelská skupina, jíž byl problém přiřazen, je odpovědná za vyřešení problému a poskytnutí příslušných informací svému vlastnímu centru podpory.

Zjištění ze zpracování problému je třeba zaznamenat pro budoucí použití.

5.5. Uzavření problému

Problém je formálně uzavřen, jakmile je vyřešen provedením změny. Fázi uzavření problému provede centrum podpory, které tento problém zaregistrovalo a informovalo centrum podpory druhé strany.

6. PLNĚNÍ ŽÁDOSTÍ

Proces plnění žádosti je komplexní řízení žádosti o novou nebo stávající službu od okamžiku jejího zaregistrování a schválení až do uzavření. Žádosti o službu jsou obvyklé drobné, předem definované, opakovatelné, časté, předem schválené a procedurální požadavky.

Níže jsou načrtnuty hlavní kroky, podle nichž je třeba postupovat:

6.1. Iniciování žádosti

Informace o žádosti o službu se předá unijnímu centru podpory nebo švýcarskému centru podpory e-mailem, telefonicky nebo prostřednictvím nástroje pro řízení IT služeb (ITSM) nebo jakéhokoli jiného dohodnutého komunikačního kanálu.

6.2. Registrování a analýza žádosti

Kontaktním místem pro všechny žádosti o službu by mělo být unijní nebo švýcarské centrum podpory podle toho, která strana žádost o službu podala. Toto centrum podpory bude odpovědné za řádné zaregistrování a analýzu žádosti o službu.

6.3. Schválení žádosti

Agent centra podpory strany, která žádost o službu podala, zkontroluje, zda jsou potřebná schválení druhé strany, a v kladném případě si je vyžádá. Jestliže žádost o službu není schválena, centrum podpory tiket aktualizuje a uzavře jej.

6.4. Plnění žádosti

Tento krok slouží k účelnému a efektivnímu zpracování žádostí o službu. Je třeba rozlišovat mezi těmito případy:

- plnění žádosti o službu se týká pouze jedné strany. V tomto případě vydá tato strana pracovní příkazy a koordinuje provedení,
- plnění žádosti o službu se týká EU i Švýcarska. V tomto případě centra podpory vydávají pracovní příkazy ve své oblasti odpovědnosti. Zpracování plnění žádosti o službu je koordinováno mezi oběma centry podpory. Celkovou odpovědnost nese centrum podpory, které žádost o službu obdrželo a iniciovalo.

Když je žádost o službu splněna, musí být nastavena do stavu Vyřešeno.

6.5. Eskalace žádosti

Centrum podpory může v případě potřeby předat nevyřízenou žádost o službu příslušnému zdroji (třetí straně).

Předává se příslušným třetím stranám, tj. unijní centrum podpory bude muset postupovat přes švýcarské centrum podpory, pokud má být žádost předána švýcarské třetí straně, a naopak.

Třetí strana, jíž byla žádost o službu předána, je odpovědná za včasné vyřízení žádosti o službu a komunikaci s centrem podpory, které žádost o službu předalo.

Centrum podpory, které žádost o službu zaregistrovalo, je odpovědné za sledování celkového stavu a přiřazení žádosti o službu.

6.6. Kontrola splnění žádosti

Odpovědné centrum podpory předloží záznam o žádosti o službu před jejím uzavřením k závěrečné kontrole kvality. Cílem je zajistit, aby byla žádost o službu opravdu zpracována a aby byly dodány všechny informace potřebné k popisu životního cyklu žádosti s dostatečnými podrobnostmi. Kromě toho je třeba zaznamenat zjištění ze zpracování žádosti pro budoucí použití.

6.7. Uzavření žádosti

Jestliže se strany, jimž byla žádost o službu přiřazena, dohodnou, že žádost byla splněna, a žadatel považuje případ za vyřešený, nastaví se stav „Uzavřeno“.

Žádost o službu je formálně uzavřena, jakmile centrum podpory, které tuto žádost o službu zaregistrovalo, provede uzavírací fázi žádosti a informuje centrum podpory druhé strany.

7. ŘÍZENÍ ZMĚN

Cílem je zajistit, aby byly používány standardizované metody a postupy za účelem efektivního a rychlého zpracování všech změn v řízení IT infrastruktury, aby se tak minimalizoval počet případných souvisejících incidentů a jejich dopad na službu. Změny IT infrastruktury mohou vznikat v reakci na problémy nebo externě vznesené požadavky, např. legislativní změny, případně aktivně za účelem zlepšení efektivity a účelnosti nebo za účelem umožnění obchodních iniciativ či jejich zohlednění.

Proces řízení změn zahrnuje různé kroky, které zachycují každou podrobnost o žádosti o změnu pro účely budoucího dohledání. Tyto procesy zajišťují, aby byla změna před provedením validována a otestována. Úspěšné provedení má na starosti proces řízení vydání.

7.1. Žádost o změnu

Žádost o změnu (RFC) se předá týmu pro řízení změn k validaci a ke schválení. Kontaktním místem pro všechny žádosti o změnu by mělo být unijní nebo švýcarské centrum podpory podle toho, která strana žádost podala. Toto centrum podpory bude odpovědné za řádné zaregistrování a analýzu žádosti.

Žádosti o změnu mohou vznikat z důvodu:

- incidentu, který změnu způsobí,
- stávajícího problému, v jehož důsledku ke změně dojde,
- požadavku na novou změnu vzneseného konečným uživatelem,
- změny v důsledku probíhající údržby,
- změny právních předpisů.

7.2. Hodnocení a plánování změn

V této fázi se provádí hodnocení změn a činností plánování. Zahrnuje stanovení priorit a plánování činností za účelem minimalizace rizik a dopadu.

Jestliže se provádění žádosti o změnu týká EU i Švýcarska, strana, která žádost o změnu zaregistrovala, ověří hodnocení a plánování změny u druhé strany.

7.3. Schválení změny

Každou zaregistrovanou žádost o změnu je třeba schválit na příslušné úrovni eskalace.

7.4. Provedení změny

K provedení změny dochází formou procesu řízení vydání. Týmy obou stran pro řízení vydání postupují podle svých vlastních procesů, které zahrnují plánování a testování. Po dokončení provedení dochází ke kontrole změny. Aby bylo zajištěno, že vše proběhlo podle plánu, je stávající proces řízení změn průběžně kontrolován a v případě potřeby aktualizován.

8. ŘÍZENÍ VYDÁNÍ

Vydání představuje jednu nebo několik změn IT služby shromážděných v plánu vydání, které musí být povoleny, připraveny, vytvořeny, otestovány a zavedeny společně. Vydání může představovat opravu chyby, změnu hardwaru nebo jiných komponentů, změny softwaru, upgrady verzí aplikací, změny dokumentace a/nebo procesů. Obsah každého vydání se řídí, testuje a zavádí jako jedna entita.

Cílem řízení vydání je naplánovat, vytvořit, otestovat, validovat a zajistit možnost poskytování navržených služeb, které budou plnit požadavky účastníků a uskutečňovat zamýšlené cíle. V průběhu koordinace návrhu budou definována a zadokumentována kritéria akceptace pro všechny změny služby, která budou předána týmům pro řízení vydání.

Vydání obvykle sestává z několika oprav problémů a vylepšení služby. Obsahuje požadovaný nový nebo změněný software a veškerý nový nebo změněný hardware potřebný k provedení schválených změn.

8.1. Plánování vydání

Prvním krokem procesu je přiřazení schválených změn do balíčků vydání a definování rozsahu a obsahu vydání. Na základě těchto informací se v dílčím procesu plánování vydání vypracuje harmonogram vytvoření, otestování a zavedení vydání.

Při plánování je třeba definovat:

- rozsah a obsah vydání,
- posouzení rizika a rizikový profil vydání,
- zákazníka/uživatele, jichž se vydání dotkne,
- tým odpovědný za vydání,
- strategii dodání a zavedení,
- zdroje pro dodání a zavedení.

Obě strany se vzájemně informují o plánování svých vydání a oknech pro údržbu. Jestliže se vydání týká EU i Švýcarska, obě strany koordinují plánování a určují společné okno pro údržbu.

8.2. Vytvoření a otestování balíčku vydání

V kroku vytváření a testování v procesu řízení vydání se stanoví způsob provedení vydání nebo balíčku vydání a údržby řízených prostředí před změnou produkce a dále proběhne otestování všech změn ve všech vydaných prostředích.

Jestliže se vydání týká EU i Švýcarska, obě strany koordinují plány dodání a testování. Zahrnuje to tyto aspekty:

- jak a kdy budou dodány jednotky vydání a komponenty služby,
- jaké jsou obvyklé doby realizace, co se stane, pokud dojde ke zpoždění,
- jak sledovat postup dodání a získat konfirmaci,
- měřítka monitorování a stanovení úspěšného zavedení vydání,
- společné testovací případy pro příslušné funkce a změny.

Na konci tohoto dílčího procesu jsou všechny potřebné komponenty vydání připraveny pro vstup do fáze skutečného provozu.

8.3. Příprava na zprovoznění

Přípravný dílčí proces zajišťuje, aby byly správně definovány komunikační plány a aby byla připravena oznámení pro rozeslání všem dotčeným účastníkům a konečným uživatelům a dále aby bylo vydání integrováno do procesu řízení změn, aby bylo zajištěno, že všechny změny budou provedeny kontrolovaně a budou schváleny potřebnými fóry.

Jestliže se vydání týká EU i Švýcarska, obě strany koordinují tyto činnosti:

- záznam žádosti o změnu pro účely naplánování a přípravy zavedení do produkčního prostředí,
- vytvoření prováděcího plánu,
- způsob návratu, aby v případě, že zavedení selže, mohl být navrácen předchozí stav,
- sdělení zaslaná všem potřebným stranám,
- žádost o schválení implementace vydání z příslušné úrovně eskalace.

8.4. Návrat do původního stavu

V případě, že zprovoznění selže nebo se při testování ukáže, že zprovoznění nebylo úspěšné nebo nesplnilo dohodnutá kritéria akceptace/kvality, týmy obou stran pro řízení vydání musí vrátit systém do předchozího stavu. Bude třeba informovat všechny potřebné účastníky, včetně dotčených/cílových konečných uživatelů. Až do schválení může být proces znovu spuštěn v kterékoli z předchozích fází.

8.5. Kontrola a uzavření vydání

Při kontrole zprovoznění je třeba provést tyto činnosti:

- získat zpětnou vazbu o spokojenosti zákazníka/uživatele s dodáním a zprovozněním služby (shromáždit zpětnou vazbu a zohlednit ji při průběžném zdokonalování služby),
- zrevidovat všechna kritéria kvality, která nebyla splněna,
- zkontrolovat, zda jsou všechny úkony, potřebné opravy a změny kompletní,
- zajistit, aby po dokončení zavádění nezůstaly nevyřešeny žádné problémy s funkčností, zdroji, kapacitou nebo výkonem,
- zkontrolovat, zda jsou zákazníkem, konečnými uživateli, provozní podporou a dalšími dotčenými stranami zdokumentovány a akceptovány všechny problémy, známé chyby a dočasná řešení,
- monitorovat incidenty a problémy způsobené zavedením (poskytnout podporu provozním týmům v rané fázi, pokud vydání způsobilo nárůst objemu práce),
- aktualizovat podkladovou dokumentaci (tj. technické informační dokumenty),
- formálně předat zavedené vydání do provozu,
- zdokumentovat získané poznatky,
- shromáždit od realizačních týmů souhrnnou dokumentaci vydání,
- formálně uzavřít vydání po ověření záznamu o žádosti o změnu.

9. ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Řízení bezpečnostních incidentů je proces řešení bezpečnostních incidentů, aby mohli být potenciálně dotčení účastníci o incidentu informováni; hodnocení incidentu a stanovení jeho priority a reakce na incident za účelem vyřešení skutečného nebo potenciálního narušení důvěrnosti, dostupnosti či integrity citlivých informací či podezření na takové narušení důvěrnosti, dostupnosti či integrity.

9.1. Kategorizace incidentů v oblasti bezpečnosti informací

Všechny incidenty s dopadem na propojení mezi unijním registrem a švýcarským registrem se analyzují za účelem zjištění, zda nedošlo k narušení důvěrnosti, integrity nebo dostupnosti jakýchkoli citlivých informací zaznamenaných v seznamu citlivých informací (SIL).

V kladném případě se incident charakterizuje jako incident v oblasti bezpečnosti informací, neprodleně se zaregistruje do nástroje řízení IT služeb (ITSM) a jako takový se řídí.

9.2. Řešení incidentů v oblasti bezpečnosti informací

Za bezpečnostní incidenty je odpovědná 3. úroveň eskalace a řešením incidentů bude pověřen specializovaný tým pro řízení incidentů (IMT).

Tým IMT odpovídá za:

- provedení první analýzy, kategorizaci a stanovení závažnosti incidentu,
- koordinaci činností mezi všemi účastníky včetně úplné dokumentace analýzy incidentu, rozhodnutí přijatých za účelem vyřešení incidentu a jakýchkoli možných zjištěných slabých stránek,
- v závislosti na závažnosti bezpečnostního incidentu včasné předání na příslušnou úroveň pro informaci a/nebo k rozhodnutí.

V procesu řízení bezpečnosti informací se všechny informace o incidentech klasifikují na nejvyšší úrovni citlivosti informací, v každém případě však nejméně jako *ETS* CITLIVÉ.

V případě probíhajícího šetření a/nebo výskytu slabé stránky, která by mohla být zneužita, se do doby než bude zjednána náprava informace klasifikují jako SPECIAL HANDLING: *ETS Critical*.

9.3. Identifikace bezpečnostních incidentů

Podle druhu bezpečnostní události určí pracovník pro bezpečnost informací příslušné organizace, které mají být zapojeny a budou zařazeny do týmu IMT.

9.4. Analýza bezpečnostních incidentů

Při zkoumání incidentu je tým IMT ve spojení se všemi zapojenými organizacemi a podle potřeby s příslušnými členy jejich týmů. V průběhu analýzy se určí rozsah ztráty důvěrnosti, integrity nebo dostupnosti aktiv a vyhodnotí se důsledky pro všechny postižené organizace. Dále se definují počáteční a následná opatření pro vyřešení incidentu a řízení jeho dopadu, včetně dopadu těchto opatření na zdroje.

9.5. Posouzení závažnosti bezpečnostního incidentu, eskalace a podávání zpráv

Tým IMT posoudí závažnost každého nového bezpečnostního incidentu po jeho charakterizaci jako bezpečnostního incidentu a neprodleně zahájí potřebná opatření podle závažnosti incidentu.

9.6. Podávání zpráv o reakcích v oblasti bezpečnosti

Tým IMT uvede informace o omezení důsledků incidentu a výsledcích obnovy do zprávy o reakci na bezpečnostní incident. Tato zpráva se předává na 3. úroveň eskalace pomocí bezpečné elektronické pošty nebo jiných vzájemně akceptovaných prostředků bezpečné komunikace.

Odpovědná strana zkontroluje omezení důsledků incidentu a výsledky obnovy a:

- opět připojí registr v případě, že byl předtím odpojen,
- zajistí komunikaci o incidentu s týmy, které se starají o registr,
- uzavře incident.

Tým IMT by měl ve zprávě o incidentu v oblasti bezpečnosti informací zabezpečeným způsobem uvést příslušné podrobnosti, aby byl zajištěn konzistentní záznam a komunikace a aby bylo možné přijmout rychlá a vhodná opatření za účelem omezení důsledků incidentu. Po dokončení tým IMT předloží v příslušné lhůtě závěrečnou zprávu o incidentu v oblasti bezpečnosti informací.

9.7. Monitorování, budování kapacit a průběžné zdokonalování

Tým IMT předává zprávy o všech bezpečnostních incidentech na 3. úroveň eskalace. Zprávy budou na této úrovni eskalace použity k určení:

- slabých míst v kontrolách bezpečnosti a/nebo provozu, které je třeba posílit,
- případné potřeby zdokonalit tento postup, aby se zlepšila účinnost při reagování na incidenty;
- možnosti školení a budování kapacit za účelem dalšího posílení odolnosti systémů registrů v oblasti bezpečnosti informací, snížení rizika budoucích incidentů a minimalizace jejich dopadu.

10. ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Cílem řízení bezpečnosti informací je zajistit důvěrnost, integritu a dostupnost utajovaných informací, dat a IT služeb organizace. Vedle technických složek včetně jejich návrhu a testování (viz technické normy pro propojování) jsou pro splnění bezpečnostních požadavků na trvalé propojení registrů potřebné následující společné provozní postupy.

10.1. Identifikace citlivých informací

Citlivost informace se posuzuje stanovením, jaký dopad na podnik by mohlo mít narušení bezpečnosti v případě této informace (například finanční ztráty, poškození pověsti, porušení právního předpisu...).

Citlivá informační aktiva se identifikují podle jejich dopadu na propojení.

Úroveň citlivosti těchto informací se posuzuje podle stupnice citlivosti platné pro toto propojení a uvedené v oddíle „Řešení incidentů v oblasti bezpečnosti informací“ tohoto dokumentu.

10.2. Úrovně citlivosti informačních aktiv

Po identifikaci se informační aktivum klasifikuje podle těchto pravidel:

- při identifikaci alespoň jedné VYSOKÉ úrovně důvěrnosti, integrity nebo dostupnosti je aktivum klasifikováno jako SPECIAL HANDLING: *ETS Critical*;
- při identifikaci alespoň jedné STŘEDNÍ úrovně u důvěrnosti, integrity nebo dostupnosti je aktivum klasifikováno jako SENSITIVE*: ETS*;
- při identifikaci pouze NÍZKÉ úrovně u důvěrnosti, integrity nebo dostupnosti je aktivum klasifikováno jako Označení EU**:** SENSITIVE: *ETS Joint Procurement.* Označení Švýcarska: LIMITED: ETS.

10.3. Přiřazení vlastníka informačních aktiv

Všechna informační aktiva by měla mít svého přiřazeného vlastníka. Informační aktiva ETS patřící k propojení mezi EUTL a SSTL nebo s ním spojená by měla být uvedena ve společném inventurním soupisu aktiv vedeném oběma stranami. Informační aktiva ETS mimo propojení mezi EUTL a SSTL by měla být uvedena v inventurním soupisu aktiv vedeném příslušnou stranou.

Strany se dohodnou na vlastnictví každého informačního aktiva patřícího k propojení mezi EUTL a SSTL nebo s ním spojeného. Vlastník informačního aktiva je odpovědný za posouzení jeho citlivosti.

Vlastník by měl mít pracovní funkci, která je přiměřená s ohledem na hodnotu přiřazeného aktiva (aktiv). Odpovědnost vlastníka za aktivum (aktiva) a jeho povinnost zachovávání potřebné úrovně důvěrnosti, integrity a dostupnosti je třeba dohodnout a formalizovat.

10.4. Registrace citlivých informací

Všechny citlivé informace se registrují v seznamu citlivých informací (SIL).

V příslušných případech se zohlední a v seznamu citlivých informací zaregistruje agregace citlivých informací, která by mohla vést k vyššímu dopadu, než je dopad jednotlivé informace (např. soubor informací uložených v systémové databázi).

Seznam citlivých informací není statický. Hrozby, zranitelnost, pravděpodobnost nebo důsledky bezpečnostních incidentů souvisejících s aktivy se mohou měnit bez jakéhokoli varovného signálu a do provozu systémů registrů mohou být zaváděna nová aktiva.

Proto je třeba seznam citlivých informací pravidelně kontrolovat a neprodleně do něj registrovat všechny nové informace identifikované jako citlivé.

Seznam citlivých informací obsahuje u každého zápisu alespoň tyto informace:

- popis informace,
- vlastníka informace,
- úroveň citlivosti,
- označení, zda informace zahrnuje osobní údaje,
- další informace, jsou-li potřebné.

10.5. Nakládání s citlivými informacemi

Pokud jsou citlivé informace zpracovávány mimo propojení mezi unijním registrem a švýcarským registrem, je třeba s nimi nakládat v souladu s pokyny pro nakládání.

S citlivými informacemi zpracovávanými v rámci propojení mezi unijním registrem a švýcarským registrem se nakládá v souladu s bezpečnostními požadavky stran.

10.6. Řízení přístupu

Cílem řízení přístupu je udělit oprávněným uživatelům právo používat službu a současně zabránit v přístupu neoprávněným uživatelům. Řízení přístupu se někdy také nazývá „správa práv“ nebo „správa identit“.

Pro trvalé propojení registrů a jeho provoz potřebují obě strany přístup k těmto komponentům:

- Wiki: prostředí pro spolupráci na výměnu společných informací, jako je plánování vydání,
- nástroj pro řízení IT služeb (ITSM) pro řízení incidentů a problémů (viz kapitola 3 „Přístup a standardy“),
- systém výměny zpráv: každá strana zajistí bezpečný přenosový systém výměny zpráv pro přenos zpráv obsahujících údaje o transakcích.

Správce švýcarského registru a ústřední správce Unie zajistí, aby byly přístupy aktuální, a budou fungovat jako kontaktní místa pro své strany pro činnosti v oblasti řízení přístupu. Žádosti o přístup se řeší podle postupů plnění žádostí.

10.7. Správa certifikátů/klíčů

Každá strana je odpovědná za správu svých vlastních certifikátů/klíčů (generování, registrace, ukládání, instalace, používání, prodloužení, zrušení, zálohování a obnova certifikátů/klíčů). Jak je uvedeno v technických normách pro propojování (LTS), používají se pouze digitální certifikáty vydané certifikačním orgánem, kterému obě strany důvěřují. Nakládání s certifikáty/klíči a jejich ukládání musí být v souladu s ustanoveními uvedenými v pokynech pro nakládání.

Každé zrušení a/nebo prodloužení certifikátů a klíčů bude koordinováno oběma stranami. Probíhá to podle postupů plnění žádostí.

Správce švýcarského registru a ústřední správce Unie si vymění certifikáty/klíče prostřednictvím zabezpečených komunikačních prostředků podle ustanovení stanovených v pokynech pro nakládání.

Každé ověření certifikátů/klíčů jakýmikoli prostředky mezi stranami bude probíhat mimo pásmo *(out of band)*.

PŘÍLOHA III

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

Postupy pro trvalé propojení registrů

Obsah

1. Glosář 10
2. Úvod 11
2.1. Oblast působnosti 11
2.2. Určení 12
3. Přístup a standardy 12
4. Řízení incidentů 13
4.1. Zjištění a záznam incidentu 13
4.2. Klasifikace a počáteční podpora 13
4.3. Šetření a diagnostika 14
4.4. Vyřešení a obnova 14
4.5. Uzavření incidentu 14
5. Řízení problémů 15
5.1. Identifikace a záznam problému 15
5.2. Stanovení priority problému 15
5.3. Šetření a diagnostika problémů 15
5.4. Vyřešení 15
5.5. Uzavření problému 15
6. Plnění žádostí 15
6.1. Iniciování žádosti 16
6.2. Registrování a analýza žádosti 16
6.3. Schválení žádosti 16
6.4. Plnění žádosti 16
6.5. Eskalace žádosti 16
6.6. Kontrola splnění žádosti 16
6.7. Uzavření žádosti 17
7. Řízení změn 18
7.1. Žádost o změnu 18

7.2. Hodnocení a plánování změn 18
7.3. Schválení změny 18
7.4. Provedení změny 18
8. Řízení vydání 18
8.1. Plánování vydání 19
8.2. Vytvoření a otestování balíčku vydání 19
8.3. Příprava na zprovoznění 19
8.4. Návrat do původního stavu 20
8.5. Kontrola a uzavření vydání 20
9. Řízení bezpečnostních incidentů 20
9.1. Kategorizace incidentů v oblasti bezpečnosti informací 20
9.2. Řešení incidentů v oblasti bezpečnosti informací 21
9.3. Identifikace bezpečnostních incidentů 21
9.4. Analýza bezpečnostních incidentů 21
9.5. Posouzení závažnosti bezpečnostního incidentu, eskalace a podávání zpráv 21
9.6. Podávání zpráv o reakcích v oblasti bezpečnosti 21
9.7. Monitorování, budování kapacit a průběžné zdokonalování 22
10. Řízení bezpečnosti informací 22
10.1. Identifikace citlivých informací 22
10.2. Úrovně citlivosti informačních aktiv 22
10.3. Přiřazení vlastníka informačních aktiv 22
10.4. Registrace citlivých informací 23
10.5. Nakládání s citlivými informacemi 23
10.6. Řízení přístupu 23
10.7. Správa certifikátů/klíčů 24
1. Glosář 29
2. Úvod 31
2.1. Oblast působnosti 31
2.2. Určení 32
3. Obecná ustanovení 32
3.1. Architektura komunikačního propojení 32
3.1.1. Výměna zpráv 32
3.1.2. Zpráva XML – podrobný popis 32

3.1.3. Okna pro příjem 32
3.1.4. Toky zpráv o transakcích 33
3.2. Zabezpečení přenosu dat 36
3.2.1. Firewall a síťové propojení 36
3.2.2. Virtuální privátní síť (VPN) 36
3.2.3. Provádění IPSec 36
3.2.4. Protokol pro bezpečný přenos zpráv. 37
3.2.5. Šifrování a podpis XML 37
3.2.6. Kryptografické klíče 37
3.3. Seznam funkcí v rámci propojení 37
3.3.1. Obchodní transakce 37
3.3.2. Protokol sesouhlasení 38
3.3.3. Testovací zpráva 38
3.4. Požadavky na vedení protokolů 38
3.5. Provozní požadavky 39
4. Ustanovení o dostupnosti 40
4.1. Návrh dostupnosti komunikace 40
4.2. Inicializace, reaktivace komunikace a plán testování 40
4.2.1. Interní testy IKT infrastruktury 41
4.2.2. Testy komunikace 41
4.2.3. Testy celého systému (end-to-end) 41
4.2.4. Bezpečnostní testy 41
4.3. Akceptační/testovací prostředí 42
5. Ustanovení o důvěrnosti a integritě 42
5.1. Infrastruktura pro testování bezpečnosti 42
5.2. Ustanovení o pozastavení propojení a jeho reaktivaci 43
5.3. Ustanovení o narušení bezpečnosti 43
5.4. Pokyny pro testování bezpečnosti 44
5.4.1. Software 44
5.4.2. Infrastruktura 44
5.5. Ustanovení o posouzení rizik 44

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 systému obchodování s emisemi jednoho či druhého subjektu.
CH	Švýcarská konfederace
CHU	Typ stacionárních povolenek, rovněž nazývaný CHU2 (odkazující na druhé kontrolní období Kjótského protokolu), vydaný Švýcarskou konfederací
CHUA	Švýcarská povolenka pro letectví
COP	Společné provozní postupy. Společně vypracované postupy pro zprovoznění propojení mezi systémem EU ETS a ETS Švýcarska
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.
Kryptografický klíč	Informace, která určuje funkční výstup kryptografického algoritmu.
Dešifrování	Opačný proces šifrování
Digitální podpis	Matematická technika používaná k validaci 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 indikace normálního provozu nebo synchronizace jiných částí výpočetního systému.
IPSEC	IP SECurity. Bezpečnostní rozšíření protokolu IP, 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 zranitelnosti v zabezpečení, která by mohl využít útočník.
Proces sesouhlasení	Proces zajištění, že dva soubory záznamů spolu souhlasí.
VPN	Virtuální privátní síť

Zkratka	Definice
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 „EU ETS“) nebo v rámci systému obchodování s emisemi Švýcarska (dále jen „ETS Švýcarska“). Za účelem zprovoznění propojení mezi EU ETS a ETS Švýcarska se zřídí 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). S cílem zprovoznit propojení mezi systémem EU ETS a ETS Švýcarska bylo v roce 2020 zavedeno prozatímní řešení. Od roku 2023 se propojení registrů mezi oběma systémy obchodování s emisemi bude postupně vyvíjet směrem k trvalému propojení registrů, jež by mělo být realizováno nejpozději v roce 2024, což umožní fungování propojených trhů, pokud jde o výhody z tržní likvidity a provádění transakcí mezi oběma propojenými systémy způsobem, který je rovnocenný jednomu trhu tvořenému dvěma systémy a který účastníkům trhu umožňuje jednat, jako by byli na jednom trhu, s výhradou pouze jednotlivých regulačních ustanovení stran (příloha II dohody).

Podle čl. 3 odst. 7 dohody správce švýcarského registru a ústřední správce registru 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 byly přijaty smíšeným výborem rozhodnutím č. 2/2020. Aktualizované technické normy pro propojování zaznamenané v tomto dokumentu přijme smíšený výbor svým rozhodnutím č. 1/2024. V souladu s tímto rozhodnutím a žádostmi smíšeného výboru správce švýcarského registru a ústřední správce Unie vypracovali a budou aktualizovat další technické pokyny, aby mohlo dojít ke zprovoznění propojení a bylo zajištěno průběžné přizpůsobování uvedených pokynů technickému pokroku a/nebo 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 EU ETS a ETS Švýcarska. 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.

Ke správnému fungování bude propojení vyžadovat procesy a postupy, aby bylo možné propojení dále zprovozňovat. Podle čl. 3 odst. 6 dohody jsou tyto záležitosti podrobně popsány v samostatném dokumentu týkajícím se společných provozních postupů přijatém rozhodnutím smíšeného výboru.

2.2. Určení

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

3. OBECNÁ USTANOVENÍ

3.1. Architektura komunikačního propojení

Účelem tohoto oddílu je poskytnout popis obecné architektury pro zprovoznění propojení mezi EU ETS a ETS Švýcarska a jednotlivých komponentů, které jej tvoří.

Protože klíčovou částí pro definování architektury je bezpečnost, byla přijata veškerá opatření, aby byla zajištěna stabilní architektura. Trvalé propojení registrů využívá mechanismus pro výměnu souborů, jako je zavedení zabezpečeného spojení Air Gap.

Technické řešení používá:

- Protokol pro bezpečný přenos zpráv.
- Zprávy XML.
- Digitální podpis a šifrování na základě XML.
- VPN.

Na následujícím obrázku je uveden celkový pohled na architekturu trvalého propojení registrů:

3.1.1. Výměna zpráv

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

Obě strany vedou 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 se řeší 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

Trvalé propojení registrů vychází z předem definovaných oken pro příjem, po nichž následuje skupina uvedených událostí. Žádosti o transakci obdržené přes propojení budou přijímány pouze v

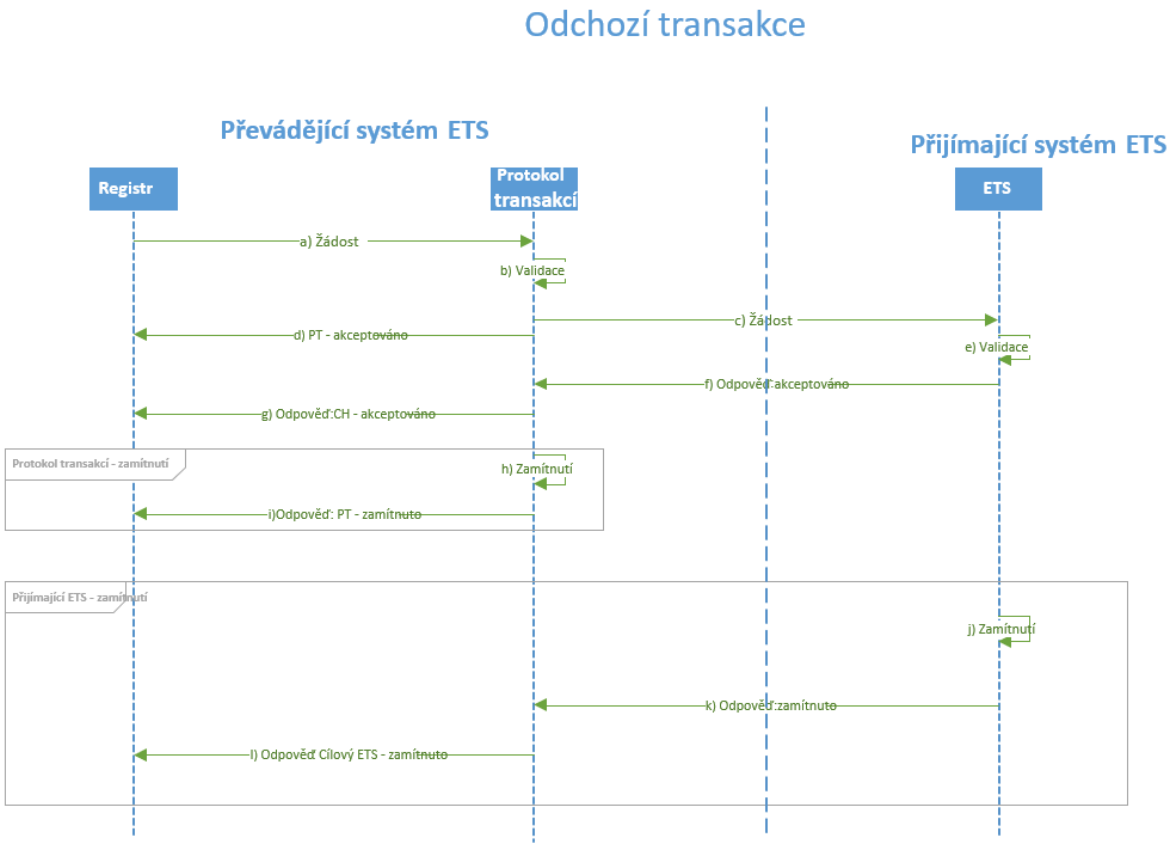
předem definovaných intervalech, což zahrnuje technickou validaci odchozích a příchozích transakcí. Kromě toho mohou každý den probíhat sesouhlasení, která mohou být spuštěna manuálně.

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. Konkrétní tok je zobrazen na následujícím sekvenčním diagramu:



Hlavní tok znázorňuje následující kroky (podle výše uvedeného obrázku):

(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 validuje žádost o transakci.
(c) Žádost o transakci se odešle do cílového systému ETS.
(d) Do registru výchozího systému ETS se zašle odpověď o akceptaci.
(e) Cílový systém ETS validuje žádost o transakci.
(f) Cílový systém ETS zašle odpověď o akceptaci zpět do protokolu transakcí výchozího systému ETS.
(g) Protokol transakcí zašle odpověď o akceptaci do registru.

Alternativní tok „Zamítnutí v protokolu transakcí“ (podle obrázku výše počínaje písmenem a) v hlavním toku):

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

(b) Protokol transakcí žádost nevaliduje.

(c) Do výchozího registru se zašle odpověď o zamítnutí.

Alternativní tok „Zamítnutí v ETS“ (podle obrázku výše počínaje písmenem d) v hlavním toku):

(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 validuje transakci.

(c) Žádost o transakci se odešle do cílového systému ETS.

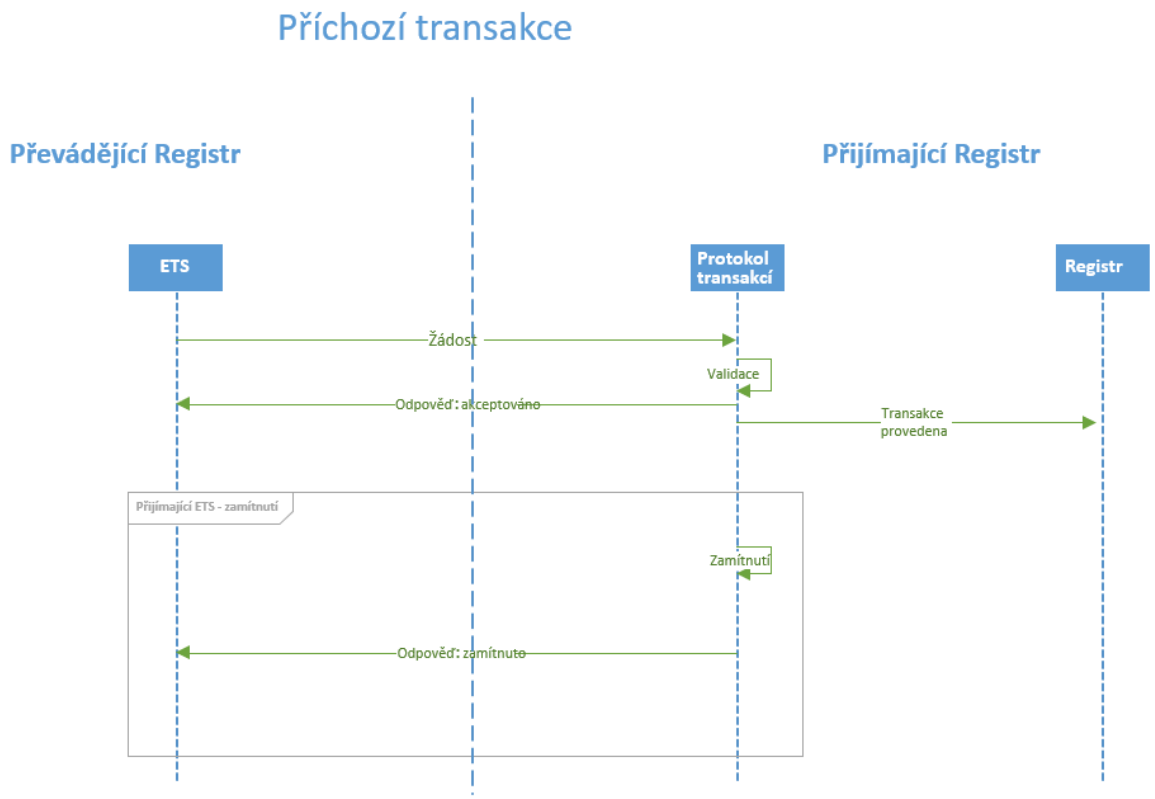
(d) Do registru výchozího systému ETS se zašle zpráva o akceptaci.

(e) Protokol transakcí přijímajícího systému ETS žádost nevaliduje.

(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 validuje žádost, zašle zprávu o akceptaci 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: Akceptováno nebo Zamítnuto (včetně důvodu zamítnutí).
  - Akceptováno: 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 akceptaci/zamítnutí,
- Stav transakce v převádějícím systému ETS bude v případě obdržení akceptace/zamítnutí 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.

(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 privátní síť (VPN)

Veškerá komunikace mezi stranami je chráněna s využitím technologie virtuální privátní sítě (VPN). Technologie VPN poskytují možnost „vytvoření tunelu“ skrz síť, jako je internet, z jednoho místa do druhého, přičemž veškerá komunikace je chráněna. Před vytvořením tunelu VPN je pro koncový bod budoucího 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. Každý koncový server VPN bude mít za použití digitálních certifikátů přístup k ústřednímu 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.

Evropská unie obecně využívá zabezpečené transevropské služby pro telematiku mezi správními orgány (STESTA) jako privátní síť založenou na internetovém protokolu (IP). Tato síť je proto vhodná i pro trvalé propojení registrů.

3.2.3. Provádění IPSec

Používání protokolu IPSec k vytvoření infrastruktury VPN typu *site-to-site* zajistí 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.

Trvalé propojení registrů používá pro bezpečnou výměnu dat mezi stranami několik šifrovacích vrstev. Oba systémy a jejich různá prostředí jsou propojeny na úrovni sítě pomocí tunelů VPN. 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 prvku „zprávy“.

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 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 pásmo *(out of band)*. Tento postup je nedílnou součástí procesu řízení bezpečnosti informačních systémů v rámci společných provozních postupů.

3.3. Seznam funkcí v rámci propojení

Propojení specifikuje přenosový systém pro sérii funkcí, které provádějí obchodní procesy vycházející z dohody. Propojení zahrnuje také specifikaci procesu sesouhlasení a testovacích 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 validaci a zpracování.

Sesouhlasení jsou nedílnou součástí bezpečnostních opatření a opatření pro 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 přijetí však bude provedeno alespoň plánované sesouhlasení.

Každá strana však může kdykoli zahájit manuální sesouhlasení.

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 ji identifikují jako testovací, a bude zodpovězena po přijetí druhým koncovým bodem.

3.4. Požadavky na vedení protokolů

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 auditu. Soubory protokolů starší 3 (tří) 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

Subsystémy EUTL i SSTL jsou implementacemi protokolu transakcí. Ty jsou vzájemně ověřeny mezi oběma systémy ETS.

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 trvalém propojení registrů jsou zprávy o sesouhlasení nedílnou součástí vyměňovaných zpráv, a proto se ukládají tak, jak je popsáno v oddíle „Archiv 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 provedení auditu 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.

3.5. Provozní požadavky

Výměna dat mezi oběma systémy není v trvalém propojení registrů zcela autonomní, což znamená, že zprovoznění propojení vyžaduje operátory a postupy. V tomto procesu je za tímto účelem podrobně popsáno několik funkcí a nástrojů.

4. USTANOVENÍ O DOSTUPNOSTI

4.1. Návrh dostupnosti komunikace

Architektura trvalého propojení registrů je v podstatě IKT infrastruktura a software, který umožňuje komunikaci mezi systémem ETS Švýcarska a systémem ETS Evropské unie. Proto se zajištění vysoké úrovně dostupnosti, integrity a důvěrnosti toku těchto dat stává zásadním aspektem, který je třeba při návrhu trvalého propojení registrů zvažovat. Protože jde o projekt, v němž hraje hlavní roli IKT infrastruktura, software na zakázku a procesy, 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, trvalé propojení registrů zřizuje odolnou VPN síť, která vytváří bezpečné komunikační tunely, jimiž může probíhat bezpečná výměna zpráv. Jiné prvky infrastruktury jsou konfigurovány na vysokou dostupnost a/nebo spoléhají na záložní 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 trvalém propojení registrů dochází k výměně údajů mezi stranami v předem stanovených intervalech. 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 časová okna na provedení každého kroku.
- Softwarové moduly pro trvalé propojení registrů provádějí asynchronní komunikaci.
- 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, reaktivace komunikace a plán testování

Všechny různé prvky zapojené do architektury trvalého propojení registrů 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 trvalé propojení registrů 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 soubor interních testů, po nichž následovala validace konektivity mezi koncovými body předtím, než začne předávání 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 zejména zahrnovat:

- kritéria a nástroje pro testování,
- role přiřazené k provedení testu,
- očekávané výsledky (pozitivní i negativní),
- časový rozvrh testu,
- záznam požadavků na výsledky testu,
- dokumentaci pro řešení problémů,
- ustanovení o eskalaci.

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

4.2.1. Interní testy IKT infrastruktury

Tyto testy mají být prováděny a/nebo kontrolovány individuálně správci registrů 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 zahájí každá strana individuálně a dokončí je ve 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 a že existuje IP konektivita typu *site-to-site*. Poté je třeba druhému konci potvrdit dosažitelnost lokálních i vzdálených prvků infrastruktury a IP konektivitu.

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 správci registrů na každém konci, jak je popsáno v částech „Pokyny pro testování bezpečnosti“ a „Ustanovení o posouzení rizik“.

Až když každá ze čtyř fází/bloků skončí s předvídatelnými výsledky, může být trvalé propojení registrů 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 validaci platformy. Správci registrů mohou kdykoli realizovat manuální individuální nebo společné testovací postupy. Aktivace provozního stavu je sama o sobě manuální proces.

Předpokládá se rovněž, 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: softwarové moduly pro trvalé propojení registrů provádějí 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. Akceptační/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.
- akceptace (ACC): toto prostředí obsahuje údaje, které nejsou skutečné nebo jsou anonymizované či reprezentativní. Je to prostředí, kde operátoři systémů obou stran validují 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 jsou tato tři prostředí na sobě zcela nezávislá, což znamená, že hardware, software, databáze, virtuální prostředí, IP adresy, porty se nastavují a provozují nezávisle na sobě.

Pokud jde o uspořádání VPN, komunikace mezi uvedenými třemi prostředími musí být zcela nezávislá, což je zajištěno použitím sítě STESTA.

5. USTANOVENÍ O DŮVĚRNOSTI A INTEGRITĚ

Bezpečnostní mechanismy a postupy předpokládají u operací probíhajících v propojení mezi registrem Unie a švýcarským registrem roli dvou osob (zásada 4 očí). Role dvou osob se uplatňuje vždy, když je to potřebné, nemusí se však používat u všech kroků prováděných správci registrů.

Bezpečnostní požadavky jsou rozebrány a řešeny v plánu pro řízení bezpečnosti, který zahrnuje podobné 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 zranitelností ve vývojové a provozní fázi):

- odděleně od produkčního prostředí,
- kde bezpečnost analyzuje tým nezávislý na vývoji a provozu systému.

Každá strana se zavazuje provádět statickou i dynamickou analýzu.

V případě dynamické analýzy (jako je penetrační testování) se obě strany zavazují omezit hodnocení zpravidla na testovací a akceptační prostředí (podle definice v části „Akceptační/testovací prostředí“). Výjimky z této zásady podléhají schválení oběma stranami.

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

Testovací infrastruktura musí být oddělena na úrovni sítě i infrastruktury od produkční infrastruktury a musí umožňovat provedení bezpečnostních testů potřebných ke kontrole souladu s bezpečnostními požadavky.

5.2. Ustanovení o pozastavení propojení a jeho reaktivaci

Existuje-li podezření, že zabezpečení švýcarského registru, SSTL, registru Unie nebo EUTL bylo ohroženo, obě strany se neprodleně vzájemně informují a pozastaví propojení mezi SSTL a EUTL.

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 (údržby, ...), tedy důvodů plánovaných,
- bezpečnostních důvodů (nebo poruch IT infrastruktury), tedy důvodů neplánovaných.

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, plánované i neplánované, bude přijato podle postupu řízení změn nebo postupu řízení bezpečnostních incidentů uvedených ve společných provozních postupech.

Reaktivace komunikace

Rozhodnutí o reaktivaci bude přijato podle popisu ve společných provozních postupech a v každém případě až po úspěšném provedení bezpečnostního testování, jak je popsáno v částech „Pokyny pro testování bezpečnosti“ a „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.

Informace přímo související s narušením bezpečnosti budou považovány za citlivé, označené jako „SPECIAL HANDLING: *ETS Critical*“ a bude s nimi nakládáno v souladu s pokyny pro nakládání, není-li stanoveno 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 dvanácti měsících nedošlo k vydání žádného důležitého softwaru, provede se testování bezpečnosti na stávajícím systému s ohledem na vývoj kybernetických hrozeb, k němuž v posledních dvanácti měsících došlo.

Testování bezpečnosti propojení registrů se provede v akceptačním 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 zranitelnosti (alespoň jednou měsíčně) a zjištěné zranitelnosti se opraví podle stejné zásady, jaká je definována v předchozí části, s využitím aktuální databáze zranitelností.

5.5. Ustanovení o posouzení rizik

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

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

- má v oblasti takového testování 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 na úrovni „SPECIAL HANDLING: ETS Critical“.