EURÓPAI
BIZOTTSÁG

Brüsszel, 2024.3.20.
COM(2024) 125 final

ANNEX

MELLÉKLET

a következőhöz:

Javaslat

A TANÁCS HATÁROZATA

az Európai Unió által az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodással létrehozott vegyes bizottságban a megállapodás II. mellékletének, a közös üzemeltetési eljárásoknak és kapcsolástechnikai szabványoknak a módosításával kapcsolatban képviselendő álláspontról

AZ EURÓPAI UNIÓ ÉS A SVÁJCI ÁLLAMSZÖVETSÉG KÖZÖTTI, AZ UNIÓS ÉS A SVÁJCI KIBOCSÁTÁSKERESKEDELMI RENDSZER ÖSSZEKAPCSOLÁSÁRÓL SZÓLÓ MEGÁLLAPODÁSSAL LÉTREHOZOTT VEGYES BIZOTTSÁG 1/2024 SZÁMÚ HATÁROZATA

(...)

a megállapodás II. mellékletének, a közös üzemeltetési eljárásoknak és a kapcsolástechnikai szabványoknak a módosításáról

A VEGYES BIZOTTSÁG,

tekintettel az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodásra[1] (a továbbiakban: megállapodás) és különösen annak 9. cikkére és 13. cikkének (2) bekezdésére,

mivel:

(1) A vegyes bizottság 2/2019. számú határozata[2] átmeneti megoldást tartalmazott az EU ETS és a svájci ETS összekapcsolásának működőképessé tételére.

(2) A vegyes bizottság a harmadik ülésén egyetértett abban, hogy meg kell vizsgálni az uniós és a svájci kibocsátásiegység-forgalmi jegyzék közötti állandó kapcsolat költséghatékonyságát.

(3) A vegyes bizottság az ötödik ülésén megállapodott az 1/2020.[3] és a 2/2020. számú[4] vegyes bizottsági határozattal létrehozott munkacsoport által benyújtott jelentésről, amelyben a munkacsoport elemezett és javasolt egy, az uniós és a svájci kibocsátásiegység-forgalmi jegyzék közötti állandó kapcsolat megvalósítására vonatkozó megközelítést.

(4) Az uniós és a svájci kibocsátásiegység-forgalmi jegyzék közötti állandó kapcsolat műszaki követelményeinek tükrözése, valamint a megállapodás II. mellékletében foglalt rendelkezéseknek a technológiai fejlődés fényében történő egyszerűsítése érdekében a megállapodás II. mellékletét módosítani kell.

(5) Annak érdekében, hogy a közös üzemeltetési eljárások és a kapcsolástechnikai szabványok összhangban legyenek a megállapodás II. mellékletével, e dokumentumokat is módosítani kell.

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

1. A megállapodás II. melléklete helyébe e határozat I. mellékletének szövege lép.

2. A megállapodás 3. cikkének (6) bekezdésében említett közös üzemeltetési eljárásokat e határozat II. melléklete tartalmazza.

3. A megállapodás 3. cikkének (7) bekezdésében említett kapcsolástechnikai szabványokat e határozat III. melléklete tartalmazza.

[1] HL L 322., 2017.12.7., 3. o.
[2] HL L 314., 2020.9.29., 68. o.
[3] HL L 226., 2021.6.25., 2. o.
[4] HL L 226., 2021.6.25., 16. o.

2. cikk

Ez a határozat az elfogadásának napján lép hatályba.

Kelt [Brüsszelben][Bernben], angol nyelven, [2024. XX]-án/-én.

a vegyes bizottság részéről

titkár az Európai Unió részéről	*az elnök*	*titkár Svájc részéről*

I. MELLÉKLET

„II. MELLÉKLET

KAPCSOLÁSTECHNIKAI SZABVÁNYOK

Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében 2020-ban egy átmeneti megoldást vezettek be. 2023-tól a két kibocsátáskereskedelmi rendszer közötti kapcsolat fokozatosan kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolattá alakul, amelyet várhatóan legkésőbb 2024-ig kell megvalósítani. Ezáltal lehetővé válik az összekapcsolt piacok működése a piaci likviditásból származó előnyök és a két összekapcsolt rendszer közötti ügyletek végrehajtása tekintetében, oly módon, hogy tulajdonképpen két rendszerből álló egyetlen piacként funkcionál, lehetővé téve a piaci szereplők számára, hogy úgy járjanak el, mintha egyetlen piacon mozognának, miközben csak a felek egyedi szabályozási rendelkezései vonatkoznak rájuk. A kapcsolástechnikai szabványok (Linking Technical Standard – LTS) a következőket határozzák meg:

– a kommunikációs kapcsolat architektúráját,

– az SSTL és az EUTL közötti kommunikációt,

– az adatátvitel biztonságát,

– a funkciók listáját (tranzakciók, egyeztetés stb.),

– a szállítási réteg meghatározását,

– az adatnaplózási követelményeket,

– az operatív intézkedéseket (telefonos ügyfélszolgálat, támogatás),

– a kommunikáció-aktiválási tervet és a tesztelési eljárást,

– a biztonsági tesztelési eljárást.

Az LTS-ek előírják, hogy a jegyzékkezelőknek/tisztviselőknek minden észszerű lépést meg kell tenniük annak biztosítása érdekében, hogy az SSTL és az EUTL, valamint a kapcsolat a hét minden napján napi 24 órában működjön, továbbá, hogy az SSTL, az EUTL és a kapcsolat működésének bármilyen jellegű megszakításai a minimumra korlátozódjanak.

Az LTS-ek további biztonsági követelményeket határoznak meg a svájci kibocsátásiegység-forgalmi jegyzék, az SSTL, az uniós kibocsátásiegység-forgalmi jegyzék és az EUTL számára, amelyeket egy „biztonságkezelési tervben” kell dokumentálni. Az LTS-ek különösen a következőket határozzák meg:

– ha felmerül a gyanú, hogy a svájci kibocsátásiegység-forgalmi jegyzék, az SSTL, az uniós kibocsátásiegység-forgalmi jegyzék vagy az EUTL biztonsága veszélybe került, a felek haladéktalanul tájékoztatják egymást, és felfüggesztik az SSTL és az EUTL közötti kapcsolatot,

– a biztonsági szabályok megsértése esetén a felek kötelezettséget vállalnak arra, hogy az információt haladéktalanul megosztják egymással. Amennyiben a technikai részletek rendelkezésre állnak, az eseményt (dátum, ok, hatás, megoldások) bemutató jelentést a

biztonsági esemény biztonság megsértéseként való azonosítását követő 24 órán belül meg kell osztani a svájci jegyzékkezelő és az uniós központi tisztviselő között.

Az LTS-ekben előírt biztonsági tesztelési eljárást az SSTL és az EUTL közötti kommunikációs kapcsolat létrehozása, illetve az SSTL vagy az EUTL új változatának vagy kiadásának esedékessége előtt el kell végezni.

Az LTS-ek két tesztelési környezetet biztosítanak a gyártási környezet mellett: a projektgazda környezetet és az elfogadási környezetet.

A felek a svájci jegyzékkezelőn és az uniós központi tisztviselőn keresztül bizonyítékot szolgáltatnak arra vonatkozóan, hogy rendszereik független biztonsági értékelését az LTS-ekben meghatározott biztonsági követelményekkel összhangban az elmúlt tizenkét hónapban elvégezték. Az LTS-ekben meghatározott biztonsági követelményeknek megfelelően a szoftver minden jelentősebb új kiadásán biztonsági tesztelést és különösen behatolási tesztelést kell végezni. A szoftverfejlesztő vagy a szoftverfejlesztő alvállalkozója nem végezheti el a behatolási tesztelést.”

II. MELLÉKLET

KÖZÖS ÜZEMELTETÉSI ELJÁRÁSOK

az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás 3. cikkének (6) bekezdése alapján

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolatra vonatkozó eljárások

Tartalomjegyzék

1. Glosszárium 10
2. Bevezetés 11
2.1. Alkalmazási kör 11
2.2. Címzettek 12
3. Megközelítés és előírások 12
4. Eseménykezelés 13
4.1. Események észlelése és rögzítése 13
4.2. Osztályozás és kezdeti támogatás 13
4.3. Kivizsgálás és diagnosztizálás 14
4.4. Rendezés és helyreállítás 14
4.5. Esemény lezárása 15
5. Problémakezelés 16
5.1. A probléma azonosítása és rögzítése 16
5.2. A probléma rangsorolása 16
5.3. A probléma kivizsgálása és diagnosztizálása 16
5.4. Rendezés 16
5.5. A probléma lezárása 16
6. Kérés teljesítése 17
6.1. Kérés kezdeményezése 17
6.2. Kérés naplózása és elemzése 17
6.3. Kérés jóváhagyása 17
6.4. Kérés teljesítése 17
6.5. Kérés felterjesztése 17
6.6. Kérés teljesítésének felülvizsgálata 18
6.7. Kérés lezárása 18
7. Változáskezelés 19
7.1. Változtatási kérelem 19

7.2. Változás értékelése és tervezése 19
7.3. Változás jóváhagyása 19
7.4. Változás végrehajtása 19
8. Kiadáskezelés 20
8.1. Kiadás tervezése 20
8.2. Kiadási csomag létrehozása és tesztelése 20
8.3. Telepítés előkészítése 21
8.4. Kiadás visszavonása 21
8.5. Kiadás felülvizsgálata és lezárása 21
9. Biztonsági események kezelése 22
9.1. Információbiztonsági esemény besorolása 22
9.2. Információbiztonsági esemény kezelése 22
9.3. Biztonsági esemény azonosítása 22
9.4. Biztonsági esemény elemzése 22
9.5. Biztonsági esemény súlyosságának meghatározása, felterjesztése és bejelentése 23
9.6. Biztonsági reagálási jelentés 23
9.7. Ellenőrzés, kapacitásépítés és folyamatos fejlesztés 23
10. Információbiztonsági irányítás 23
10.1. Érzékeny információk azonosítása 24
10.2. Az információs eszközök érzékenységi szintjei 24
10.3. Az információs eszköz tulajdonosának hozzárendelése 24
10.4. Érzékeny információk nyilvántartása 24
10.5. Érzékeny információk kezelése 25
10.6. Hozzáférés-kezelés 25
10.7. Tanúsítvány- / Kulcskezelés 25

1. GLOSSZÁRIUM

1-1. táblázat: Rövidítések és fogalommeghatározások

Rövidítés/Kifejezés	Fogalommeghatározás
Tanúsító hatóság	Elektronikus tanúsítványokat kiállító szervezet
CH	Svájci Államszövetség

ETS	Kibocsátáskereskedelmi rendszer
EU	Európai Unió
Információs eszköz	Valamely vállalat vagy szervezet számára értékes információ
IT	Információtechnológia
ITIL	Információtechnológiai infrastruktúra könyvtár (Information Technology Infrastructure Library)
LTS	Kapcsolástechnikai szabványok (Linking Technical Standards)
Kibocsátásiegység-forgalmi jegyzék	Az ETS keretében kiadott kibocsátási egységek elszámolására szolgáló rendszer, amely nyomon követi az elektronikus számlákon tartott kibocsátási egységek tulajdonosait.
Wiki	Weboldal, amely lehetővé teszi a felhasználók számára információk és ismeretek megosztását tartalom közvetlenül webböngészőn keresztül történő hozzáadásával vagy átdolgozásával

2. BEVEZETÉS

Az Európai Unió és a Svájci Államszövetség közötti 2017. november 23-i, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás (a továbbiakban: megállapodás) rendelkezik az uniós kibocsátáskereskedelmi rendszerben (a továbbiakban: EU ETS) vagy a svájci kibocsátáskereskedelmi rendszerben (a továbbiakban: svájci ETS) felhasználható kibocsátási egységek kölcsönös elismeréséről. Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében létre kell hozni az uniós kibocsátásiegység-forgalmi jegyzék európai uniós ügyleti jegyzőkönyve (EUTL) és a svájci kibocsátásiegység-forgalmi jegyzék svájci kiegészítő ügyleti jegyzőkönyve (SSTL) közötti közvetlen kapcsolatot, amely lehetővé teszi a két ETS bármelyikében kiadott kibocsátásiegység-forgalmi jegyzékek egymás közötti átruházását (a megállapodás 3. cikkének (2) bekezdése). Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében 2020-ban egy átmeneti megoldást vezettek be. 2023-tól a két kibocsátáskereskedelmi rendszer közötti kapcsolat fokozatosan kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolattá alakul, amelyet várhatóan legkésőbb 2024-ig kell megvalósítani. Ezáltal lehetővé válik az összekapcsolt piacok működése a piaci likviditásból származó előnyök és a két összekapcsolt rendszer közötti ügyletek végrehajtása tekintetében, oly módon, hogy tulajdonképpen két rendszerből álló egyetlen piacként funkcionál, lehetővé téve a piaci szereplők számára, hogy úgy járjanak el, mintha egyetlen piacon mozognának, miközben csak a felek egyedi szabályozási rendelkezései vonatkoznak rájuk. (A megállapodás II. melléklete)

A megállapodás 3. cikkének (6) bekezdése értelmében a svájci jegyzékkezelőnek és az uniós központi tisztviselőnek a vonatkozó jogszabályok prioritásainak figyelembevételével meg kell határoznia az összekapcsolás működőképességéhez szükséges műszaki vagy egyéb kérdésekkel kapcsolatos közös üzemeltetési eljárásokat. A jegyzékkezelő és a központi tisztviselő által kidolgozott közös üzemeltetési eljárások a vegyes bizottság határozatával történő elfogadásukat követően lépnek hatályba.

A közös üzemeltetési eljárásokat a vegyes bizottság az 1/2020. számú határozatával fogadta el. Az ebben a dokumentumban rögzítettek szerint az aktualizált közös üzemeltetési eljárásokat a vegyes bizottság az 1/2024. számú határozatával fogadja majd el. E határozat értelmében a vegyes bizottság kéréseivel összhangban a svájci jegyzékkezelő és az uniós központi tisztviselő további technikai iránymutatásokat dolgozott ki és aktualizál majd az összekapcsolás működőképessé tétele érdekében, valamint azért, hogy biztosítsák azoknak a műszaki fejlődéshez, valamint a kapcsolat védelmére és biztonságára, illetve hatékony és eredményes működésére vonatkozó új követelményekhez való folyamatos hozzáigazítását.

2.1. Alkalmazási kör

Ez a dokumentum a megállapodás feleinek közös álláspontját képviseli az EU ETS és a svájci ETS kibocsátásiegység-forgalmi jegyzékei összekapcsolása eljárási alapjainak megteremtése tekintetében. Felvázolja az átfogó eljárási követelményeket az üzemeltetéssel összefüggésben, de szükség lesz további technikai iránymutatásokra is a kapcsolat működőképessé tétele érdekében.

A megfelelő működéshez a kapcsolat műszaki előírásokat igényel működőképességének megőrzése érdekében. A megállapodás 3. cikkének (7) bekezdése szerint ezeket a kérdéseket a Kapcsolástechnikai szabványok című dokumentum részletezi, amelyet külön kell elfogadni a vegyes bizottság határozatával.

A közös üzemeltetési eljárások célja az EU ETS és a svájci ETS kibocsátásiegység-forgalmi jegyzékei közötti kapcsolat működésével összefüggő hatékony és eredményes IT szolgáltatások biztosítása, különösen a szolgáltatáskérések teljesítése, a szolgáltatási hibák orvoslása, a problémák megoldása, valamint a rendszeres üzemeltetési feladatoknak az informatikai szolgáltatások irányítására vonatkozó nemzetközi szabványokkal összhangban történő elvégzése tekintetében.

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolathoz csak a következő közös üzemeltetési eljárásokra lesz szükség, amelyek e dokumentum részét képezik:

- Eseménykezelés
- Problémakezelés
- Kérés teljesítése
- Változáskezelés
- Kiadáskezelés
- Biztonsági események kezelése
- Információbiztonsági irányítás

2.2. Címzettek

E közös üzemeltetési eljárások célközönsége az uniós és a svájci kibocsátásiegység-forgalmi jegyzéket támogató csoportok.

3. MEGKÖZELÍTÉS ÉS ELŐÍRÁSOK

A következő elv alkalmazandó minden közös üzemeltetési eljárás tekintetében:

- Az EU és a Svájci Államszövetség megállapodnak abban, hogy a közös üzemeltetési eljárásokat az ITIL (Information Technology Infrastructure Library, 4. változat) alapján határozzák meg. Az ebben a szabványban foglalt gyakorlatokat újból fel kell használni és hozzá kell igazítani a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolathoz kapcsolódó sajátos igényekhez.
- A közös üzemeltetési eljárások kezeléséhez szükséges kommunikáció és koordináció a két fél között a Svájci Államszövetség és az EU kibocsátásiegység-forgalmi jegyzék ügyfélszolgálatán keresztül történik. A feladatok kiosztására mindig az egyik fél területén belül kerül sor.
- Amennyiben nézeteltérés adódik valamely közös üzemeltetési eljárás kezelésével kapcsolatban, azt mindkét ügyfélszolgálat részvételével elemezni és rendezni kell. Ha nem sikerül egyetértésre jutni, a közös megoldás keresését fel kell terjeszteni a következő szintre.

Felterjesztési szintek	**EU**	**CH**
1. szint	Uniós ügyfélszolgálat	Svájci ügyfélszolgálat
2. szint	Uniós üzemeltetésirányító	Svájci kibocsátásiegység-forgalmi jegyzék alkalmazás irányítója
3. szint	Vegyes bizottság (amely átruházhatja ezt a feladatot a megállapodás 12. cikkének (5) bekezdésére tekintettel)	

4. szint	Vegyes bizottság, a 3. szint átruházása esetén

- Mindegyik fél meghatározhatja a saját kibocsátásiegység-forgalmi jegyzéke működtetésére vonatkozó eljárásokat, figyelembe véve az ezekhez a közös üzemeltetési eljárásokhoz kapcsolódó követelményeket és interfészeket.
- A közös üzemeltetési eljárásokat, így különösen az eseménykezelést, a problémakezelést és a kérések teljesítését, valamint a felek közötti kommunikációt informatikai szolgáltatások irányítási eszköze támogatja.
- Ezenfelül lehetőség van e-mail útján történő információcserére is.
- Mindkét fél gondoskodik arról, hogy az információbiztonsági követelmények teljesüljenek a kezelési utasításokkal összhangban.

4. ESEMÉNYKEZELÉS

Az eseménykezelési folyamat célja az IT szolgáltatásoknak az eseményt követő mihamarabbi visszaállítása a szokásos szolgáltatási szintre, a lehető legkevesebb fennakadást okozva az üzleti tevékenységben.

Az eseménykezelés során továbbá jelentéstételi célokból nyilvántartást kell vezetni az eseményekről, és az eseménykezelésnek össze kell fonódnia más folyamatokkal a folyamatos fejlesztés biztosítása érdekében.

Globális perspektívából szemlélve az eseménykezelés a következő tevékenységeket foglalja magában:

- Események észlelése és rögzítése
- Osztályozás és kezdeti támogatás
- Kivizsgálás és diagnosztizálás
- Rendezés és helyreállítás
- Esemény lezárása

Az eseménykezelési folyamat az esemény teljes életciklusa során felel a felelősségviselés, az ellenőrzés, a nyomon követés és a kommunikáció folyamatos kezeléséért.

4.1. Események észlelése és rögzítése

Az eseményt észlelheti egy támogató csoport, automatizált ellenőrző eszköz vagy a szokásos megfigyelést végző műszaki személyzet.

Az észlelést követően az eseményt rögzíteni kell, és egyedi azonosítót kell hozzárendelni, ami lehetővé teszi az esemény megfelelő nyomon követését és ellenőrzését. Az esemény egyedi azonosítója az eseményt felvető fél (uniós vagy svájci) ügyfélszolgálata által a közös jegyrendszerben hozzárendelt azonosító, amelyet az adott eseménnyel kapcsolatos minden kommunikáció során használni kell.

A kapcsolattartó pont valamennyi esemény vonatkozásában a jegyet naplózó fél ügyfélszolgálata.

4.2. Osztályozás és kezdeti támogatás

Az események osztályozásának célja annak megértése és azonosítása, hogy mely rendszer és/vagy szolgáltatás érintett, és milyen mértékben. A hatékonyság érdekében az osztályozás során az

eseményt már az első alkalommal a megfelelő erőforráshoz kell irányítani az esemény rendezésének felgyorsítása céljából.

Az osztályozási szakaszban sor kerül az esemény besorolására és rangsorolására annak hatása és sürgőssége alapján, a prioritási szempontból releváns időkeret szerinti kezelés érdekében.

Amennyiben az esemény potenciális hatással lehet érzékeny adatok bizalmas kezelésére vagy sértetlenségére és/vagy a rendszer rendelkezésre állására, az eseményt biztonsági eseménynek kell nyilvánítani, majd ezt követően az e dokumentum „Biztonsági események kezelése” című fejezetében leírt eljárás szerint kell kezelni.

Lehetőség szerint a jegyet naplózó ügyfélszolgálat kezdeti diagnosztizálást végez. Ennek során az ügyfélszolgálat megvizsgálja, hogy az esemény ismert hiba-e. Amennyiben igen, a rendezési útvonal vagy a megkerülő megoldás már ismert és dokumentált.

Ha az ügyfélszolgálatnak sikerül megoldania az eseményt, akkor ezen a ponton lényegében lezárja az eseményt, mivel teljesült az eseménykezelés elsődleges célja (nevezetesen a végfelhasználó számára nyújtott szolgáltatás gyors visszaállítása). Ha nem, akkor az ügyfélszolgálat felterjeszti az eseményt a megfelelő rendezési csoporthoz további kivizsgálás és diagnosztizálás érdekében.

4.3. Kivizsgálás és diagnosztizálás

Az események kivizsgálására és diagnosztizálására akkor kerül sor, ha a kezdeti diagnosztizálás során az ügyfélszolgálat nem tudja rendezni az eseményt, ezért azt megfelelő módon felterjesztik. Az események felterjesztése teljes mértékben a kivizsgálási és diagnosztizálási folyamat része.

A kivizsgálási és diagnosztizálási szakaszban általános gyakorlat az esemény ellenőrzött körülmények között történő rekonstruálásának megkísérlése. Az esemény kivizsgálása és diagnosztizálása során fontos megérteni az eseményhez vezető lépések megfelelő sorrendjét.

A felterjesztés annak a felismerése, hogy az esemény nem rendezhető az adott támogatási szinten, és azt át kell adni egy magasabb szintű támogató csoportnak vagy a másik félnek. A felterjesztésnek két útja lehet: vízszintes (funkcionális) vagy függőleges (hierarchikus).

Az eseményt rögzítő és elindító ügyfélszolgálat feladata az esemény felterjesztése a megfelelő erőforráshoz, valamint az esemény általános állapotának és hozzárendelésének nyomon követése.

Az a fél, amelyhez az eseményt hozzárendelték, felel azért, hogy biztosítsa a kért intézkedések kellő időben történő végrehajtását, valamint hogy visszajelzést adjon saját ügyfélszolgálatának.

4.4. Rendezés és helyreállítás

Az események rendezésére és helyreállítására azt követően kerül sor, hogy az eseményt minden részletében megértették. Az esemény megoldásának megtalálása azt jelenti, hogy azonosították a probléma orvoslásának a módját. A megoldás alkalmazása a helyreállítási szakaszban történik.

Miután a megfelelő erőforrások rendezték a szolgáltatási hibát, az eseményt visszairányítják a megfelelő ügyfélszolgálathoz, amely naplózta az eseményt, és amely megerősíti az esemény kezdeményezője felé, hogy a hiba orvoslásra került és az esemény lezárható. Az esemény kezelése során tett megállapításokat rögzíteni kell későbbi felhasználás érdekében.

A helyreállítást végezheti az IT támogató személyzet, illetve arra úgy is sor kerülhet, hogy a végfelhasználót követendő utasításokkal látják el.

4.5. Esemény lezárása

A lezárás az eseménykezelési folyamat utolsó lépése, amelyre röviddel az esemény rendezését követően kerül sor.

A lezárási szakasz során elvégzendő tevékenységek ellenőrzőlistáján az alábbiakat kell kiemelni:

- az eseményhez rendelt kezdeti besorolás ellenőrzése;
- az eseményhez kapcsolódó összes információ megfelelő rögzítése;
- az esemény megfelelő dokumentálása és a tudásbázis frissítése;
- az esemény által közvetlenül vagy közvetve érintett összes érdekelt fél megfelelő tájékoztatása.

Az esemény hivatalos lezárására azt követően kerül sor, hogy az ügyfélszolgálat végrehajtotta az esemény lezárási szakaszt, és erről tájékoztatták a másik felet.

Az esemény lezárását követően nincs mód annak újbóli megnyitására. Amennyiben az esemény rövid időn belül ismételten előfordul, nem kerül sor az eredeti esemény újbóli megnyitására, hanem új eseményt kell naplózni.

Amennyiben az eseményt az uniós és a svájci ügyfélszolgálat is nyomon követi, a végleges lezárás annak az ügyfélszolgálatnak a feladata, amely a jegyet naplózta.

5. PROBLÉMAKEZELÉS

Ezt az eljárást minden alkalommal követni kell, amikor problémát azonosítanak, és ezzel elindul a problémakezelési folyamat. A problémakezelés középpontjában a minőség javítása és a felmerült események mértékének csökkentése áll. Egy probléma egy vagy több esemény oka is lehet. Esemény bejelentésekor az eseménykezelés célja a szolgáltatás mielőbbi helyreállítása, lehetőleg megkerülő megoldások alkalmazásával. Probléma keletkezése esetén a cél a problémát kiváltó ok kivizsgálása egy olyan változtatás meghatározása érdekében, amely biztosítja, hogy a probléma és az ahhoz kapcsolódó események többé ne forduljanak elő.

5.1. A probléma azonosítása és rögzítése

Attól függően, hogy melyik fél kezdeményezte a jegyet, az uniós vagy a svájci ügyfélszolgálat lesz a kapcsolattartó pont a problémával kapcsolatos ügyek vonatkozásában.

A probléma egyedi azonosítója az informatikai szolgáltatások irányítása által hozzárendelt azonosító. Az azonosítót minden esetben használni kell az adott problémával kapcsolatban folytatott kommunikáció során.

A problémát kiválthatja valamilyen esemény, illetve önálló kezdeményezés alapján is regisztrálható a rendszerben bármely időpontban talált hibák kijavítása érdekében.

5.2. A probléma rangsorolása

A problémák az eseményekhez hasonlóan kategóriákba sorolhatók súlyosságuk és prioritásuk szerint, nyomon követésük megkönnyítése érdekében, figyelembe véve a kapcsolódó események hatását és előfordulási gyakoriságát.

5.3. A probléma kivizsgálása és diagnosztizálása

Mindegyik fél felvethet problémát, és a kezdeményező fél ügyfélszolgálata felel a probléma naplózásáért, megfelelő erőforráshoz történő hozzárendeléséért és általános állapotának nyomon követéséért.

A rendezésért felelős csoport, amelyhez a problémát felterjesztették, felel a probléma kellő időben történő kezeléséért és az ügyfélszolgálattal való kommunikációért.

Kérésre mindkét fél köteles biztosítani a meghatározott intézkedések elvégzését, és visszajelzést adni saját ügyfélszolgálatának.

5.4. Rendezés

A rendezésért felelős csoport, amelyhez a problémát hozzárendelték, felel a probléma rendezéséért és saját fele ügyfélszolgálatának megfelelő tájékoztatásáért.

A probléma kezelése során tett megállapításokat rögzíteni kell későbbi felhasználás érdekében.

5.5. A probléma lezárása

A probléma hivatalos lezárására azt követően kerül sor, hogy a problémát rendezik a változtatás végrehajtásával. A probléma lezárási szakaszát az az ügyfélszolgálat végzi, amely a problémát naplózta és tájékoztatta a másik fél ügyfélszolgálatát.

6. KÉRÉS TELJESÍTÉSE

A kérésteljesítési folyamat valamely új vagy meglévő szolgáltatás iránti kérelem végpontok közötti kezelése attól a ponttól, amikor azt rögzítik és jóváhagyják, egészen a lezárásig. A szolgáltatáskérések általában kisebb, előre meghatározott, megismételhető, gyakori, előzetesen jóváhagyott és eljárási kérelmek.

A követendő fő lépések a következők:

6.1. Kérés kezdeményezése

A szolgáltatáskéréssel kapcsolatos információkat e-mail útján, telefonon vagy az informatikai szolgáltatásirányítási eszközön keresztül, illetve bármely más elfogadott kommunikációs csatornán keresztül benyújtják az uniós vagy a svájci ügyfélszolgálatnak.

6.2. Kérés naplózása és elemzése

Minden szolgáltatáskérés esetében a kapcsolattartó pont az uniós vagy a svájci ügyfélszolgálat, attól függően, hogy melyik fél terjesztette elő a szolgáltatáskérést. Ez az ügyfélszolgálat felel a szolgáltatáskérés megfelelő gondossággal történő naplózásáért és elemzéséért.

6.3. Kérés jóváhagyása

A szolgáltatáskérést előterjesztő fél ügyfélszolgálati megbízottja ellenőrzi, hogy szükség van-e a másik fél részéről történő bármilyen jóváhagyásra, és amennyiben igen, akkor eljár annak megszerzése érdekében. Amennyiben a szolgáltatáskérés nem kerül jóváhagyásra, az ügyfélszolgálat frissíti és lezárja a jegyet.

6.4. Kérés teljesítése

Ez a lépés a szolgáltatáskérések hatékony és eredményes kezelésére irányul. Különbséget kell tenni az alábbi esetek között:

- A szolgáltatáskérés teljesítése csak az egyik felet érinti. Ebben az esetben az adott fél megrendeli a munkát és koordinálja a végrehajtást.
- A szolgáltatáskérés teljesítése az EU-t és Svájcot egyaránt érinti. Ebben az esetben az ügyfélszolgálat adja ki a feladatkörébe tartozó munkamegbízásokat. A szolgáltatáskérés teljesítését a két ügyfélszolgálat közösen koordinálja. Az általános felelősség azt az ügyfélszolgálatot terheli, amelyik megkapta és kezdeményezte a szolgáltatáskérést.

A szolgáltatáskérés teljesítését követően azt rendezett státuszúra kell állítani.

6.5. Kérés felterjesztése

Az ügyfélszolgálat szükség esetén felterjesztheti a függőben lévő szolgáltatáskérést a megfelelő erőforráshoz (harmadik félhez).

A felterjesztéseket a megfelelő harmadik felek felé kell megtenni, vagyis az uniós ügyfélszolgálatnak a svájci ügyfélszolgálaton keresztül kell felterjesztést tennie svájci harmadik fél felé, és fordítva.

Az a harmadik fél, amelyhez a szolgáltatáskérést felterjesztették, felel a szolgáltatáskérés kellő időben történő kezeléséért és a szolgáltatáskérést felterjesztő ügyfélszolgálattal való kommunikációért.

A szolgáltatáskérést naplózó ügyfélszolgálat felel a szolgáltatáskérés általános állapotának és hozzárendelésének nyomon követéséért.

6.6. Kérés teljesítésének felülvizsgálata

A felelős ügyfélszolgálat végső minőség-ellenőrzésre benyújtja a szolgáltatáskérési dokumentumokat azok lezárása előtt. Meg kell bizonyosodni arról, hogy a szolgáltatáskérés ténylegesen feldolgozásra került, és hogy a kérés életciklusának- leírásához szükséges összes információt kellő részletességgel benyújtották. Ezenfelül a kérés feldolgozása során tett megállapításokat rögzíteni kell későbbi felhasználás érdekében.

6.7. Kérés lezárása

Amennyiben a megjelölt felek egyetértenek abban, hogy a szolgáltatáskérés teljesült, és a kérelmező is rendezettnek tekinti az ügyet, a „Lezárva” státuszt kell beállítani.

A szolgáltatáskérés hivatalos lezárására azt követően kerül sor, hogy a szolgáltatáskérést naplózó ügyfélszolgálat végrehajtotta a kérés lezárási szakaszt, és erről tájékoztatták a másik fél ügyfélszolgálatát.

7. VÁLTOZÁSKEZELÉS

Biztosítani kell szabványosított módszerek és eljárások alkalmazását az IT infrastruktúra irányítását érintő valamennyi változtatás hatékony és azonnali kezelésére annak érdekében, hogy minimálisra lehessen csökkenteni a kapcsolódó események számát és azok szolgáltatásra gyakorolt hatását. Az IT infrastruktúrában bekövetkező változások felléphetnek reaktív jelleggel, problémákra vagy külső fél által megszabott követelményekre – pl. jogszabályi változásokra – válaszul, vagy proaktív módon, a hatékonyság és eredményesség javítására törekedve, illetve üzleti kezdeményezések lehetővé tétele vagy figyelembevétele érdekében.

A változáskezelési folyamat különböző lépésekből áll, amelyek során a változtatás iránti kérelem minden részletét rögzítik a jövőbeni nyomon követés érdekében. Ezek a folyamatok biztosítják, hogy sor kerüljön a változtatás jóváhagyására és tesztelésére még annak bevezetése előtt. A kiadáskezelési folyamat biztosítja a sikeres bevezetést.

7.1. Változtatási kérelem

A változtatási kérelmet a változáskezelési csoporthoz kell benyújtani ellenőrzésre és jóváhagyásra. Minden változtatási kérelem esetében a kapcsolattartó pont az uniós vagy a svájci ügyfélszolgálat, attól függően, hogy melyik fél terjesztette elő a változtatási kérelmet. Ez az ügyfélszolgálat felel a változtatási kérelem megfelelő gondossággal történő naplózásáért és elemzéséért.

A változtatási kérelmek a következőkön alapulhatnak:

- változást okozó esemény;
- meglévő probléma, amely változást eredményez;
- egy végfelhasználó új változtatást kér;
- folyamatban lévő karbantartás eredményeképp bekövetkező változás;
- jogszabályi változás.

7.2. Változás értékelése és tervezése

Ebben a szakaszban kerül sor a változások értékeléséhez és tervezéséhez kapcsolódó tevékenységekre. Rangsorolási és tervezési tevékenységeket foglal magában a kockázatok és hatások minimálisra csökkentése érdekében.

Ha a változtatási kérelem végrehajtása az EU-t és a Svájci Államszövetséget is érinti, a változtatási kérelmet naplózó fél a másik féllel ellenőrzi a változás értékelését és tervezését.

7.3. Változás jóváhagyása

Minden rögzített változtatási kérelem esetében szükség van a megfelelő felterjesztési szint jóváhagyására.

7.4. Változás végrehajtása

A változás végrehajtására a kiadáskezelési folyamat során kerül sor. Mindkét fél kiadáskezelési csoportja a saját eljárását követi, amely magában foglalja a tervezést és a tesztelést. A változás felülvizsgálatára a végrehajtást követően kerül sor. A meglévő változáskezelési folyamatot állandóan ellenőrizni és szükség szerint frissíteni kell annak biztosítása érdekében, hogy minden a terv szerint történjen.

8. KIADÁSKEZELÉS

A kiadás valamely információtechnológiai szolgáltatásban eszközölt egy vagy több változtatás, amelyeket a kiadási tervben gyűjtenek össze, és amelyeket együttesen kell engedélyezni, előkészíteni, felépíteni, tesztelni és bevezetni. Egy kiadás magában foglalhat egy hibajavítást, a hardver vagy más alkatrészek megváltoztatását, a szoftver módosításait, az alkalmazási verziók frissítéseit, a dokumentációban és/vagy a folyamatokban eszközölt változtatásokat. Az egyes kiadások tartalmát önálló egységként kezelik, tesztelik és telepítik.

A kiadáskezelés célja a tervezett szolgáltatások megtervezése, létrehozása, tesztelése és ellenőrzése, valamint a szolgáltatásnyújtáshoz szükséges képesség biztosítása, ezáltal pedig az érdekelt felek elvárásainak teljesítése és a kitűzött célok elérése. A szolgáltatásban eszközölt valamennyi változtatás vonatkozásában az elfogadási kritériumok a tervezési koordináció során kerülnek meghatározásra és dokumentálásra, majd azokat közlik a kiadáskezelési csoportokkal.

A kiadás általában több probléma kijavítását és szolgáltatásfejlesztéseket foglal magában. Tartalmazza a kért új vagy módosított szoftvert, valamint a jóváhagyott változtatások végrehajtásához szükséges bármely új vagy módosított hardvert.

8.1. Kiadás tervezése

A folyamat első lépése során az engedélyezett változtatásokat kiadási csomagokhoz rendelik hozzá, és meghatározzák a kiadások alkalmazási körét és tartalmát. Ezen információk alapján a kiadástervezési alfolyamat- során meghatározzák a kiadás létrehozásának, tesztelésének és telepítésének az ütemtervét.

A tervezés során meg kell határozni a következőket:

- a kiadás alkalmazási köre és tartalma;
- a kiadásra vonatkozó kockázatértékelés és kockázati profil;
- a kiadás által érintett ügyfél/felhasználók;
- a kiadásért felelős csoport;
- teljesítési és telepítési stratégia;
- a kiadáshoz és a telepítéshez szükséges erőforrások.

A felek tájékoztatják egymást kiadástervezési és -karbantartási időszakaikról. Amennyiben egy kiadás az EU-t és a Svájci Államszövetséget is érinti, a felek összehangolják a tervezést és közös karbantartási időszakot határoznak meg.

8.2. Kiadási csomag létrehozása és tesztelése

A kiadáskezelési folyamat létrehozási és tesztelési lépése a kiadás vagy a kiadási csomag végrehajtására és a gyártást megelőzően az ellenőrzött környezetek fenntartására, valamint az összes kiadott környezetben bekövetkezett összes változás tesztelésére vonatkozó megközelítést alkalmaz.

Amennyiben egy kiadás az EU-t és a Svájci Államszövetséget is érinti, összehangolják a teljesítési terveket és a teszteket. Ez a következő szempontokra terjed ki:

- hogyan és mikor kerülnek teljesítésre a kiadási egységek és a szolgáltatási elemek;
- Melyek a tipikus átfutási idők; mi történik késedelem esetén;
- hogyan kell nyomon követni a teljesítés előrehaladását és hogyan kell megerősítést szerezni;

- mérési módszer a kiadás telepítésére irányuló erőfeszítések sikerének nyomon követésére és meghatározására;
- gyakori tesztelési esetek a releváns funkciók és változtatások vonatkozásában.

Ennek az alfolyamatnak a végén minden szükséges kiadási elem készen áll az élesben történő telepítés szakaszára.

8.3. Telepítés előkészítése

Az előkészítési alfolyamat biztosítja a kommunikációs tervek helyes meghatározását, valamint hogy az értesítések készen álljanak arra, hogy elküldjék őket az összes érdekelt félnek és érintett végfelhasználónak, valamint hogy a kiadás beépüljön a változáskezelési folyamatba annak érdekében, hogy minden változtatás ellenőrzött módon kerüljön elvégzésre, és jóváhagyják a szükséges fórumok.

Amennyiben egy kiadás az EU-t és a Svájci Államszövetséget is érinti, összehangolják a következő tevékenységeket:

- változtatási kérelmek nyilvántartása a gyártási környezetbe való telepítés ütemezése és előkészítése érdekében;
- végrehajtási terv elkészítése;
- visszamenőleges megközelítés annak érdekében, hogy a telepítés meghiúsulása esetén visszaállítható legyen a korábbi állapot;
- értesítés küldése az összes szükséges félnek;
- jóváhagyás kérése a kiadás végrehajtására a megfelelő felterjesztési szinttől.

8.4. Kiadás visszavonása

Ha a telepítés meghiúsul, vagy ha a tesztelés során megállapításra kerül, hogy a telepítés sikertelen volt vagy nem felelt meg a megállapodás szerinti elfogadási / minőségi kritériumoknak, mindkét fél kiadáskezelési csoportjának vissza kell térnie az előző állapothoz. Tájékoztatni kell az összes szükséges érdekelt felet, köztük az érintett / megcélzott végfelhasználókat. A jóváhagyás függvényében a folyamat bármelyik korábbi szakaszban újraindulhat.

8.5. Kiadás felülvizsgálata és lezárása

A telepítés felülvizsgálata során a következő tevékenységeket kell elvégezni:

- visszajelzések fogadása a telepítéssel kapcsolatos fogyasztói, felhasználói és szolgáltatásnyújtási elégedettségről (a visszajelzések összegyűjtése és figyelembevétele a szolgáltatás folyamatos javítása érdekében);
- minden olyan minőségi kritérium áttekintése, amely nem teljesült;
- annak ellenőrzése, hogy minden intézkedés, szükséges javítás és változtatás befejeződött-e;
- annak biztosítása, hogy a telepítés végén ne legyenek a képességgel, az erőforrásokkal, a kapacitással vagy a teljesítménnyel kapcsolatos problémák;
- annak ellenőrzése, hogy az ügyfél, a végfelhasználók, az operatív támogatás és egyéb érintett felek dokumentáltak és elfogadtak minden problémát, ismert hibát és megkerülő megoldást;
- a telepítés által okozott események és problémák ellenőrzése (korai támogatás nyújtása az operatív csoportoknak arra az esetre, ha a kiadás a munka mennyiségének növekedését okozta);
- a támogató dokumentumok frissítése (pl. műszaki adatközlő lapok);
- a kiadás telepítésének hivatalos átadása a szolgáltatásüzemeltetésnek;

- a tapasztalatok dokumentálása;
- a kiadás összefoglaló dokumentumának begyűjtése a végrehajtó csoportoktól;
- a kiadás hivatalos lezárása a változtatási kérelmek nyilvántartásának ellenőrzése után.

9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A biztonsági események kezelése az a folyamat, amelynek célja a biztonsági események kezelése a következők lehetővé tétele érdekében: az esemény közlése a potenciálisan érintett érdekelt felekkel; az esemény értékelése és rangsorolása; valamint az eseményre adott válasz az érzékeny információs eszközök bizalmas jellege, rendelkezésre állása vagy sértetlensége bármely tényleges, vélt vagy lehetséges megsértésének rendezése érdekében.

9.1. Információbiztonsági esemény besorolása

Az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kapcsolatot érintő összes eseményt elemezni kell, hogy meg lehessen állapítani az érzékeny információk jegyzékében rögzített bármely érzékeny információ bizalmas jellegének, sértetlenségének vagy rendelkezésre állásának esetleges megsértését.

Ilyen esetben az eseményt információbiztonsági eseményként kell jellemezni, haladéktalanul rögzíteni kell az informatikai szolgáltatások irányítási eszközében és ennek megfelelően kell kezelni.

9.2. Információbiztonsági esemény kezelése

A biztonsági események a 3. felterjesztési szint felelősségi körébe tartoznak, az események rendezésével pedig külön eseménykezelő csoport foglalkozik.

Az eseménykezelő csoport a következőkért felel:

- az esemény első elemzése, besorolása és súlyosságának osztályozása;
- intézkedések koordinálása az összes érdekelt fél között, beleértve az eseményelemzés, az esemény kezelésére irányuló döntések és az esetlegesen azonosított gyengeségek teljes dokumentálását;
- a biztonsági esemény súlyosságától függően az esemény kellő időben történő felterjesztése a megfelelő tájékoztatási és/vagy döntési szintre.

Az információbiztonsági irányítási folyamat során az eseményekre vonatkozó összes információ a legmagasabb érzékenységi szinten kerül besorolásra, de semmiképpen sem sorolható be ÉRZÉKENY: *ETS* szint alatt.

Folyamatban lévő kivizsgálás esetén és/vagy kihasználható gyengeség esetén annak orvoslásáig az információ KÜLÖNLEGES KEZELÉST IGÉNYLŐ: *ETS kritikus* besorolásba kerül.

9.3. Biztonsági esemény azonosítása

A biztonsági esemény típusa alapján az információbiztonsági tisztviselő meghatározza azokat a megfelelő szervezeteket, amelyeket be kell vonni, és amelyeknek részt kell venniük az eseménykezelő csoportban.

9.4. Biztonsági esemény elemzése

Az eseménykezelő csoport kapcsolatot tart fenn az összes érintett szervezettel és adott esetben azok csoportjainak megfelelő tagjaival az esemény felülvizsgálata érdekében. Az elemzés során meg kell határozni, hogy milyen mértékben sérült az adott eszköz bizalmas jellege, integritása vagy

rendelkezésre állása, és értékelni kell az összes érintett szervezetre gyakorolt hatást. Ezt követően meg kell határozni az esemény rendezéséhez és hatásának kezeléséhez szükséges kezdeti és nyomonkövetési intézkedéseket, ideértve ezeknek az intézkedéseknek az erőforrásokra gyakorolt hatását is.

9.5. Biztonsági esemény súlyosságának meghatározása, felterjesztése és bejelentése

Az eseménykezelő csoport értékeli minden új biztonsági esemény súlyosságát azok besorolását követően, majd megteszi a haladéktalanul szükséges intézkedéseket az esemény súlyosságának függvényében.

9.6. Biztonsági reagálási jelentés

Az információbiztonsági eseményre való reagálásról szóló jelentésben az eseménykezelő csoport leírja az esemény megfékezésével és helyreállításával kapcsolatban elért eredményeket. A jelentést biztonságos e-mail vagy más kölcsönösen elfogadott biztonságos kommunikációs eszköz útján továbbítják a 3. felterjesztési szinthez.

A felelős fél áttekinti az esemény megfékezésével és helyreállításával kapcsolatban elért eredményeket és:

- korábbi szétkapcsolás esetén ismételten csatlakoztatja a kibocsátásiegység-forgalmi jegyzéket;
- tájékoztatást nyújt az eseményekről a kibocsátásiegység-forgalmi jegyzék csoportjainak;
- lezárja az eseményt.

Az eseménykezelő csoportnak biztonságos módon meg kell adnia a megfelelő adatokat az információbiztonsági eseményről szóló jelentésben annak érdekében, hogy biztosítsa a következetes nyilvántartást és kommunikációt, valamint hogy lehetővé tegye az esemény megfékezésére irányuló gyors és megfelelő intézkedést. Az eseménykezelő csoport kellő időben rendelkezésre bocsátja az információbiztonsági eseményről szóló végleges jelentést annak elkészítését követően.

9.7. Ellenőrzés, kapacitásépítés és folyamatos fejlesztés

Az eseménykezelő csoport minden biztonsági eseményről jelentést tesz a 3. felterjesztési szint felé. A jelentések alapján ez a felterjesztési szint meghatározza a következőket:

- gyenge pontok a biztonsági ellenőrzésben és/vagy az üzemeltetésben, amelyeket meg kell erősíteni;
- ezen eljárás megerősítésének esetleges szükségessége, az eseményekre való reagálás hatékonyságának javítása érdekében;
- képzési és kapacitásépítési lehetőségek a kibocsátásiegység-forgalmi jegyzékek információbiztonsági ellenálló képességének további megerősítése, a jövőbeni események kockázatának csökkentése és hatásának minimalizálása érdekében.

10. INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁS

Az információbiztonsági irányítás célja a szervezetek minősített információi, adatai és IT szolgáltatásai bizalmas jellegének, sértetlenségének és rendelkezésre állásának a biztosítása. A tervezést és a tesztelést is magukban foglaló műszaki elemeken felül (lásd a kapcsolástechnikai szabványokat) az alábbi közös üzemeltetési eljárásokra van szükség a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolatra vonatkozó biztonsági követelmények teljesítéséhez.

10.1. Érzékeny információk azonosítása

Adott információ érzékenységének értékelésére az információval kapcsolatos biztonság megsértése által az üzleti tevékenységre gyakorolt lehetséges hatás (pl. pénzügyi veszteségek, arculatromlás, jogszabályok megsértése...) szintjének meghatározásával kerül sor.

Az érzékeny információs eszközöket az összekapcsolásra gyakorolt hatásuk alapján kell meghatározni.

Ennek az információnak az érzékenységi szintjét az erre az összekapcsolásra alkalmazandó érzékenységi skála alapján kell meghatározni, amelynek a leírását e dokumentum „Információbiztonsági esemény kezelése” című része tartalmazza.

10.2. Az információs eszközök érzékenységi szintjei

Az információs eszköz azonosításakor sor kerül annak osztályozására az alábbi szabályok alkalmazásával:

- legalább egy MAGAS bizalmassági, sértetlenségi vagy rendelkezésreállási szint azonosítása esetén az eszköz KÜLÖNLEGES KEZELÉST IGÉNYLŐ: *ETS kritikus* besorolást kap;
- legalább egy KÖZEPES bizalmassági, sértetlenségi vagy rendelkezésreállási szint azonosítása esetén az eszköz ÉRZÉKENY: *ETS* besorolást kap;
- csak ALACSONY bizalmassági, sértetlenségi vagy rendelkezésreállási szintek azonosítása esetén az eszköz Jelölés az EU-ban: ÉRZÉKENY: *ETS közös közbeszerzés* besorolást kap. Jelölés Svájcban: KORLÁTOZOTT HOZZÁFÉRÉSŰ: ETS.

10.3. Az információs eszköz tulajdonosának hozzárendelése

Minden információs eszköznek hozzárendelt tulajdonossal kell rendelkeznie. Az ETS azon információs eszközeit, amelyek az EUTL és az SSTL közötti kapcsolathoz tartoznak vagy ahhoz kapcsolódnak, a két fél által fenntartott közös eszközleltárjegyzékbe kell felvenni. Az ETS azon információs eszközeit, amelyek az EUTL és az SSTL közötti kapcsolaton kívül esnek, az adott fél által fenntartott eszközleltárjegyzékbe kell felvenni.

A feleknek meg kell állapodniuk az EUTL és az SSTL közötti kapcsolathoz tartozó vagy ahhoz kapcsolódó minden egyes információs eszköz tulajdonosa tekintetében. Az információs eszköz tulajdonosának feladata az információs eszköz érzékenységének értékelése.

A tulajdonosnak a hozzárendelt eszköz(ök) értékének megfelelő szintű munkatapasztalattal kell rendelkeznie. Formális keretek között megállapodásra kell jutni a tulajdonosnak az eszközzel (eszközökkel) kapcsolatos felelősségével és a szükséges bizalmassági, sértetlenségi és rendelkezésreállási szint fenntartására vonatkozó kötelezettségével kapcsolatban.

10.4. Érzékeny információk nyilvántartása

Minden érzékeny információt rögzíteni kell az érzékeny információk jegyzékében.

Adott esetben figyelembe kell venni az érzékeny információk összesítését, amely nagyobb hatást eredményezhet, mint egyetlen információ, és rögzíteni kell az érzékeny információk jegyzékében (pl. a rendszer adatbázisban tárolt információkészlet).

Az érzékeny információk jegyzéke nem statikus. A fenyegetések, sebezhetőségek, az eszközökkel kapcsolatos biztonsági események valószínűsége vagy következményei minden jel nélkül megváltozhatnak, és új eszközök kerülhetnek bevezetésre a jegyzékrendszerek üzemeltetésében.

Ezért az érzékeny információk jegyzékét rendszeresen felül kell vizsgálni, és minden érzékenynek minősített információt haladéktalanul rögzíteni kell az érzékeny információk jegyzékében.

Az érzékeny információk jegyzékének minden rögzített tétel tekintetében legalább a következőket kell tartalmaznia:

- az információ leírása;
- az információ tulajdonosa;
- érzékenységi szint;
- annak feltüntetése, hogy az információ tartalmaz-e személyes adatokat;
- szükség esetén további információk.

10.5. Érzékeny információk kezelése

Amennyiben az érzékeny információ feldolgozására az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kapcsolaton kívül kerül sor, az érzékeny információt a kezelési utasításokkal összhangban kell kezelni.

Az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kapcsolat útján feldolgozott érzékeny információkat a felek biztonsági követelményeivel összhangban kell kezelni.

10.6. Hozzáférés-kezelés

A hozzáférés-kezelés célja, hogy az engedéllyel rendelkező felhasználók számára jogot biztosítson valamely szolgáltatás igénybevételére, miközben megakadályozza illetéktelen felhasználók hozzáférését. A hozzáférés-kezelést időnként a „jogkezelés” vagy a „személyazonosság-kezelés” kifejezéssel jelölik.

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat és annak üzemeltetése vonatkozásában mindkét félnek hozzáféréssel kell rendelkeznie a következő komponensekhez:

- Wiki: Együttműködési környezet általános információk – pl. kiadástervezés – cseréjéhez;
- informatikai szolgáltatások irányítási eszköze események és problémák kezeléséhez (lásd a „Megközelítés és előírások” című 3. fejezetet);
- Üzenetváltási rendszer: mindegyik Fél biztonságos üzenetváltási rendszert biztosít az ügyleti adatokat tartalmazó üzenetek továbbításához.

A svájci jegyzékkezelő és az uniós központi tisztviselő biztosítja, hogy a hozzáférések naprakészek legyenek, és feleik vonatkozásában kapcsolattartó pontként járnak el a hozzáférés-kezelési tevékenységeket illetően. A hozzáférési kérelmeket a kérésteljesítési eljárások szerint kezelik.

10.7. Tanúsítvány- / Kulcskezelés

Mindegyik fél felel a saját tanúsítvány- / kulcskezeléséért (tanúsítványok / kulcsok létrehozása, nyilvántartása, tárolása, telepítése, használata, megújítása, visszavonása, biztonsági mentése és helyreállítása). Amint az a kapcsolástechnikai szabványokban szerepel, csak mindkét fél által megbízhatónak tartott tanúsító hatóság által kiállított elektronikus tanúsítványok használhatók. A tanúsítványok / kulcsok kezelését és tárolását a kezelési utasításokban foglalt rendelkezések szerint kell végezni.

A tanúsítványok és kulcsok visszavonását és/vagy megújítását mindkét félnek koordinálnia kell. Ez a kérésteljesítési eljárásokkal összhangban történik.

A svájci jegyzékkezelő és az uniós központi tisztviselő között biztonságos kommunikációs eszközök útján kerül sor a tanúsítványok / kulcsok kicserélésére, a kezelési utasításokban foglalt rendelkezésekkel összhangban.

A tanúsítványok / kulcsok bármilyen módon történő hitelesítése független csatornán keresztül történik.

III. MELLÉKLET

KAPCSOLÁSTECHNIKAI SZABVÁNYOK (LTS-EK)

az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás 3. cikkének (7) bekezdése alapján

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolatra vonatkozó előírás

Tartalomjegyzék

1. Glosszárium 31
2. Bevezetés 33
2.1. Alkalmazási kör 33
2.2. Címzettek 34
3. Általános rendelkezések 34
3.1. A kommunikációs kapcsolat architektúrája 34
3.1.1. Üzenetváltás 34
3.1.2. XML üzenet – Magas szintű leírás 34
3.1.3. Befogadási ablakok 35
3.1.4. Ügyleti üzenetek folyamata 35
3.2. Adatátvitel biztonsága 38
3.2.1. Tűzfal és hálózati összekapcsolás 38
3.2.2. Virtuális magánhálózat (VPN) 39
3.2.3. IPSec megvalósítása 39
3.2.4. Biztonságos üzenettovábbítási protokoll. 39
3.2.5. XML titkosítás és aláírás 39
3.2.6. Rejtjelezési kulcsok 40
3.3. A kapcsolat keretében végzett funkciók listája 40
3.3.1. Üzleti ügyletek 40
3.3.2. Egyeztetési protokoll 41
3.3.3. Próbaüzenet 41
3.4. Adatnaplózási követelmények 41
3.5. Üzemeltetési követelmények 42
4. Elérhetőségre vonatkozó rendelkezések 43
4.1. A kommunikáció elérhetőségének tervezése 43
4.2. Kezdeményezés, kommunikáció, újbóli aktiválás és vizsgálati terv 43

4.2.1. Belső IKT-infrastruktúra vizsgálatok 44
4.2.2. Kommunikációs vizsgálatok 44
4.2.3. Az egész rendszerre kiterjedő (végpontok közötti) vizsgálatok 44
4.2.4. Biztonsági tesztek 45
4.3. Elfogadási/Tesztelési környezetek 45
5. Titoktartásra és sértetlenségre vonatkozó rendelkezések 46
5.1. Biztonsági tesztelési infrastruktúra 46
5.2. A kapcsolat felfüggesztésére és újbóli aktiválására vonatkozó rendelkezések 46
5.3. A biztonság megsértésére vonatkozó rendelkezések 47
5.4. Biztonsági tesztelésre vonatkozó útmutató 47
5.4.1. Szoftver 47
5.4.2. Infrastruktúra 48
5.5. Kockázatértékelésre vonatkozó rendelkezések 48

1. GLOSSZÁRIUM

1-1. táblázat: Üzleti rövidítések és fogalommeghatározások

Rövidítés/Kifejezés	Fogalommeghatározás
Kibocsátási egység	Egy meghatározott időszakban egy szén-dioxid tonna-egyenérték kibocsátására való jogosultság, amely az egyik ETS követelményeinek teljesítésére érvényes.
CH	Svájci Államszövetség
CHU	Helyhez kötött kibocsátási egység típusa, más néven CHU2 (a kiotói jegyzék 2. kötelezettségvállalási időszakára utalva), svájci kibocsátások vonatkozásában.
CHUA	Svájci légi közlekedési kibocsátási egység
COP	Közös üzemeltetési eljárások Közösen kidolgozott eljárások az EU ETS és a svájci ETS összekapcsolásának működőképessé tételére.
ETR	Kibocsátásiegység-forgalmi jegyzék
ETS	Kibocsátáskereskedelmi rendszer
EU	Európai Unió

Rövidítés/Kifejezés	Fogalommeghatározás
EUA	EU általános célú kibocsátási egység
EUAA	EU légi közlekedési kibocsátási egység
EUTL	Európai uniós ügyleti jegyzőkönyv
Kibocsátásiegység-forgalmi jegyzék	Az ETS keretében kiadott kibocsátási egységek elszámolására szolgáló rendszer, amely nyomon követi az elektronikus számlákon tartott kibocsátási egységek tulajdonosait.
SSTL	Svájci kiegészítő ügyleti jegyzőkönyv
Ügylet	Olyan folyamat a kibocsátásiegység-forgalmi jegyzékben, amelynek keretében kibocsátási egységet vezetnek át egy számláról egy másikra.
Ügyleti jegyzőkönyv rendszer	Az ügyleti jegyzőkönyv feljegyzést tartalmaz az egyik kibocsátásiegység-forgalmi jegyzékből a másikba küldött minden egyes javasolt ügyletről.

1-2. táblázat: Műszaki rövidítések és fogalommeghatározások

Rövidítés	Fogalommeghatározás
Nyilvános kulcsú kriptográfia	Nyilvános és magánkulcsokat használ adatok titkosításához és visszafejtéséhez.
Tanúsító hatóság	Elektronikus tanúsítványokat kiállító szervezet.
Rejtjelezési kulcs	A rejtjelezési algoritmus funkcionális kimenetét meghatározó információ.
Visszafejtés	A titkosítással ellentétes folyamat.
Digitális aláírás	Üzenet, szoftver vagy elektronikus dokumentum eredetiségének és sértetlenségének a hitelesítésére alkalmazott matematikai módszer.
Titkosítás	Információk vagy adatok kóddá történő átalakítása, különösen jogosulatlan hozzáférés megakadályozása érdekében.
Fájl beolvasása	A fájl olvasásának folyamata.
Tűzfal	Hálózatbiztonsági készülék vagy szoftver, amely felügyeli és szabályozza a bejövő és kimenő hálózati forgalmat előre meghatározott szabályok alapján.
Szívdobbanás-felügyelet	Hardware vagy szoftver által létrehozott vagy felügyelt időszakos jel az üzemszerű működés jelzése vagy a számítógépes rendszer egyéb részeinek szinkronizálása érdekében.
IPSEC	IP biztonság. Hálózati protokollkészlet, amely hitelesíti és titkosítja az adatcsomagokat két számítógép között IP-hálózaton keresztül történő biztonságos, titkosított kommunikáció biztosítása érdekében.
Behatolási tesztelés	Számítógépes rendszer, hálózat vagy webes alkalmazás támadók által kihasználható biztonsági sebezhetőségeinek felderítésére irányuló tesztelés.
Egyeztetési folyamat	Folyamat, amely biztosítja az egyezést két külön nyilvántartás között.
VPN	Virtuális magánhálózat.

Rövidítés	Fogalommeghatározás
XML:	Bővíthető jelölőnyelv. Lehetővé teszi a tervezők számára saját, személyre szabott címkék létrehozását, lehetővé téve adatok meghatározását, továbbítását, hitelesítését és értelmezését alkalmazások között, valamint szervezetek között.

2. BEVEZETÉS

Az Európai Unió és a Svájci Államszövetség közötti 2017. november 23-i, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás (a továbbiakban: a megállapodás) rendelkezik az uniós kibocsátáskereskedelmi rendszerben (a továbbiakban: EU ETS) vagy a svájci kibocsátáskereskedelmi rendszerben (a továbbiakban: svájci ETS) felhasználható kibocsátási egységek kölcsönös elismeréséről. Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében létre kell hozni az uniós kibocsátásiegység-forgalmi jegyzék európai uniós ügyleti jegyzőkönyve (EUTL) és a svájci kibocsátásiegység-forgalmi jegyzék svájci kiegészítő ügyleti jegyzőkönyve (SSTL) közötti közvetlen kapcsolatot, amely lehetővé teszi a két ETS bármelyikében kiadott kibocsátásiegység-forgalmi jegyzékek egymás közötti átruházását (a megállapodás 3. cikkének (2) bekezdése). Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében 2020-ban egy átmeneti megoldást vezettek be. 2023-tól a két kibocsátáskereskedelmi rendszer közötti kapcsolat fokozatosan kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolattá alakul, amelyet várhatóan legkésőbb 2024-ig kell megvalósítani. Ezáltal lehetővé válik az összekapcsolt piacok működése a piaci likviditásból származó előnyök és a két összekapcsolt rendszer közötti ügyletek végrehajtása tekintetében, oly módon, hogy tulajdonképpen két rendszerből álló egyetlen piacként funkcionál, lehetővé téve a piaci szereplők számára, hogy úgy járjanak el, mintha egyetlen piacon mozognának, miközben csak a felek egyedi szabályozási rendelkezései vonatkoznak rájuk (a megállapodás II. melléklete).

A megállapodás 3. cikkének (7) bekezdése értelmében a svájci jegyzékkezelő és az uniós központi tisztviselő a megállapodás II. mellékletben foglalt elveken alapuló kapcsolástechnikai szabványokat (LTS-ek) dolgoz ki, amelyek tartalmazzák az SSTL és az EUTL közötti stabil és biztonságos kapcsolat létrehozásának részletes követelményeit. A jegyzékkezelő és a központi tisztviselő által kidolgozott LTS-ek azt követően lépnek hatályba, amikor a vegyes bizottság a határozatával elfogadja azokat.

A kapcsolástechnikai szabványokat a vegyes bizottság a 2/2020. számú határozatával fogadta el. Az ebben a dokumentumban rögzítettek szerint az aktualizált kapcsolástechnikai szabványokat a vegyes bizottság az 1/2024. számú határozatával fogadja majd el. E határozat értelmében a vegyes bizottság kéréseivel összhangban a svájci jegyzékkezelő és az uniós központi tisztviselő további technikai iránymutatásokat dolgozott ki és aktualizál majd az összekapcsolás működőképessé tétele érdekében, valamint azért, hogy biztosítsák azoknak a műszaki fejlődéshez, valamint a kapcsolat védelmére és biztonságára, illetve hatékony és/vagy eredményes működésére vonatkozó új követelményekhez való folyamatos hozzáigazítását.

2.1. Alkalmazási kör

Ez a dokumentum a megállapodás feleinek közös álláspontját képviseli az EU ETS és a svájci ETS kibocsátásiegység-forgalmi jegyzékei összekapcsolása műszaki alapjainak megteremtése tekintetében. Miközben felvázolja a műszaki előírások kiindulási alapját az architektúrára, a

szolgáltatásra és a biztonságra vonatkozó követelményekkel összefüggésben, szükség lesz további részletes iránymutatásokra is a kapcsolat működőképessé tétele érdekében.

A megfelelő működéshez a kapcsolat folyamatokat és eljárásokat igényel az összekapcsolás további működőképessége érdekében. A megállapodás 3. cikkének (6) bekezdése szerint ezeket a kérdéseket a közös üzemeltetési eljárásokat tartalmazó külön dokumentum részletezi, amelyet a vegyes bizottság fogad el a határozatával.

2.2. Címzettek

E dokumentum címzettje a svájci jegyzékkezelő és az uniós központi tisztviselő.

3. ÁLTALÁNOS RENDELKEZÉSEK

3.1. A kommunikációs kapcsolat architektúrája

E szakasz célja, hogy ismertesse az EU ETS és a svájci ETS közötti kapcsolat és annak különböző alkotóelemei működőképessé tételének általános architektúráját.

Mivel a biztonság az architektúra meghatározásának kulcsfontosságú eleme, minden intézkedés megtételére sor került a stabil architektúra biztosítása érdekében. A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat fájlcserélő mechanizmust alkalmaz a biztonságos légréskapcsolat megvalósításaként.

A műszaki megoldás az alábbiakat alkalmazza:

- Biztonságos üzenettovábbítási protokoll.
- XML üzenetek.
- XML alapú digitális aláírás és titkosítás.
- VPN.

Az alábbi leírás átfogó képet fest a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat architektúrájáról:

3.1.1. Üzenetváltás

Az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kommunikáció üzenetváltási mechanizmuson alapul, biztonságos csatornákon keresztül. Mindkét oldal saját adattárral rendelkezik a beérkező üzenetek számára.

Mindkét Fél nyilvántartást vezet a beérkező üzenetekről és a feldolgozási adatokról.

A hibákat és a váratlan állapotokat figyelmeztetés formájában jelenteni kell, és szükség van a támogató csoportok közötti emberi kapcsolatra.

A hibák és a váratlan események kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt eseménykezelési folyamatban meghatározott üzemeltetési eljárásokat.

3.1.2. XML üzenet – Magas szintű leírás

Az XML üzenet az alábbiak egyikét tartalmazza:

- egy vagy több ügyleti kérelem és/vagy egy vagy több ügyleti válaszadás,
- egy művelet/válasz az egyeztetéshez kapcsolódóan,

- egy próbaüzenet.

Minden üzenet a következőket tartalmazó fejléccel rendelkezik:

- származási ETS rendszer,
- sorszám.

3.1.3. Befogadási ablakok

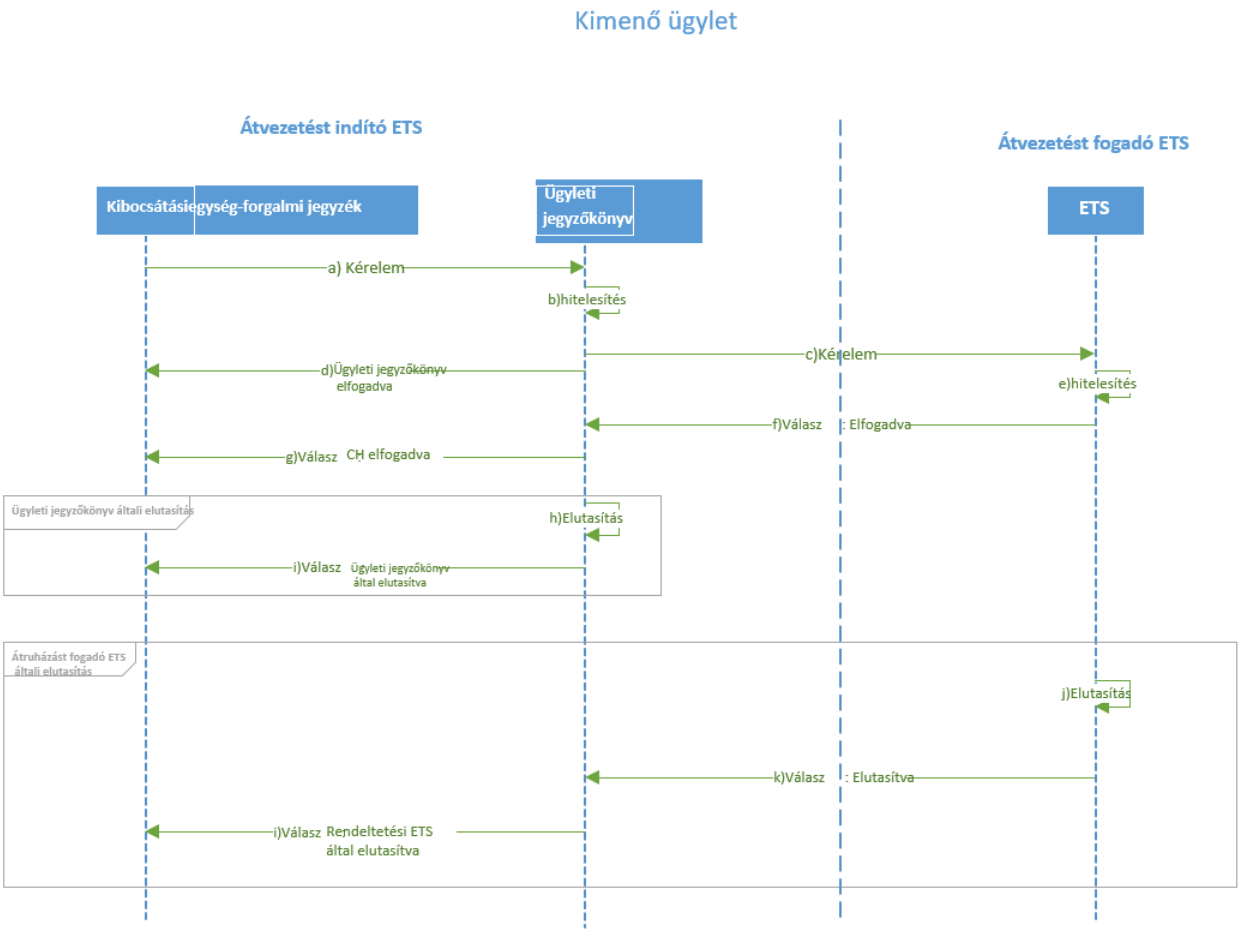
A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat előre meghatározott befogadási ablakokon alapul, amelyeket megnevezett események csoportja követ. A kapcsolaton keresztül beérkező ügyleti kérelmek csak előre meghatározott időközönként kerülnek befogadásra, ami magában foglalja a kimenő és a bejövő ügyletek műszaki érvényesítését. Ezenfelül napi szintű egyeztetésekre kerülhet sor, amelyek manuálisan kezdeményezhetők.

Az ezen események bármelyikének a gyakoriságában és/vagy időzítésében bekövetkező változások kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt kérésteljesítési folyamatban meghatározott üzemeltetési eljárásokat.

3.1.4. Ügyleti üzenetek folyamata

Kimenő ügyletek

Ez az átvezetést indító ETS nézőpontját tükrözi. A konkrét folyamatot az alábbi folyamatábra jeleníti meg:



A fő folyamat a következő lépésekből áll (lásd a fenti rajzon):

(a) Az átvezetést indító ETS-ben az ügyleti kérelmet elküldik a kibocsátásiegység-forgalmi jegyzékből az ügyleti jegyzőkönyvbe, amint valamennyi üzleti késedelem megszűnik (adott esetben 24 órás késedelem).

(b) Az ügyleti jegyzőkönyv érvényesíti az ügyleti kérelmet.

(c) Az ügyleti kérelmet elküldik a rendeltetési ETS-nek.

(d) Az elfogadó választ elküldik a származási ETS kibocsátásiegység-forgalmi jegyzékének.

(e) A rendeltetési ETS érvényesíti az ügyleti kérelmet.

(f) A rendeltetési ETS visszaküldi az elfogadó választ a származási ETS ügyleti jegyzőkönyvéhez.

(g) az ügyleti jegyzőkönyv elküldi az elfogadó választ a kibocsátásiegység-forgalmi jegyzéknek.

Alternatív folyamat: „Ügyleti jegyzőkönyv általi elutasítás” (lásd a fenti rajzon, a fő folyamat a) pontjából kiindulva):

(a) A származási rendszerben az ügyleti kérelmet elküldik a kibocsátásiegység-forgalmi jegyzékből az ügyleti jegyzőkönyvbe, amint valamennyi üzleti késedelem megszűnik (adott esetben 24 órás késedelem).

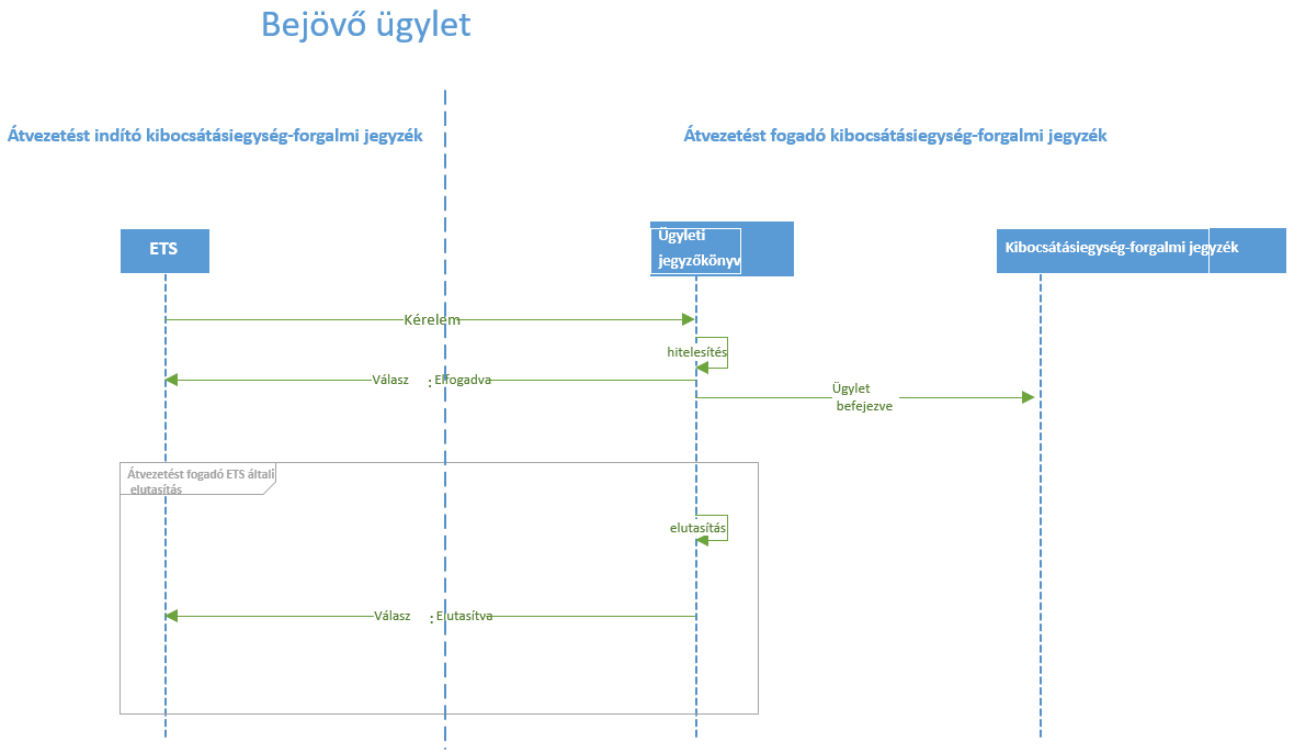
(b) Az ügyleti jegyzőkönyv nem érvényesíti a kérelmet.

(c) elutasító üzenetet küldenek a származási kibocsátásiegység-forgalmi jegyzékhez.

Alternatív folyamat: „ETS általi elutasítás” (lásd a fenti rajzon, a fő folyamat d) pontjából kiindulva):

(a) A származási ETS-ben az ügyleti kérelmet elküldik a kibocsátásiegység-forgalmi jegyzékből az ügyleti jegyzőkönyvbe, amint valamennyi üzleti késedelem megszűnik (adott esetben 24 órás késedelem).
(b) Az ügyleti jegyzőkönyv érvényesíti az ügyletet.
(c) Az ügyleti kérelmet elküldik a rendeltetési ETS-nek.
(d) Az elfogadó üzenetet elküldik a származási ETS kibocsátásiegység-forgalmi jegyzékének.
(e) Az átvezetést fogadó ETS ügyleti jegyzőkönyve nem érvényesíti az ügyletet.
(f) Az átvezetést fogadó ETS elküldi az elutasító választ az átvezetést indító ETS ügyleti jegyzőkönyvéhez.
(g) az ügyleti jegyzőkönyv elküldi az elutasítást a kibocsátásiegység-forgalmi jegyzéknek.

Bejövő ügyletek



Ez az átvezetést fogadó ETS nézőpontját tükrözi. A konkrét folyamatot az alábbi folyamatábra jeleníti meg:

Az ábra a következőket mutatja:

(1) Amikor az átvezetést fogadó ETS ügyleti jegyzőkönyve érvényesíti a kérelmet, elküldi az elfogadó üzenetet az átvezetést indító ETS-nek, valamint „ügylet lezárva” üzenetet küld az átvezetést fogadó ETS kibocsátásiegység-forgalmi jegyzékének.

(2) Amikor egy bejövő kérelem elutasításra kerül az átvezetést fogadó ügyleti jegyzőkönyvben, az ügyleti kérelmet nem küldik el az átvezetést fogadó ETS kibocsátásiegység-forgalmi jegyzékének.

Protokoll

Az ügyleti üzenet ciklus csak két üzenetet foglal magában:

- átvezetést indító ETS → Átvezetést fogadó ETS ügyleti javaslat.
- Átvezetést fogadó ETS → Átvezetést indító ETS ügyleti válasz: vagy Elfogadva vagy Elutasítva (az elutasítás indokával együtt).
  - Elfogadva: az ügyletet teljesítik.
  - Elutasítva: az ügyletet leállítják.

Az ügylet státusza

- Az átvezetést indító ETS ügyleti státusza „javasolt” lesz a kérelem elküldésekor.
- Az átvezetést fogadó ETS ügyleti státusza „javasolt” lesz a kérelem beérkezésekor és annak kezelése során.
- Az átvezetést fogadó ETS ügyleti státusza „teljesített”/„leállított” lesz, amikor a javaslat feldolgozásra kerül. Ezt követően az átvezetést fogadó ETS elküldi a megfelelő elfogadó/elutasító üzenetet.
- Az átvezetést indító ETS ügyleti státusza teljesített / leállított lesz, amikor az elfogadás / elutasítás beérkezik és feldolgozásra kerül.
- Az átvezetést indító ETS-ben az ügyleti státusz javasolt marad, amennyiben nem érkezik válasz.
- Az átvezetést fogadó ETS „leállított” státuszba helyez minden olyan ügyletet, amely több, mint 30 percen át javasolt marad.

Az ügyletekkel kapcsolatos események kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt eseménykezelési folyamatban meghatározott üzemeltetési eljárásokat.

3.2. Adatátvitel biztonsága

Az adatok továbbításuk során négy biztonsági szinten mennek át:

(1) Hálózati hozzáférés-vezérlés: tűzfal és hálózati összekapcsolási réteg.

(2) Titkosítás az átvitel szintjén: VPN.

(3) Titkosítás a munkamenet szintjén: biztonságos üzenettovábbítási protokoll.

(4) Titkosítás az alkalmazás szintjén: XML tartalom titkosítás és aláírás.

3.2.1. Tűzfal és hálózati összekapcsolás

A kapcsolat hardver alapú tűzfallal védett hálózaton keresztül jön létre. A tűzfal konfigurálása olyan szabályok alapján történik, hogy csak „regisztrált” kliensek kapcsolódhatnak a VPN szerverhez.

3.2.2. Virtuális magánhálózat (VPN)

A Felek közötti kommunikáció minden esetben virtuális magánhálózat (VPN) technológiával védett. A VPN technológiák lehetőséget nyújtanak a hálózaton – pl. az interneten – történő áthaladásra „alagúton” keresztül egyik ponttól a másikig, a kommunikációk mindenkori védelme mellett. A VPN

alagút létrehozását megelőzően elektronikus tanúsítvány kiállítására kerül sor egy leendő kliens végpont részére, amely lehetővé teszi a kliens számára, hogy igazolja a személyazonosságát az összekapcsolás igénylése során. Mindegyik Fél felel azért, hogy saját VPN végpontján telepítse a tanúsítványt. Az elektronikus tanúsítványok használatával mindkét oldal VPN szervere hozzáférést kap egy központi hatósághoz a hitelesítő adatok egyeztetése érdekében. Az alagút-létrehozási folyamat során titkosítás kerül meghatározásra, biztosítva az alagúton keresztül zajló kommunikációk védelmét.

A kliens VPN végpontokat úgy kell konfigurálni, hogy biztosítva legyen a VPN alagút folyamatos fenntartása a Felek közötti megbízható, kétirányú, valós idejű kommunikáció mindenkori lehetővé tétele érdekében.

Az Európai Unió általában a közigazgatási rendszerek közötti biztonságos transzeurópai telematikai szolgáltatások (STESTA) hálózatát használja IP-alapú magánhálózatként. Ezért ez a hálózat megfelelő a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat esetében is.

3.2.3. IPSec megvalósítása

Az IPSec protokollnak a helyek közötti VPN-infrastruktúra létrehozásához történő használata biztosítja a helyek közötti hitelesítést, az adatok sértetlenségét, valamint az adatok titkosítását. Az IPSec VPN konfigurációk biztosítják a VPN kapcsolat két végpontja közötti megfelelő hitelesítést. A Felek azonosítják és hitelesítik a távoli klienst az IPSec kapcsolaton keresztül, a másik oldal által elismert tanúsító hatóság által kiadott elektronikus tanúsítványok használatával.

Az IPSec továbbá biztosítja az adatok sértetlenségét a VPN alagúton keresztül zajló kommunikációk során. Az adatcsomagokat a VPN által létrehozott hitelesítési információk felhasználásával kivonatolják (hashed) és aláírják. Az adatok bizalmas jellegét hasonlóképpen, IPSec titkosítás lehetővé tételével biztosítják.

3.2.4. Biztonságos üzenettovábbítási protokoll.

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat több titkosítási rétegre támaszkodik a Felek közötti biztonságos adatcsere érdekében. Mindkét rendszer és azok különböző környezetei a hálózat szintjén vannak összekapcsolva VPN alagutakon keresztül. Az alkalmazás szintjén a fájlok átvitelére biztonságos üzenettovábbítási protokoll alkalmazásával kerül sor munkamenet szinten.

3.2.5. XML titkosítás és aláírás

Az XML fájlokon belül az aláírás és a titkosítás két szinten történik. Minden ügyleti kérelem, ügyleti válasz és egyeztető üzenet egyenként kerül aláírásra, elektronikus úton.

A második lépésben az „üzenet” elem minden aleleme egyenként titkosításra kerül.

Ezen túlmenően, a harmadik lépésben sor kerül a gyökérelem elektronikus úton történő aláírására, a teljes üzenet sértetlenségének és letagadhatatlanságának biztosítása érdekében. Ez az XML-be beágyazott adatok magas szintű védelmét eredményezi. A műszaki végrehajtásra a World Wide Web Konzorcium előírásaival összhangban kerül sor.

Az üzenet visszafejtéséhez ezt a folyamatot kell követni, fordított sorrendben.

3.2.6. Rejtjelezési kulcsok

A titkosítás és az aláírás nyilvános kulcsú kriptográfia alkalmazásával történik.

Az IPSec konkrét esetében mindkét Fél által megbízhatónak tartott tanúsító hatóság által kiállított elektronikus tanúsítványokat kell használni. Ez a tanúsító hatóság ellenőrzi a személyazonosságot és olyan tanúsítványokat ad ki, amelyekkel a szervezetek egyértelműen azonosíthatók, és amelyek felhasználhatók a Felek közötti biztonságos adatkommunikációs csatornák létrehozásához.

A kommunikációs csatornák és az adatfájlok aláírására és rejtjelezésére rejtjelezési kulcsok alkalmazásával kerül sor. A nyilvános tanúsítványokat a Felek elektronikus úton cserélik ki egymással, biztonságos csatornákat használva, és azokat független csatornákon keresztül hitelesítik. Ez az eljárás a közös üzemeltetési eljárásokban foglalt információbiztonsági irányítási folyamat szerves részét képezi.

3.3. A kapcsolat keretében végzett funkciók listája

A kapcsolat meghatározza az átviteli rendszert a megállapodásból eredő üzleti folyamatokat végrehajtó funkciók vonatkozásában. A kapcsolat magában foglalja továbbá az egyeztetési folyamat és a próbaüzenetek vonatkozásában történő meghatározást, ami lehetővé teszi a szívdobbanás felügyelet megvalósítását.

3.3.1. Üzleti ügyletek

Üzleti szempontból a kapcsolat négy (4) típusú ügyleti kérelmet vesz figyelembe:

- Külső átvezetés:
  - Az ETS-ek összekapcsolásának hatálybalépését követően az uniós és a svájci kibocsátási egységek helyettesíthetők, ezáltal pedig teljes mértékben átruházhatók a Felek között.
  - A kapcsolaton keresztül végzett átvezetés egy átvezetést indító számlát érint az egyik ETS-ben és egy átvezetést fogadó számlát a másik ETS-ben.
  - az átvezetés a négy (4) típusú kibocsátási egység bármekkora mennyiségét magában foglalhatja:
    - Svájci általános célú kibocsátási egységek (CHU)
    - Svájci légi közlekedési kibocsátási egységek (CHUA)
    - EU általános célú kibocsátási egységek (EUA)
    - EU légi közlekedési kibocsátási egységek (EUAA)
- Nemzetközi kiosztás:

Azok a légijármű-üzembentartók, amelyek az egyik ETS igazgatása alá tartoznak, amely kötelezettségekkel bír a másik ETS felé, és amelyek jogosultak arra, hogy ettől a második ETS-től kibocsátási egységeket vegyenek át térítésmentesen, ingyenes légi közlekedési kibocsátási egységeket kapnak a második ETS-től a nemzetközi kiosztási ügylet útján.

- A nemzetközi kiosztás visszavonása:

Erre az ügyletre akkor kerül sor, ha a légijármű-üzembentartó számlájára a másik ETS által kiosztott ingyenes kibocsátási egységeket teljes mértékben vissza kell vonni.

- Indokolatlanul kiosztott kibocsátásiegység-mennyiség visszaadása:

Hasonló a visszavonáshoz, de ebben az esetben a kiosztást nem kell teljes mértékben visszavonni, csak a túlzott mennyiségben kiosztott kibocsátási egységeket kell visszaadni a kiosztó ETS-nek.

3.3.2. Egyeztetési protokoll

Az egyeztetésekre csak az üzenetek befogadására, hitelesítésére és feldolgozására rendelkezésére álló időkereten belül kerülhet sor.

Az egyeztetések az összekapcsolás biztonságára és a következetességére irányuló intézkedések szerves részét képezik. Bármely ütemterv elkészítése előtt a Felek megállapodnak az egyeztetés pontos időzítése tekintetében. Napi szinten ütemezett egyeztetésre is sor kerülhet, amennyiben ezt mindkét Fél elfogadja. Legalább egy ütemezett egyeztetést kell végrehajtani azonban a befogadást követően.

Ugyanakkor bármelyik Fél bármikor kezdeményezhet manuális egyeztetéseket.

Az ütemezett egyeztetés időzítésében és gyakoriságában bekövetkező változások kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt kérésteljesítési folyamatban meghatározott üzemeltetési eljárásokat.

3.3.3. Próbaüzenet

A próbaüzenet a végpontok közötti kommunikáció tesztelésére szolgál. Az üzenet olyan adatokat tartalmaz, amelyek azt próbaüzenetként azonosítják, és az üzenet átvételét követően a másik végpont választ küld.

3.4. Adatnaplózási követelmények

Tekintettel arra, hogy mindkét Félnek szüksége van arra, hogy folyamatosan pontos és következetes információk álljanak rendelkezésükre, valamint az egyeztetési folyamat során a következetlenségek kiküszöböléséhez használható eszköz biztosítása érdekében a Feleknek négy (4) típusú adatrögzítést kell fenntartaniuk:

- Ügyleti jegyzőkönyvek,
- Egyeztetési jegyzőkönyvek,
- Üzenet archívum,
- Belső ellenőrzési jegyzőkönyvek.

Az ezekben a jegyzőkönyvekben rögzített adatokat legalább három (3) hónapig meg kell őrizni hibaelhárítási célokból, az adatok további megőrzése pedig az alkalmazandó jogtól függ mindkét végponton, ellenőrzés céljából. A három (3) hónapnál régebbi jegyzőkönyv fájlok egy független információtechnológiai rendszerben, biztonságos helyen archiválhatók úgy, hogy azok észszerű időn belül visszakereshetők és hozzáférhetők legyenek.

Ügyleti jegyzőkönyvek

Mind az EUTL, mind az SSTL alrendszer ügyleti jegyzőkönyv megvalósítások. A két ETS-rendszert egyeztetik.

Pontosabban az ügyleti jegyzőkönyvek nyilvántartásként szolgálnak a másik ETS-nek küldött minden egyes javasolt ügyletről. Minden bejegyzés tartalmazza az ügyleti tartalom összes területét, valamint az ügylet későbbi kimenetelét (a fogadó ETS válasza). Az ügyleti jegyzőkönyvek nyilvántartást vezetnek továbbá a bejövő ügyletekről, valamint a származási ETS-nek küldött válaszról.

Egyeztetési jegyzőkönyvek

Az egyeztetési jegyzőkönyvben rögzítésre kerülnek a Felek egyeztetéssel kapcsolatos üzenetváltásai, beleértve az egyeztetési azonosítót, az időbélyegzőt és az egyeztetés eredményét is: Egyeztetési státusz: „Megfelel” vagy „Eltérések”. A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolatban szereplő egyeztetési üzenetek az üzenetváltások szerves részét képezik, ezért azokat az „Üzenet archiválása” részben leírtak szerint tárolják.

Mindkét Fél köteles az egyeztetési jegyzőkönyvben rögzíteni minden kérelmet és az arra adott választ. Habár nem kerül sor az egyeztetési jegyzőkönyvben szereplő adatok közvetlen megosztására magának az egyeztetésnek a részeként, a következetlenségek kiküszöbölése érdekében szükség lehet az ilyen adatokhoz való hozzáférésre.

Üzenet archiválása

Mindkét Fél köteles archiválni a kicserélt – elküldött és beérkezett – adatok (az XML fájlok) egy példányát, valamint rögzíteni azt, hogy azok vagy az XML üzenetek megfelelő formátumúak voltak-e vagy sem.

Az archiválás elsősorban ellenőrzés céljából történik, hogy bizonyítékok álljanak rendelkezésre arra vonatkozóan, hogy mit küldtek el a másik Félnek, illetve mi érkezett a másik Féltől. Ebben az értelemben a fájlokkal együtt a kapcsolódó tanúsítványokat is archiválni kell.

Ezek a fájlok is további információkkal szolgálhatnak a hibaelhárításhoz.

Belső ellenőrzési jegyzőkönyv

Ezek a jegyzőkönyveket mindkét Fél önállóan határozza meg és használja.

3.5. Üzemeltetési követelmények

A két rendszer közötti adatcsere nem teljesen autonóm jellegű a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat során, tehát szükség van üzemeltetőkre és eljárásokra a kapcsolat működőképessé tételéhez. E folyamat során számos feladatkör és eszköz kap részletes leírást.

4. ELÉRHETŐSÉGRE VONATKOZÓ RENDELKEZÉSEK

4.1. A kommunikáció elérhetőségének tervezése

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat architektúráját alapvetően olyan IKT-infrastruktúra és szoftver képezi, amely lehetővé teszi a svájci ETS és az EU ETS közötti kommunikációt. Az ilyen adatáramlás magas szintű elérhetőségének, sértetlenségének és titkosságának a biztosítása olyan lényeges szempont, amit figyelembe kell venni a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat tervezése során. Tekintettel arra, hogy ez egy olyan projekt, amelyben az IKT-infrastruktúra, az egyedi szoftver és a folyamatok alapvető szerepet játszanak, mindhárom elemet figyelembe kell venni egy ellenállóképes rendszer kialakítása érdekében.

IKT-infrastruktúra ellenálló képessége

E dokumentum általános rendelkezéseket taglaló része tartalmazza az architektúra építőelemeinek leírását. Az IKT-infrastruktúra tekintetében a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolattal létrejön egy ellenálló VPN hálózat, amely biztonságos kommunikációs csatornákat hoz létre, amelyeken keresztül biztonságos üzenetváltásokra kerülhet sor. Az infrastruktúra többi eleme úgy van konfigurálva, hogy biztosítva legyen a magas szintű elérhetőség és/vagy tartalékmechanizmusok rendelkezésre állása.

Egyedi szoftver ellenálló képessége

Az egyedileg kifejlesztett szoftvermodulok növelik az ellenálló képességet azzal, hogy adott ideig újra megkísérlik a kommunikációt a másik Féllel, ha bármilyen oknál fogva az nem elérhető.

Szolgáltatás ellenálló képessége

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolatban a Felek közötti adatcserékre előre meghatározott időközönként kerül sor. Az előre ütemezett adatcserék során előírt bizonyos lépéseknél szükség van a rendszerüzemeltetők és/vagy a jegyzékkezelők általi manuális beavatkozásra. Tekintettel erre, valamint a cserék elérhetőségének és eredményességének fokozása érdekében:

- Az üzemeltetési eljárások időablakokat biztosítanak az egyes lépések végrehajtásához.
- A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolathoz tartozó szoftvermodulok aszinkron kommunikációt valósítanak meg.
- Az automatikus egyeztetési folyamat kimutatja, hogy voltak-e problémák a másik oldalon az adatfájlok beolvasása során.
- Az ellenőrzési folyamatokat (IKT-infrastruktúra és egyedi szoftvermodulok) figyelembe veszik az eseménykezelési eljárásokban, és azok elindítják ezeket az eljárásokat (a közös üzemeltetési eljárásokat tartalmazó dokumentumban meghatározottak szerint). Azok az eljárások, amelyek az eseményeket követően az üzemszerű működés helyreállításához szükséges idő lerövidítésére irányulnak, alapvető fontosságúak a magas elérhetőségi arányok biztosításához.

4.2. Kezdeményezés, kommunikáció, újbóli aktiválás és vizsgálati terv

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat architektúrájában foglalt összes különböző elemet egy sor egyéni és csoportos vizsgálatnak kell alávetni annak megerősítése érdekében, hogy a platform készen áll az IKT-infrastruktúra és az információs rendszer szintjén. Ezek a működési vizsgálatok kötelező előfeltételnek tekintendők minden alkalommal, amikor a

platform a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat állapotát átállítja felfüggesztettről működőképesre.

A kapcsolat működőképes állapotának aktiválásához ezt követően szükség van az előzetesen meghatározott vizsgálati terv sikeres kivitelezésére. Ez megerősíti, hogy mindegyik kibocsátásiegység-forgalmi jegyzék elvégzett először egy sor belső vizsgálatot, majd elvégezte a végpontok közötti hálózati összekapcsoltság érvényesítését, a Felek közötti gyártási ügyletek benyújtásának megkezdése előtt.

A vizsgálati tervnek tartalmaznia kell az átfogó vizsgálati stratégiát és a vizsgálati infrastruktúrára vonatkozó részleteket. Minden vizsgálati blokk minden egyes eleme tekintetében a tervnek különösen a következőket kell tartalmaznia:

- Vizsgálati kritériumok és eszközök,
- A vizsgálatok elvégzése érdekében kiosztott szerepek,
- Várt eredmények (pozitív és negatív),
- Vizsgálati ütemterv,
- A vizsgálati eredményekre vonatkozó követelmények rögzítése,
- Hibaelhárítási dokumentumok,
- Felterjesztésre vonatkozó rendelkezések.

A működőképes állapot aktiválására irányuló vizsgálatok folyamata négy (4) elvi blokkra vagy szakaszra osztható:

4.2.1. Belső IKT-infrastruktúra vizsgálatok

Ezeket a vizsgálatokat a jegyzékkezelők mindkét oldalon egyedileg végzik el és/vagy ellenőrzik.

Az IKT-infrastruktúra minden elemét mindkét oldalon egyedileg kell tesztelni. Ez kiterjed az infrastruktúra minden egyes alkotóelemére. Ezek a vizsgálatok elvégezhetők automatikusan vagy manuálisan, de igazolniuk kell, hogy az infrastruktúra minden eleme működőképes.

4.2.2. Kommunikációs vizsgálatok

Ezek a vizsgálatok egyedileg kezdődnek mindkét Félnél, és a másik oldallal együttműködve fejeződnek be.

Amint az egyes elemek működőképessé válnak, ellenőrizni kell a két kibocsátásiegység-forgalmi jegyzék közötti kommunikációs csatornákat. Ennek során mindkét Fél ellenőrzi, hogy van-e működőképes internet-hozzáférés, létrehozták-e a VPN-alagutakat, és van-e helyek közötti IP-kapcsolat. Ezt követően a másik Fél felé meg kell erősíteni a helyi és távoli infrastruktúra elemek és az IP-kapcsolat elérhetőségét.

4.2.3. Az egész rendszerre kiterjedő (végpontok közötti) vizsgálatok

Ezeket a vizsgálatokat mindkét oldalon el kell végezni, és az eredményeket közölni kell a másik Féllel.

A kommunikációs csatornák, valamint a két kibocsátásiegység-forgalmi jegyzék minden egyes alkotóelemének vizsgálatát követően mindkét oldal szimulált ügyleteket és egyeztetést dolgoz ki, amelyek bemutatják a kapcsolat keretében végrehajtandó összes funkciót.

4.2.4. Biztonsági tesztek

Ezeket a vizsgálatokat a jegyzékkezelők elvégzik és/vagy kezdeményezik mindkét oldalon, a „Biztonsági vizsgálatokra vonatkozó útmutató” és a „Kockázatértékelésre vonatkozó rendelkezések” című szakaszban leírtak szerint.

A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat csak azt követően tekinthető működőképes állapotúnak, hogy mind a négy szakasz / blokk lezárult kiszámítható eredményekkel.

Vizsgálati erőforrások

Mindkét Fél meghatározott vizsgálati erőforrásokra (meghatározott IKT-infrastruktúrára, szoftverre és hardverre) támaszkodik, továbbá a platform manuális és folyamatos hitelesítésének támogatása érdekében vizsgálati funkciókat fejleszt ki saját rendszeréhez. Az egyénileg vagy együttműködés keretében végzett manuális vizsgálati eljárások bármikor, bármelyik jegyzékkezelő által végrehajthatók. A működőképes állapot aktiválása önmagában véve manuális folyamat.

A tervek szerint a platform rendszeres időközönként automatikus ellenőrzéseket is végez. Ezen ellenőrzések célja a platform elérhetőségének javítása az infrastruktúrával vagy a szoftverrel kapcsolatos problémák korai felismerése révén. Ez a platform ellenőrzési terv két elemből áll:

- IKT-infrastruktúra ellenőrzése: Az infrastruktúrát mindkét oldalon ellenőrzik az IKT-infrastruktúra szolgáltatók. Az automatikus vizsgálatok kiterjednek a különböző infrastruktúra elemekre és a kommunikációs csatornák elérhetőségére.
- Alkalmazás ellenőrzése: A kibocsátásiegység-forgalmi jegyzékek közötti állandó összekapcsolási szoftvermodulok az alkalmazás szintjén megvalósítják a rendszerkommunikáció ellenőrzését (manuálisan és/vagy rendszeres időközönként), melynek során megvizsgálják az összekapcsolás végpontok közötti elérhetőségét a kapcsolaton keresztül végzett bizonyos ügyletek szimulálása révén.

4.3. Elfogadási/Tesztelési környezetek

Az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék architektúrája az alábbi három környezetet foglalja magában:

- Gyártási (Production – PROD): ez a környezet tartalmazza a valós adatokat és folyamatokat, valamint a valós ügyleteket.
- Elfogadási (Acceptance – ACC): ez a környezet nem valós vagy anonimizált, reprezentatív adatokat tartalmaz. Ez az a környezet, ahol mindkét Fél rendszerüzemeltetői érvényesítik az új kiadásokat.
- Tesztelési (Test – TEST): ez a környezet nem valós vagy anonimizált, reprezentatív adatokat tartalmaz. Ez a környezet a jegyzékkezelőkre korlátozódik, és az integrációs tesztek Felek általi elvégzésére szolgál.

A VPN kivételével a három környezet teljes mértékben független egymástól, ami azt jelenti, hogy a hardver, a szoftver, az adatbázisok, a virtuális környezetek, az IP-címek, a portok egymástól függetlenül kerülnek kialakításra, és azok egymástól függetlenül működnek.

Ami a VPN elrendezését illeti, a három környezet közötti kommunikációnak teljesen függetlennek kell lennie; ez a STESTA használatával biztosítandó.

5. TITOKTARTÁSRA ÉS SÉRTETLENSÉGRE VONATKOZÓ RENDELKEZÉSEK

A biztonsági mechanizmusok és eljárások kétszemélyes szerepkört (négy szem elve) írnak elő az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kapcsolat során végzett műveletek vonatkozásában. Szükség esetén mindig kétszemélyes szerepkör alkalmazandó, de előfordulhat, hogy az nem alkalmazható a jegyzékkezelők által végzett valamennyi lépés esetén.

A biztonsági előírásokat figyelembe kell venni és követni kell a biztonságirányítási tervben, ami a biztonság esetleges megsértését követően a biztonsági események kezeléséhez kapcsolódó folyamatokat is magában foglalja. E folyamatok operatív részének a leírását a közös üzemeltetési eljárások tartalmazzák.

5.1. Biztonsági tesztelési infrastruktúra

A Felek vállalják, hogy biztonsági tesztelési infrastruktúrát hoznak létre (a fejlesztés és az üzemeltetés szakaszában a sebezhetőségek felismeréséhez használt közös szoftverek és hardverek alkalmazásával):

- a gyártási környezettől elkülönítve,
- ahol a biztonság elemzését a rendszer fejlesztésétől és üzemeltetésétől független csoport végzi.

A Felek vállalják statikus és dinamikus elemzések végzését egyaránt.

Dinamikus elemzés (pl. behatolási tesztelés) esetén a Felek vállalják, hogy az értékeléseket általában a tesztelési és az elfogadási környezetekre korlátozzák (az „Elfogadási / Tesztelési környezetek” című részben foglaltak szerint). E szabálytól való eltérés esetén szükség van a Felek jóváhagyására.

A gyártási környezetben való telepítést megelőzően a kapcsolat minden szoftvermodulját („A kommunikációs kapcsolat architektúrája” című részben foglaltak szerint) tesztelni kell.

A tesztelési infrastruktúrát a hálózat és az infrastruktúra szintjén egyaránt el kell különíteni a gyártási szinttől, és annak lehetővé kell tennie a biztonsági előírásoknak való megfelelés ellenőrzéséhez szükséges biztonsági vizsgálatok elvégzését.

5.2. A kapcsolat felfüggesztésére és újbóli aktiválására vonatkozó rendelkezések

Amennyiben felmerül annak a gyanúja, hogy a svájci kibocsátásiegység-forgalmi jegyzék, az SSTL, az uniós kibocsátásiegység-forgalmi jegyzék vagy az EUTL biztonsága veszélybe került, a Felek haladéktalanul tájékoztatják egymást, és felfüggesztik az SSTL és az EUTL közötti kapcsolatot.

Az információk megosztására, valamint a felfüggesztésről és az újbóli aktiválásról szóló határozat meghozatalára vonatkozó eljárások a közös üzemeltetési eljárásokban foglalt kérésteljesítési folyamat részét képezik.

Felfüggesztések

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolatnak a megállapodás II. melléklete szerinti felfüggesztésére az alábbiak miatt kerülhet sor:

- adminisztratív okok (például karbantartás), ami tervezett,
- biztonsági okok (vagy az informatikai infrastruktúra meghibásodásai), ami nem tervezett.

Veszélyhelyzetben az egyik Fél tájékoztatja a másik Felet és egyoldalúan felfüggeszti a kibocsátásiegység-forgalmi jegyzékek közötti kapcsolatot.

Amennyiben határozat születik a kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat felfüggesztéséről, a Felek ennek megfelelően biztosítják a kapcsolat hálózati szinten történő megszakítását (a bejövő és kimenő kapcsolatok részben vagy teljes egészében történő blokkolásával).

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat felfüggesztéséről szóló határozat – akár tervezett vagy nem tervezett – meghozatalára a közös üzemeltetési eljárásokban foglalt változáskezelési eljárás vagy biztonsági események kezelésére vonatkozó eljárás szerint kerül sor.

A kommunikáció újbóli aktiválása

Az újbóli aktiválásra vonatkozó határozat meghozatalára a közös üzemeltetési eljárásokban foglaltak szerint kerül sor, és semmi esetre sem a „Biztonsági tesztelésre vonatkozó útmutató”, illetve a „Kezdeményezés, kommunikáció, újbóli aktiválás és vizsgálati terv” című részben leírt biztonsági tesztelési eljárások sikeres befejezése előtt.

5.3. A biztonság megsértésére vonatkozó rendelkezések

A biztonság megsértése az érzékeny információk bizalmasságát és sértetlenségét és/vagy az ilyen információkat kezelő rendszer elérhetőségét érintő biztonsági eseménynek minősül.

Az érzékeny információk az Érzékeny információk jegyzékében kerülnek meghatározásra, és azok a rendszerben vagy bármely ahhoz kapcsolódó egységben kezelhetők.

A biztonság megsértéséhez közvetlenül kapcsolódó információk érzékenynek tekintendők, „KÜLÖNLEGES KEZELÉST IGÉNYLŐ: *ETS Critical*” (ETS kritikus jelentőségű információ) megjelölést kapnak, és eltérő rendelkezések hiányában azokat a kezelési utasításokkal összhangban kell kezelni.

A biztonság megsértését minden esetben a közös üzemeltetési eljárások „Biztonsági események kezelése” című fejezetében foglaltak szerint kell kezelni.

5.4. Biztonsági tesztelésre vonatkozó útmutató

5.4.1. Szoftver

A biztonság tesztelését, adott esetben ideértve a behatolási tesztelést, legalább a szoftver összes főbb kiadásain el kell végezni az LTS-ekben foglalt biztonsági előírások szerint, az összekapcsolás és a kapcsolódó kockázatok biztonsági szintjének megállapítása érdekében.

Amennyiben az elmúlt 12 hónapban nem jött létre jelentős kiadás, a biztonsági tesztelést a meglévő rendszeren kell elvégezni, figyelembe véve a számítógépes fenyegetés alakulását az elmúlt 12 hónapban.

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat biztonsági tesztelését az elfogadási környezetben kell elvégezni, valamint – szükség esetén – a gyártási környezetben, a Felek közötti koordináció és kölcsönös megállapodás keretében.

A webes alkalmazások tesztelése során be kell tartani a nemzetközi nyílt szabványokat, köztük az Open Web Application Security Project (OWASP) keretében kidolgozott előírásokat.

5.4.2. Infrastruktúra

A gyártási rendszert támogató infrastruktúrát rendszeresen át kell vizsgálni a sebezhetőségek felismerése érdekében (legalább havonta egyszer), és az észlelt sebezhetőségeket az előző szakaszban ismertetett elv alapján ki kell javítani naprakész sebezhetőségi adatbázis felhasználásával.

5.5. Kockázatértékelésre vonatkozó rendelkezések

Amennyiben szükség van behatolási tesztelésre, azt a biztonsági tesztelés keretében kell elvégezni.

A biztonsági tesztelés elvégzésére a Felek szerződést köthetnek egy erre szakosodott vállalattal, feltéve, hogy az adott vállalat:

- rendelkezik az ilyen biztonsági teszteléshez szükséges készségekkel és tapasztalattal,
- nem közvetlenül a fejlesztőnek és/vagy a fejlesztő alvállalkozójának jelentő vállalat, továbbá nem vesz részt a kapcsolat szoftverének fejlesztésében, és nem a fejlesztő alvállalkozója,
- titoktartási megállapodást írt alá, amelyben vállalta, hogy az eredményeket bizalmasan, a kezelési utasításoknak megfelelően „KÜLÖNLEGES KEZELÉST IGÉNYLŐ: ETS kritikus” jelentőségű információként kezeli.