EUROPSKA
KOMISIJA

Bruxelles, 20.3.2024.
COM(2024) 125 final

ANNEX

PRILOG

Prijedlogu odluke Vijeća

o stajalištu koje treba zauzeti u ime Europske unije u Zajedničkom odboru osnovanom na temelju Sporazuma između Europske unije i Švicarske Konfederacije o povezivanju njihovih sustava trgovanja emisijama stakleničkih plinova u pogledu izmjene Priloga II. Sporazumu, zajedničkih operativnih postupaka i tehničkih standarda za povezivanje

ODLUKA br. 1/2024 ZAJEDNIČKOG ODBORA OSNOVANOG NA TEMELJU SPORAZUMA IZMEĐU EUROPSKE UNIJE I ŠVICARSKE KONFEDERACIJE O POVEZIVANJU NJIHOVIH SUSTAVA TRGOVANJA EMISIJAMA STAKLENIČKIH PLINOVA

od …

u pogledu izmjene Priloga II. Sporazumu, zajedničkih operativnih postupaka i tehničkih standarda za povezivanje

ZAJEDNIČKI ODBOR,

uzimajući u obzir Sporazum između Europske unije i Švicarske Konfederacije o povezivanju njihovih sustava trgovanja emisijama stakleničkih plinova[1] (dalje u tekstu „Sporazum”), a posebno njegov članak 9. i članak 13. stavak 2.,

budući da:

(1) Odlukom Zajedničkog odbora br. 2/2019[2] predviđeno je privremeno rješenje kojim bi se uspostavila veza između ETS-a EU-a i ETS-a Švicarske.

(2) Na svojem trećem sastanku Zajednički odbor postigao je dogovor o tome da je potrebno analizirati troškovnu učinkovitost trajne veze između registra Unije i registra Švicarske.

(3) Na svojem petom sastanku Zajednički odbor postigao je dogovor o izvješću koje je podnijela radna skupina osnovana odlukama Zajedničkog odbora 1/2020[3] i 2/2020[4] i u kojem je ta radna skupina analizirala i preporučila pristup za uspostavljanje trajne veze između registra Unije i registra Švicarske.

(4) Kako bi se uzeli u obzir tehnički zahtjevi za trajnu vezu između registra Unije i registra Švicarske te kako bi se odredbe Priloga II. Sporazumu pojednostavnile s obzirom na tehnološki razvoj, Prilog II. Sporazumu trebalo bi izmijeniti.

(5) Kako bi se osigurala dosljednost zajedničkih operativnih postupaka i tehničkih standarda za povezivanje s Prilogom II. Sporazumu, te bi dokumente isto tako trebalo izmijeniti,

DONIO JE OVU ODLUKU:

Članak 1.

1. Prilog II. Sporazumu zamjenjuje se tekstom u Prilogu I ovoj Odluci.

2. Zajednički operativni postupci iz članka 3. stavka 6. Sporazuma utvrđeni su u Prilogu II. ovoj Odluci.

3. Tehnički standardi za povezivanje iz članka 3. stavka 7. Sporazuma utvrđeni su u Prilogu III. ovoj Odluci.

Članak 2.

Ova Odluka stupa na snagu na dan donošenja.

---

[1] SL L 322, 7.12.2017., str. 3.
[2] SL L 314, 29.9.2020., str. 68.
[3] SL L 226, 25.6.2021., str. 2.
[4] SL L 226, 25.6.2021., str. 16.

Sastavljeno na engleskom u [Bruxellesu] [Bernu] [xx 2024.]

Za Zajednički odbor

Tajnica za Europsku uniju	*Predsjednica*	*Tajnica za Švicarsku*

PRILOG I.

„PRILOG II.

TEHNIČKI STANDARDI ZA POVEZIVANJE

Privremeno rješenje koje je omogućilo operativnost veze između ETS-a EU-a i ETS-a Švicarske uvedeno je 2020. Od 2023. veza između registara tih dvaju sustava trgovanja emisijama postupno će se razvijati u trajnu vezu između registara. Očekuje se da će se uspostaviti najkasnije 2024., čime se omogućuje funkcioniranje povezanih tržišta s obzirom na koristi od likvidnosti tržišta i izvršenja transakcija između dvaju povezanih sustava na način koji je istovjetan jednom tržištu koje čine dva sustava i koji sudionicima na tržištu omogućuje da djeluju kao da su na jednom tržištu, podložno samo pojedinačnim regulatornim odredbama stranaka. U tehničkim standardima za povezivanje utvrđuju se:

– struktura komunikacijske veze,

– komunikacija između SSTL-a i EUTL-a,

– sigurnost prijenosa podataka,

– popis funkcija (transakcije, usklađivanje…),

– definicija sloja prijenosa,

– zahtjevi u pogledu bilježenja podataka,

– operativna rješenja (korisnička podrška, tehnička podrška),

– plan aktiviranja komunikacije i postupak testiranja,

– postupak testiranja sigurnosti.

U tehničkim standardima za povezivanje utvrđuje se da administratori moraju poduzeti sve razumne mjere kako bi osigurali da SSTL, EUTL i veza budu operativni 24 sata dnevno i sedam dana u tjednu te da prekidi u radu SSTL-a, EUTL-a i veze budu što kraći.

U tehničkim standardima za povezivanje utvrđuju se dodatni sigurnosni zahtjevi za švicarski registar, SSTL, registar Unije i EUTL, koji se dokumentiraju u „planu upravljanja sigurnošću”. U tehničkim standardima za povezivanje posebno se utvrđuje sljedeće:

– ako se posumnja da je sigurnost švicarskog registra, SSTL-a, registra Unije ili EUTL-a ugrožena, obje stranke odmah o tome obavješćuju jedna drugu te suspendiraju vezu između SSTL-a i EUTL-a,

– u slučaju povrede sigurnosti stranke se obvezuju da će jedna drugu odmah obavijestiti o tome. U mjeri u kojoj su raspoložive tehničke pojedinosti, administrator švicarskog registra i središnji administrator Unije u roku od 24 sata nakon što je sigurnosni incident utvrđen kao povreda sigurnosti razmjenjuju izvješće u kojemu je opisan predmetni incident (datum, uzrok, učinak, mjere za njegovo rješavanje).

Postupak testiranja sigurnosti utvrđen u tehničkim standardima za povezivanje provodi se prije uspostavljanja komunikacijske veze između SSTL-a i EUTL-a te kad god je potrebna nova verzija ili izdanje SSTL-a ili EUTL-a.

Tehnički standardi za povezivanje uz proizvodno okruženje predviđaju još dva ispitna okruženja: razvojno ispitno okruženje i prihvatno okruženje.

Preko administratora švicarskog registra i središnjeg administratora Unije stranke pružaju dokaze da je u zadnjih dvanaest mjeseci provedena neovisna sigurnosna procjena njihovih sustava u skladu sa sigurnosnim zahtjevima utvrđenima u tehničkim standardima za povezivanje. Testiranja sigurnosti, posebice testiranje na probijanje, provode se na svim većim novim izdanjima softvera u skladu sa sigurnosnim zahtjevima utvrđenima u tehničkim standardima za povezivanje. Testiranje na probijanje ne provodi poduzeće koje je razvilo predmetni softver ni njegov podizvođač.”

PRILOG II.

ZAJEDNIČKI OPERATIVNI POSTUPCI

u skladu s člankom 3. stavkom 6. Sporazuma između Europske unije i Švicarske Konfederacije o povezivanju njihovih sustava trgovanja emisijama stakleničkih plinova

Postupci za trajnu vezu između registara

Sadržaj

1. Pojmovnik 10
2. Uvod 11
2.1. Područje primjene 11
2.2. Adresati 12
3. Pristup i standardi 12
4. Upravljanje incidentima 13
4.1. Otkrivanje i bilježenje incidenata 13
4.2. Klasifikacija i početna potpora 13
4.3. Istraživanje i dijagnosticiranje 14
4.4. Rješavanje i oporavak 14
4.5. Zatvaranje incidenta 14
5. Upravljanje problemima 16
5.1. Identifikacija i bilježenje problema 16
5.2. Određivanje prioriteta problema 16
5.3. Istraživanje i dijagnosticiranje problema 16
5.4. Rješavanje problema 16
5.5. Zatvaranje problema 16
6. Ispunjavanje zahtjeva 17
6.1. Aktivacija zahtjeva 17
6.2. Evidentiranje i analiza zahtjeva 17
6.3. Odobrenje zahtjeva 17
6.4. Ispunjavanje zahtjeva 17
6.5. Upućivanje zahtjeva na višu razinu 17
6.6. Preispitivanje ispunjavanja zahtjeva 18
6.7. Zatvaranje zahtjeva 18
7. Upravljanje promjenama 19
7.1. Zahtjev za promjenu 19

7.2. Evaluacija i planiranje promjene 19
7.3. Odobrenje promjene 19
7.4. Provedba promjene 19
8. Upravljanje izdanjima....19
8.1. Planiranje izdanja....20
8.2. Izrada i testiranje paketa izdanja....20
8.3. Priprema uvođenja 20
8.4. Uklanjanje novog izdanja 21
8.5. Preispitivanje i zaključenje izdanja 21
9. Upravljanje incidentima u području sigurnosti....21
9.1. Kategorizacija incidenata u području sigurnosti informacija 22
9.2. Upravljanje incidentima u području sigurnosti informacija 22
9.3. Identifikacija incidenata u području sigurnosti....22
9.4. Analiza incidenata u području sigurnosti 22
9.5. Procjena težine, upućivanje na više razine i izvješćivanje o incidentima u području sigurnosti....22
9.6. Izvješćivanje o sigurnosnom odgovoru 22
9.7. Praćenje, izgradnja kapaciteta i stalno poboljšavanje....23
10. Upravljanje sigurnošću informacija....23
10.1. Identifikacija osjetljivih informacija....23
10.2. Stupnjevi osjetljivosti informacijske imovine 23
10.3. Određivanje vlasnika informacijske imovine 24
10.4. Registracija osjetljivih informacija....24
10.5. Postupanje s osjetljivim informacijama....24
10.6. Upravljanje pristupom 24
10.7. Upravljanje certifikatima/ključevima 25

1. POJMOVNIK

Tablica 1. Pokrate i definicije

Pokrata/termin	Definicija
Certifikacijsko tijelo	Subjekt koji izdaje digitalne certifikate

CH	Švicarska Konfederacija
ETS	Sustav trgovanja emisijama
EU	Europska unija
IMT	Tim za upravljanje incidentima (eng. *Incident Management Team*)
Informacijska imovina	Informacija koja je vrijedna poduzeću ili organizaciji
IT	Informacijska tehnologija
ITIL	Popis infrastrukture informacijskih tehnologija (eng. *Information Technology Infrastructure Library*)
ITSM	Upravljanje IT uslugama
LTS	Tehnički standardi za povezivanje (eng. *Linking Technical Standards*)
Registar	Sustav za obračunavanje emisijskih jedinica izdanih u okviru ETS-a, u kojem se prati vlasništvo nad emisijskim jedinicama koje se drže na elektroničkim računima
RFC	Zahtjev za promjenu (eng. *Request For Change*)
SIL	Popis osjetljivih informacija (eng. *Sensitive Information List*)
SR	Zahtjev za uslugu (eng. *Service Request*)
Wiki	Internetska stranica koja korisnicima omogućava razmjenu informacija i znanja dodavanjem ili prilagođavanjem sadržaja izravno putem internetskog preglednika

2. UVOD

Sporazumom između Europske unije i Švicarske Konfederacije o povezivanju njihovih sustava trgovanja emisijama stakleničkih plinova od 23. studenog 2017. („Sporazum”) omogućava se međusobno priznavanje emisijskih jedinica koje se mogu iskoristiti za ispunjenje obveze u okviru sustava trgovanja emisijskim jedinicama stakleničkih plinova Europske unije („ETS EU-a”) ili sustava trgovanja emisijskim jedinicama Švicarske („ETS Švicarske”). Kako bi veza između ETS-a EU-a i ETS-a Švicarske postala operativna, uspostavlja se izravna veza između dnevnika transakcija Europske unije (EUTL) u okviru registra Unije i Švicarskog dopunskog dnevnika transakcija (SSTL) u okviru švicarskog registra, čime će se omogućiti prijenos emisijskih jedinica izdanih u okviru tih ETS-ova iz jednog registra u drugi (članak 3. stavak 2. Sporazuma). Privremeno rješenje koje je omogućilo operativnost veze između ETS-a EU-a i ETS-a Švicarske uvedeno je 2020. Od 2023. veza između registara tih dvaju sustava trgovanja emisijama postupno će se razvijati u trajnu vezu između registara. Očekuje se da će se uspostaviti najkasnije 2024., čime se omogućuje funkcioniranje povezanih tržišta s obzirom na koristi od likvidnosti tržišta i izvršenja transakcija između dvaju povezanih sustava na način koji je istovjetan jednom tržištu koje čine dva sustava i koji sudionicima na tržištu omogućuje da djeluju kao da su na jednom tržištu, podložno samo pojedinačnim regulatornim odredbama stranaka. (Prilog II. Sporazumu).

U skladu s člankom 3. stavkom 6. Sporazuma administrator švicarskog registra i središnji administrator Unije utvrđuju zajedničke operativne postupke povezane s tehničkim i drugim pitanjima i potrebne za funkcioniranje veze, uzimajući pri tom u obzir prioritete domaćeg zakonodavstva. Zajednički operativni postupci koje utvrde administratori počinju proizvoditi učinke kad se donesu odlukom Zajedničkog odbora.

Zajedničke operativne postupke donio je Zajednički odbor Odlukom br. 1/2020. Kako je navedeno u tom dokumentu, ažurirane zajedničke operativne postupke donijet će Zajednički odbor Odlukom br. 1/2024. U skladu s tom odlukom i zahtjevima Zajedničkog odbora administrator švicarskog registra i središnji administrator Unije izradili su i ažurirat će daljnje tehničke smjernice kako bi veza postala operativna i kako bi se osiguralo da se zajednički operativni postupci stalno prilagođavaju tehničkom napretku i novim zahtjevima u pogledu sigurnosti i zaštite veze te njezina djelotvornog i učinkovitog funkcioniranja.

2.1. Područje primjene

Ovaj dokument predstavlja zajednički dogovor stranaka Sporazuma u pogledu utvrđivanja proceduralnih temelja veze između registara ETS-a EU-a i ETS-a Švicarske. Iako se u njemu navode opći postupovni zahtjevi u pogledu rada, bit će potrebne dodatne tehničke smjernice kako bi veza postala operativna.

Za njezino pravilno funkcioniranje bit će potrebne tehničke specifikacije za bolju operativnost. U skladu s člankom 3. stavkom 7. Sporazuma ta su pitanja detaljno razrađena u dokumentu o tehničkim standardima za povezivanje, koji treba biti zasebno donesen odlukom Zajedničkog odbora.

Cilj je zajedničkih operativnih postupaka osigurati da se IT usluge povezane s funkcioniranjem veze između registara ETS-a EU-a i ETS-a Švicarske pružaju djelotvorno i učinkovito, posebno za ispunjavanje zahtjeva za uslugu, rješavanje propusta u pružanju usluga, rješavanje problema te obavljanje rutinskih operativnih zadaća u skladu s međunarodnim standardima za upravljanje IT uslugama.

Za trajnu vezu između registara bit će potrebni samo sljedeći zajednički operativni postupci, koji su dio ovog dokumenta:

- upravljanje incidentima,
- upravljanje problemima,
- ispunjavanje zahtjeva,
- upravljanje promjenama,
- upravljanje izdanjima,
- upravljanje incidentima u području sigurnosti,
- upravljanje sigurnošću informacija.

2.2. Adresati

Ovi zajednički operativni postupci namijenjeni su timovima za potporu registara EU-a i Švicarske.

3. PRISTUP I STANDARDI

Sljedeće se načelo primjenjuje na sve zajedničke operativne postupke:

- EU i Švicarska suglasni su utvrditi zajedničke operativne postupke na temelju Popisa infrastrukture informacijskih tehnologija (ITIL, verzija 4.). Prakse iz tog standarda ponovno se upotrebljavaju i prilagođavaju posebnim potrebama povezanima s trajnom vezom između registara,
- komunikacija i koordinacija potrebne za obradu zajedničkih operativnih postupaka između dviju stranaka provode se putem službi za podršku u okviru registara Švicarske i EU-a. Zadaće se uvijek dodjeljuju unutar jedne stranke,
- slučajeve neslaganja o postupanju u okviru određenog zajedničkog operativnog postupka analiziraju i rješavaju obje službe za podršku. Ako se ne može postići dogovor, zajedničko rješenje traži se na sljedećoj razini:

Razine upućivanja	EU	CH
1. razina	EU-ova služba za podršku	Švicarska služba za podršku
2. razina	EU-ov upravitelj operacija	Švicarski upravitelj za primjenu registra
3. razina	Zajednički odbor (koji može delegirati tu odgovornost uzimajući u obzir članak 12. stavak 5. Sporazuma o povezivanju)	
4. razina	Zajednički odbor, u slučaju delegiranja s 3. razine	

- svaka stranka može utvrditi postupke za rad svojeg sustava registra, uzimajući u obzir zahtjeve i sučelja povezane s navedenim zajedničkim operativnim postupcima,
- alat za upravljanje IT uslugama (ITSM) upotrebljava se za potporu zajedničkim operativnim postupcima, posebno za upravljanje incidentima, upravljanje problemima i ispunjavanje zahtjeva te komunikaciju između stranaka,

- osim toga, dopuštena je i razmjena informacija e-poštom,
- obje stranke osiguravaju ispunjavanje zahtjeva u pogledu sigurnosti informacija u skladu s uputama o postupanju.

4. UPRAVLJANJE INCIDENTIMA

Cilj je postupka za upravljanje incidentima vratiti IT usluge na uobičajenu razinu što je brže moguće nakon incidenta i uz minimalan prekid poslovanja.

U okviru upravljanja incidentima također bi trebalo voditi evidenciju incidenata za potrebe izvješćivanja te bi se taj postupak trebao integrirati s drugim procesima kako bi se potaknulo stalno poboljšavanje.

Upravljanje incidentima općenito obuhvaća sljedeće aktivnosti:

- otkrivanje i bilježenje incidenata,
- klasifikaciju i početnu potporu,
- istraživanje i dijagnosticiranje,
- rješavanje i oporavak,
- zatvaranje incidenata.

Tijekom životnog ciklusa incidenta na temelju postupka za upravljanje incidentima utvrđuje se odgovornost u svakom trenutku te način nadzora, praćenja i komunikacije.

4.1. Otkrivanje i bilježenje incidenata

Incident može otkriti skupina za podršku, automatizirani alat za praćenje ili tehničko osoblje koje provodi rutinski nadzor.

Nakon što se incident otkrije, mora se zabilježiti i mora mu se dodijeliti jedinstvena identifikacijska oznaka kako bi se omogućilo pravilno praćenje i nadzor incidenta. Jedinstvena identifikacijska oznaka incidenta identifikacijska je oznaka koju je u zajedničkom sustavu za otvaranje zahtjeva dodijelila služba za podršku stranke koja je prijavila incident (EU ili Švicarska) i mora se upotrebljavati u svoj komunikaciji povezanoj s tim incidentom.

Kontaktna točka za svaki incident trebala bi biti služba za podršku stranke koja je prijavila incident.

4.2. Klasifikacija i početna potpora

Cilj klasifikacije incidenta jest razumjeti i utvrditi koji su sustav i/ili usluga pogođeni i u kojoj mjeri. Djelotvornom klasifikacijom incident bi se odmah trebao usmjeriti do odgovarajućeg resursa kako bi se što brže riješio.

U fazi klasifikacije incident bi se trebao kategorizirati i trebalo bi mu odrediti prioritet u skladu s njegovim učinkom i hitnošću kako bi se riješio u odgovarajućem vremenskom okviru.

Ako bi incident mogao utjecati na povjerljivost ili cjelovitost osjetljivih podataka i/ili na dostupnost sustava, proglašava se i sigurnosnim incidentom te se njime nadalje upravlja u skladu s postupkom definiranim u poglavlju „Upravljanje incidentima u području sigurnosti” ovog dokumenta.

Ako je moguće, početnu dijagnozu obavlja služba za podršku koja je prijavila incident. Tijekom tog postupka ta će služba za podršku vidjeti radi li se o već poznatoj pogrešci. U tom će slučaju način rješavanja ili zaobilaženja incidenta već biti poznat i dokumentiran.

Ako služba za podršku u toj fazi uspješno riješi incident, zatvorit će ga jer je glavna svrha upravljanja incidentima (brza ponovna uspostava usluge za krajnjeg korisnika) ispunjena. Ako ga ne riješi, proslijedit će ga odgovarajućoj skupini za rješavanje incidenata radi daljnjeg istraživanja i dijagnosticiranja.

4.3. Istraživanje i dijagnosticiranje

Istraživanje i dijagnosticiranje incidenata provode se kad služba za podršku ne može riješiti incident u okviru početne dijagnoze te ga stoga upućuje na odgovarajuću razinu. Upućivanje incidenata sastavni je dio postupka istraživanja i dijagnosticiranja.

Uobičajena je praksa u fazi istraživanja i dijagnosticiranja pokušati ponoviti incident u kontroliranim uvjetima. Tijekom istraživanja i dijagnosticiranja važno je razumjeti točan redoslijed događaja koji su doveli do incidenta.

Upućivanje znači uviđanje da se incident ne može riješiti na trenutačnoj razini potpore i da se mora proslijediti skupini za potporu na višoj razini ili drugoj stranci. Incident se može uputiti na dva načina: horizontalno (funkcionalno) ili vertikalno (hijerarhijski).

Služba za podršku koja je zabilježila i otvorila incident odgovorna je za upućivanje incidenta prema odgovarajućem resursu te za praćenje općeg statusa i dodjele incidenta.

Stranka kojoj je incident dodijeljen odgovorna je za osiguravanje pravovremene provedbe traženih mjera i pružanje povratnih informacija svojoj službi za podršku.

4.4. Rješavanje i oporavak

Rješavanje incidenata i oporavak provode se nakon postizanja potpunog razumijevanja incidenta. Pronalaženje rješenja incidenta znači da je utvrđen način da se taj problem ukloni. Čin rješavanja faza je oporavka.

Nakon što odgovarajući resursi riješe propust u pružanju usluge, incident se vraća u relevantnu službu za podršku koja je prijavila incident te ta služba s pokretačem incidenta potvrđuje da je pogreška ispravljena i da se incident može zatvoriti. Rezultati obrade incidenta bilježe se za buduću uporabu.

Oporavak može obaviti osoblje za informatičku podršku ili se krajnjem korisniku daju upute koje treba slijediti.

4.5. Zatvaranje incidenta

Zatvaranje je završni korak u postupku upravljanja incidentima i odvija se ubrzo nakon rješavanja incidenta.

Među radnjama koje treba obaviti u fazi zatvaranja ističu se sljedeće:

- provjera početne kategorizacije incidenta,
- pravilno bilježenje svih informacija povezanih s incidentom,
- odgovarajuće dokumentiranje incidenta i ažuriranje baze znanja,
- odgovarajuća komunikacija sa svim dionicima na koje incident izravno ili neizravno utječe.

Incident se službeno zatvara nakon što služba za podršku završi fazu zatvaranja incidenta i o tome obavijesti drugu stranku.

Nakon što se incident zatvori, više se ne otvara. Ako se incident uskoro ponovi, ne otvara se prvotni incident nego se prijavljuje novi.

Ako incident prate službe za podršku EU-a i Švicarske, konačno zatvaranje odgovornost je službe za podršku koja ga je prijavila.

5. UPRAVLJANJE PROBLEMIMA

Taj bi postupak trebalo slijediti kad god se utvrdi problem i stoga pokrene postupak za upravljanje problemima. Upravljanje problemima usmjereno je na poboljšanje kvalitete i smanjenje broja zabilježenih incidenata. Problem može biti uzrok jednog ili više incidenata. Kad se prijavi incident, cilj je upravljanja incidentima što brže ponovno uspostaviti uslugu, među ostalim zaobilaženjem problema. Kad se pojavi problem, cilj je pronaći njegov uzrok kako bi se utvrdilo što je potrebno promijeniti kako bi se osiguralo da više ne dođe do tog problema ni povezanih incidenata.

5.1. Identifikacija i bilježenje problema

Ovisno o tome koja je stranka prijavila problem, kontaktna točka za pitanja povezana s tim problemom bit će služba za podršku EU-a ili Švicarske.

Jedinstvena identifikacijska oznaka problema identifikacijska je oznaka koju dodjeljuje služba za upravljanje IT uslugama (ITSM) i mora se upotrebljavati u svoj komunikaciji povezanoj s tim problemom.

Problem može biti uzrokovan incidentom ili može u bilo kojem trenutku biti pokrenut na vlastitu inicijativu kako bi se otklonile poteškoće otkrivene u sustavu.

5.2. Određivanje prioriteta problema

Kako bi se olakšalo njihovo praćenje, problemi se mogu kategorizirati prema ozbiljnosti i prioritetu na isti način kao i incidenti, uzimajući u obzir učinak povezanih incidenata i njihovu učestalost.

5.3. Istraživanje i dijagnosticiranje problema

Svaka stranka može prijaviti problem. Služba za podršku stranke koja je prijavila problem bit će odgovorna za evidentiranje problema, dodjeljivanje problema odgovarajućem resursu i praćenje općeg statusa problema.

Skupina za rješavanje problema kojoj je određeni problem upućen odgovorna je za njegovo pravovremeno rješavanje i komunikaciju sa službom za podršku.

Obje su stranke odgovorne za izvršavanje dodijeljenih radnji i pružanje povratnih informacija svojoj službi za podršku na zahtjev.

5.4. Rješavanje problema

Skupina za rješavanje problema kojoj je problem dodijeljen odgovorna je za njegovo rješavanje i pružanje relevantnih informacija službi za podršku svoje stranke.

Rezultati obrade problema bilježe se za buduću uporabu.

5.5. Zatvaranje problema

Problem se službeno zatvara nakon što se riješi unošenjem potrebnih promjena. Fazu zatvaranja problema provodi služba za podršku koja je evidentirala problem i obavijestila službu za podršku druge stranke.

6. ISPUNJAVANJE ZAHTJEVA

Postupak ispunjavanja zahtjeva je sveobuhvatno upravljanje zahtjevom za novu ili postojeću uslugu od trenutka registracije zahtjeva, preko njegova odobrenja do zatvaranja. Zahtjevi za usluge obično su mali, unaprijed definirani, ponovljivi, česti, prethodno odobreni i postupovni zahtjevi.

Glavni koraci koje treba slijediti navedeni su u nastavku.

6.1. Aktivacija zahtjeva

Informacije povezane sa zahtjevom za uslugu dostavljaju se službi za podršku EU-a ili Švicarske e-poštom, telefonski, putem alata za upravljanje IT uslugama (ITSM) ili nekim drugim dogovorenim komunikacijskim kanalom.

6.2. Evidentiranje i analiza zahtjeva

Kontaktna točka za sve zahtjeve za usluge trebala bi biti služba za podršku EU-a ili Švicarske, ovisno o tome koja je stranka uputila zahtjev za uslugu. Ta služba za podršku bit će odgovorna za evidentiranje i analizu zahtjeva za uslugu s dužnom pažnjom.

6.3. Odobrenje zahtjeva

Zaposlenik službe za podršku stranke koja je uputila zahtjev za uslugu provjerava treba li druga stranka dati kakva odobrenja te, ako je to slučaj, počinje ishoditi ta odobrenja. Ako zahtjev za uslugu nije odobren, služba za podršku ažurira i zatvara taj zahtjev.

6.4. Ispunjavanje zahtjeva

Tim se korakom omogućuje djelotvorno i učinkovito postupanje sa zahtjevima za usluge. Potrebno je razlikovati sljedeće slučajeve:

- ispunjavanje zahtjeva za uslugu odnosi se samo na jednu stranku: u tom slučaju ta stranka izdaje radne naloge i koordinira izvršenje,
- u ispunjavanje zahtjeva za uslugu uključene su obje stranke (i EU i Švicarska): u tom slučaju službe za podršku izdaju radne naloge u područjima za koja su nadležne. Provedba zahtjeva za uslugu koordinira se između obiju službi za podršku. Sveukupnu odgovornost snosi služba za podršku koja je primila i aktivirala zahtjev za uslugu.

Nakon što je zahtjev za uslugu ispunjen, mora mu se dodijeliti status „Riješeno”.

6.5. Upućivanje zahtjeva na višu razinu

Služba za podršku može neriješeni zahtjev za uslugu prema potrebi uputiti odgovarajućem resursu (trećoj strani).

Zahtjevi se upućuju odgovarajućoj trećoj strani, tj. služba za podršku EU-a morat će se za upućivanje trećoj strani u Švicarskoj konzultirati sa službom za podršku Švicarske, i obrnuto.

Treća strana kojoj je upućen zahtjev za uslugu odgovorna je za pravovremenu obradu tog zahtjeva i komunikaciju sa službom za podršku koja ga je uputila.

Služba za podršku koja je evidentirala zahtjev za uslugu odgovorna je za njegovu dodjelu i praćenje njegova općeg statusa.

6.6. Preispitivanje ispunjavanja zahtjeva

Prije zatvaranja zahtjeva za uslugu nadležna služba za podršku podnosi njegovu evidenciju na završnu kontrolu kvalitete. Cilj je osigurati da se zahtjev za uslugu u potpunosti obradi i da sve informacije potrebne za opis životnog ciklusa zahtjeva budu dovoljno detaljne. Osim toga, potrebno je zabilježiti i rezultate obrade zahtjeva za buduću uporabu.

6.7. Zatvaranje zahtjeva

Ako su stranke suglasne da je zahtjev za uslugu ispunjen i podnositelj zahtjeva smatra da je predmet riješen, zahtjev dobiva status „Zatvoreno”.

Zahtjev za uslugu službeno se zatvara nakon što služba za podršku koja je zahtjev evidentirala završi fazu zatvaranja i o tome obavijesti službu za podršku druge stranke.

7. UPRAVLJANJE PROMJENAMA

Cilj je osigurati primjenu standardiziranih metoda i postupaka za učinkovitu i brzu provedbu svih promjena u kontroli IT infrastrukture kako bi se smanjio broj i učinak svih povezanih incidenata na uslugu. Promjene u IT infrastrukturi mogu se pojaviti reaktivno – kao odgovor na probleme ili vanjske zahtjeve, npr. zakonodavne promjene, ili proaktivno – kao rezultat rada na poboljšanju učinkovitosti i djelotvornosti ili radi omogućavanja ili provedbe poslovnih inicijativa.

Postupak upravljanja promjenama uključuje više koraka, koji obuhvaćaju sve pojedinosti o zahtjevu za promjenu radi budućeg praćenja. Tim se postupcima osigurava da se promjena prije uvođenja potvrdi i testira. Postupak upravljanja izdanjima primjenjuje se radi uspješnog uvođenja.

7.1. Zahtjev za promjenu

Zahtjev za promjenu podnosi se timu za upravljanje promjenama na potvrdu i odobrenje. Kontaktna točka za sve zahtjeve za promjenu trebala bi biti služba za podršku EU-a ili Švicarske, ovisno o tome koja je stranka podnijela zahtjev. Služba za podršku bit će odgovorna za evidentiranje i analizu zahtjeva s dužnom pažnjom.

Izvori zahtjeva za promjenu mogu biti sljedeći:

- incident koji uzrokuje promjenu,
- postojeći problem koji dovodi do promjene,
- krajnji korisnik koji traži novu promjenu,
- promjena koja je posljedica tekućeg održavanja,
- zakonodavne promjene.

7.2. Evaluacija i planiranje promjene

Ta faza uključuje aktivnosti procjene i planiranja promjene. Ona obuhvaća utvrđivanje prioriteta i aktivnosti planiranja kako bi se minimizirali rizik i posljedice.

Ako izvršavanje zahtjeva za promjenu utječe i na EU i na Švicarsku, stranka koja je evidentirala taj zahtjev s drugom strankom provjerava evaluaciju i planiranje promjene.

7.3. Odobrenje promjene

Svaki registrirani zahtjev za promjenu mora biti odobren na odgovarajućoj razini.

7.4. Provedba promjene

Promjene se provode u okviru postupka upravljanja izdanjima. Timovi za upravljanje izdanjima obiju stranaka slijede vlastite postupke koji uključuju planiranje i ispitivanje. Promjene se preispituju nakon dovršetka provedbe. Kako bi se osiguralo da je sve izvršeno u skladu s planom, postojeći postupak upravljanja promjenama stalno se preispituje i ažurira kad god je to potrebno.

8. UPRAVLJANJE IZDANJIMA

Izdanje predstavlja jednu ili više promjena IT usluge, objedinjenih u planu izdanja, koje će trebati zajedno odobriti, pripremiti, izraditi, testirati i uvesti. Jedno izdanje može biti popravak *buga*, promjena hardvera ili drugih komponenti, promjena softvera, nadogradnja verzija aplikacije te promjena dokumentacije i/ili postupaka. Sadržajem svakog izdanja upravlja se, testira ga se i uvodi kao jedinstvenu cjelinu.

Cilj je upravljanja izdanjima planirati, izraditi, testirati, potvrditi i omogućiti pružanje osmišljenih usluga kojima će se ispuniti zahtjevi dionika i postići željeni ciljevi. Kriteriji prihvatljivosti za sve promjene usluge definiraju se i dokumentiraju tijekom koordinacije projektiranja te se dostavljaju timovima za upravljanje izdanjima.

Izdanje se obično sastoji od niza rješenja za probleme i poboljšanja određene usluge. Sadržava novi ili izmijenjeni potrebni softver te novi ili izmijenjeni hardver potreban za provedbu odobrenih promjena.

8.1. Planiranje izdanja

U prvom koraku postupka odobrene se promjene raspoređuju u pakete izdanja te se utvrđuju opseg i sadržaj izdanja. Na temelju tih informacija u potpostupku planiranja izdanja utvrđuje se vremenski raspored za izradu, testiranje i uvođenje izdanja.

Tijekom planiranja trebalo bi utvrditi:

- opseg i sadržaj izdanja,
- procjenu rizika i profil rizika za predmetno izdanje,
- klijente/korisnike na koje utječe predmetno izdanje,
- tim odgovoran za predmetno izdanje,
- strategiju isporuke i uvođenja,
- resurse za izdanje i njegovo uvođenje.

Svaka stranka obavješćuje drugu stranku o svojim planovima za nova izdanja i razdobljima održavanja. Ako novo izdanje utječe i na EU i na Švicarsku, oni koordiniraju planiranje i utvrđuju zajedničko razdoblje održavanja.

8.2. Izrada i testiranje paketa izdanja

U fazi izrade i testiranja u postupku upravljanja izdanjima utvrđuje se pristup provedbi izdanja ili paketa izdanja te održavanju kontroliranih okruženja prije promjene proizvodnje, kao i testiranju svih promjena u svim okruženjima novog izdanja.

Ako novo izdanje utječe i na EU i na Švicarsku, oni koordiniraju planove isporuke i testiranja. To uključuje sljedeće aspekte:

- način i vrijeme isporuke dijelova izdanja i komponenti usluge,
- uobičajene rokove isporuke, što se događa u slučaju kašnjenja,
- način praćenja napretka isporuke i dobivanja potvrde,
- parametre za praćenje i utvrđivanje uspjeha uvođenja novog izdanja,
- uobičajene testne slučajeve za relevantne funkcije i promjene.

Na kraju tog potpostupka sve potrebne komponente za novo izdanje spremne su za fazu uvođenja u praksi.

8.3. Priprema uvođenja

Potpostupkom pripreme osigurava se da komunikacijski planovi budu ispravno utvrđeni i da obavijesti budu spremne za slanje svim dionicima i krajnjim korisnicima za koje su bitne te da izdanje bude integrirano u postupak upravljanja promjenama kako bi se osiguralo da se sve promjene provode na kontroliran način i da ih odobravaju odgovarajući forumi.

Ako novo izdanje utječe i na EU i na Švicarsku, oni koordiniraju sljedeće aktivnosti:

- evidentiranje zahtjeva za promjenu za potrebe utvrđivanja rasporeda i pripreme uvođenja u proizvodno okruženje,
- izradu plana provedbe,
- pristup uklanjanju novog izdanja kako bi se u slučaju neuspjelog uvođenja moglo ponovno uvesti prethodno stanje,
- slanje obavijesti svim potrebnim strankama,
- traženje odobrenja za provedbu izdanja od relevantne razine.

8.4. Uklanjanje novog izdanja

Ako uvođenje ne uspije ili ako se testiranjem utvrdi da je uvođenje bilo neuspješno ili da nije ispunilo dogovorene kriterije prihvatljivosti/kvalitete, timovi za upravljanje izdanjima obiju stranaka morat će vratiti sustav u prethodno stanje. Trebat će obavijestiti sve potrebne dionike, uključujući krajnje korisnike na koje je novo izdanje utjecalo ili bilo usmjereno. Dok se čeka odobrenje, postupak može biti ponovno započet u bilo kojoj od prethodnih faza.

8.5. Preispitivanje i zaključenje izdanja

U preispitivanje novog izdanja trebalo bi uključiti sljedeće radnje:

- prikupljanje povratnih informacija o zadovoljstvu klijenata i korisnika odnosno o kvaliteti usluge uvođenja (prikupljanje povratnih informacija i njihovo razmatranje u svrhu stalnog poboljšavanja usluge),
- preispitivanje svih kriterija kvalitete koji nisu ispunjeni,
- provjeravanje jesu li izvršene sve radnje, potrebni popravci i promjene,
- osiguravanje da nakon završetka uvođenja nema nikakvih problema u pogledu sposobnosti, resursa, kapaciteta ili rada,
- provjeravanje da su klijenti, krajnji korisnici, operativna podrška i druge stranke na koje utječe novo izdanje registrirali i prihvatili eventualne probleme, utvrđene pogreške i metode zaobilaženja problema,
- praćenje incidenata i problema uzrokovanih uvođenjem novog izdanja (operativnim timovima pružiti ranu potporu ako je izdanje prouzročilo povećanje opsega rada),
- ažuriranje popratne dokumentacije (tj. dokumenata s tehničkim informacijama),
- službeno prepuštanje uvođenja novog izdanja timu za provedbu usluga,
- dokumentiranje stečenih iskustava,
- dobivanje dokumenta sa sažetkom izdanja od provedbenih timova,
- službeno zaključenje izdanja nakon provjere evidencije zahtjeva za promjenu.

9. UPRAVLJANJE INCIDENTIMA U PODRUČJU SIGURNOSTI

Upravljanje incidentima u području sigurnosti postupak je za rješavanje incidenata u području sigurnosti kako bi se omogućila komunikacija o incidentima s dionicima na koje bi oni mogli utjecati, evaluacija incidenata i određivanje prioriteta te odgovor na incidente radi saniranja svake povrede povjerljivosti, dostupnosti ili cjelovitosti osjetljive informacijske imovine do koje je stvarno došlo, na koju se sumnja ili do koje bi moglo doći.

9.1. Kategorizacija incidenata u području sigurnosti informacija

Svi incidenti koji utječu na vezu između registra Unije i švicarskog registra analiziraju se kako bi se utvrdila moguća povreda povjerljivosti, cjelovitosti ili dostupnosti svih osjetljivih informacija zabilježenih na popisu osjetljivih informacija (SIL).

U tom se slučaju incident smatra incidentom u području sigurnosti informacija i odmah se kao takav registrira u alatu za upravljanje IT uslugama (ITSM) te se njime upravlja na odgovarajući način.

9.2. Upravljanje incidentima u području sigurnosti informacija

Za incidente u području sigurnosti odgovorna je 3. razina upućivanja, a rješava ih poseban tim za upravljanje incidentima (IMT).

IMT je odgovoran za:

- provođenje prve analize, kategorizaciju i ocjenu težine incidenta,
- koordiniranje mjera među svim dionicima, uključujući potpunu dokumentaciju o analizi incidenta, odlukama donesenima za rješavanje incidenta i eventualnim utvrđenim nedostacima,
- ovisno o težini incidenta u području sigurnosti, njegovo pravovremeno upućivanje na odgovarajuću razinu radi informiranja i/ili donošenja odluke.

U postupku upravljanja sigurnošću informacija svim informacijama koje se odnose na incidente dodjeljuje se najviši stupanj osjetljivosti, koji u svakom slučaju ne smije biti niži od SENSITIVE (OSJETLJIVO): *ETS*.

Za istraživanje koje je u tijeku i/ili nedostatak koji bi se mogao zloupotrijebiti, sve do njegova otklanjanja, informacije se klasificiraju kao „SPECIAL HANDLING (POSEBNO POSTUPANJE): *ETS Critical (ETS kritično)*".

9.3. Identifikacija incidenata u području sigurnosti

Na temelju vrste događaja u području sigurnosti službenik za sigurnost informacija utvrđuje odgovarajuće organizacije koje će sudjelovati i biti dio IMT-a.

9.4. Analiza incidenata u području sigurnosti

IMT se radi preispitivanja incidenta povezuje sa svim uključenim organizacijama i relevantnim članovima njihovih timova, ovisno o slučaju. Tijekom analize utvrđuje se opseg gubitka povjerljivosti, cjelovitosti ili dostupnosti imovine te se procjenjuju posljedice za sve pogođene organizacije. Zatim se definiraju početne i naknadne mjere za rješavanje incidenta i upravljanje njegovim učinkom, uključujući učinak tih mjera na resurse.

9.5. Procjena težine, upućivanje na više razine i izvješćivanje o incidentima u području sigurnosti

Nakon što se za novi incident utvrdi da je incident u području sigurnosti, IMT procjenjuje njegovu težinu i u skladu s tim započinje s hitnim potrebnim mjerama.

9.6. Izvješćivanje o sigurnosnom odgovoru

U izvješće o odgovoru na incident u području sigurnosti informacija IMT uključuje rezultate postupka zaustavljanja i oporavka nakon incidenta. To se izvješće dostavlja na 3. razinu upućivanja sigurnom e-poštom ili drugim obostrano prihvaćenim sredstvom sigurne komunikacije.

Odgovorna stranka preispituje rezultate postupka zaustavljanja i oporavka te:

- ponovno povezuje registar ako je veza prethodno bila prekinuta,
- timovima u okviru registara dostavlja komunikaciju o incidentu,
- zatvara incident.

IMT bi u izvješće o odgovoru na incident u području sigurnosti informacija trebao na siguran način uključiti relevantne pojedinosti kako bi se osiguralo dosljedno evidentiranje i komunikacija te kako bi se omogućilo brzo i primjereno djelovanje za zaustavljanje incidenta. Nakon dovršetka izvješća o odgovoru na incident u području sigurnosti informacija, IMT ga pravovremeno dostavlja.

9.7. Praćenje, izgradnja kapaciteta i stalno poboljšavanje

Izvješća o svim incidentima u području sigurnosti IMT dostavlja 3. razini upućivanja, koja će ta izvješća upotrijebiti za utvrđivanje:

- slabih točaka u sigurnosnim kontrolama i/ili operacijama koje je potrebno ojačati,
- eventualne potrebe za poboljšanjem navedenog postupka kako bi se omogućio djelotvorniji odgovor na incidente,
- prilika za osposobljavanje i izgradnju kapaciteta kako bi se dodatno povećala otpornost sustava registara u pogledu sigurnosti informacija, smanjio rizik od budućih incidenata i minimizirao njihov učinak.

10. UPRAVLJANJE SIGURNOŠĆU INFORMACIJA

Cilj je upravljanja sigurnošću informacija osigurati povjerljivost, cjelovitost i dostupnost klasificiranih informacija, podataka i IT usluga organizacije. Kako bi se ispunili sigurnosni zahtjevi za trajnu vezu između registara, osim tehničkih komponenti, uključujući konstrukciju i testiranje (vidjeti LTS), potrebni su zajednički operativni postupci navedeni u nastavku.

10.1. Identifikacija osjetljivih informacija

Osjetljivost određene informacije procjenjuje se utvrđivanjem razine učinka koji bi povreda sigurnosti povezana s tom informacijom mogla imati na poduzeće (npr. financijski gubici, pad ugleda, kršenje zakona...).

Osjetljivost informacijske imovine utvrđuje se na temelju njezina utjecaja na povezivanje.

Stupanj osjetljivosti tih informacija procjenjuje se u skladu s ljestvicom osjetljivosti koja se primjenjuje na to povezivanje i detaljno se opisuje u odjeljku „Upravljanje incidentima u području sigurnosti informacija” ovog dokumenta.

10.2. Stupnjevi osjetljivosti informacijske imovine

Informacijska se imovina nakon identifikacije klasificira na temelju sljedećih pravila:

- ako se identificira najmanje jedan VISOKI stupanj povjerljivosti, cjelovitosti ili dostupnosti, imovina se klasificira kao „SPECIAL HANDLING (POSEBNO POSTUPANJE): *ETS Critical (ETS kritično)*”,
- ako se identificira najmanje jedan SREDNJI stupanj povjerljivosti, cjelovitosti ili dostupnosti, imovina se klasificira kao „ SENSITIVE (OSJETLJIVO): *ETS*”,
- ako se identificira najmanje jedan NISKI stupanj povjerljivosti, cjelovitosti ili dostupnosti, imovina se klasificira kao oznaka EU-a: „SENSITIVE (OSJETLJIVO): *Zajednička javna nabava*

u okviru ETS-a (ETS Joint Procurement)”. Oznaka Švicarske: „LIMITED (OGRANIČENO): ETS”.

10.3. Određivanje vlasnika informacijske imovine

Za svaku informacijsku imovinu trebao bi biti određen vlasnik. Informacijska imovina ETS-a koja pripada vezi između EUTL-a i SSTL-a ili je s njom povezana trebala bi biti uključena u zajednički popis imovine, koji vode obje stranke. Informacijska imovina ETS-a izvan veze između EUTL-a i SSTL-a trebala bi biti uključena u popis imovine koji vodi predmetna stranka.

Stranke se dogovaraju o vlasništvu nad svakom informacijskom imovinom koja pripada vezi između EUTL-a i SSTL-a ili je s njom povezana. Vlasnik informacijske imovine odgovoran je za procjenu njezine osjetljivosti.

Vlasnik bi trebao imati odgovarajuću razinu funkcije koja odgovara vrijednosti dodijeljene imovine. Trebalo bi dogovoriti i formalizirati vlasnikovu odgovornost za imovinu i obvezu održavanja potrebne razine povjerljivosti, cjelovitosti i dostupnosti.

10.4. Registracija osjetljivih informacija

Sve osjetljive informacije upisuju se na popis osjetljivih informacija (SIL).

Skup osjetljivih informacija koji bi mogao imati veće posljedice nego jedna informacija sama uzima se u obzir i bilježi u SIL-u (npr. skup informacija pohranjenih u bazi podataka sustava).

SIL nije statičan. Prijetnje, slabosti, vjerojatnost ili posljedice incidenata u području sigurnosti imovine mogu se promijeniti bez ikakve obavijesti, a u rad sustava registara može se uvesti nova imovina.

Stoga se SIL redovito preispituje, a svi novi podaci koji se identificiraju kao osjetljivi odmah se u njega upisuju.

U SIL-u se za svaki unos navode barem sljedeći podaci:

- opis informacije,
- vlasnik informacije,
- stupanj osjetljivosti,
- naznaka sadržava li informacija osobne podatke,
- dodatne informacije po potrebi.

10.5. Postupanje s osjetljivim informacijama

S osjetljivim informacijama koje se obrađuju izvan veze između registra Unije i švicarskog registra postupa se u skladu s uputama o postupanju.

S osjetljivim informacijama koje se obrađuju u vezi između registra Unije i švicarskog registra stranke postupaju u skladu sa sigurnosnim zahtjevima stranaka.

10.6. Upravljanje pristupom

Cilj je upravljanja pristupom ovlaštenim korisnicima dodijeliti pravo korištenja usluge, a neovlaštenim korisnicima onemogućiti pristup. Upravljanje pristupom ponekad se naziva i „upravljanje pravima” ili „upravljanje identitetom”.

Za trajnu vezu između registara i njezino funkcioniranje obje stranke trebaju imati pristup sljedećim komponentama:

- Wikiju – suradničkom okruženju za razmjenu zajedničkih informacija, primjerice o planiranju izdanja,
- alatu za upravljanje IT uslugama (ITSM) radi upravljanja incidentima i problemima (vidjeti poglavlje 3. „Pristup i standardi”),
- sustavu za razmjenu poruka: svaka stranka osigurava siguran sustav za razmjenu poruka koje sadržavaju podatke o transakcijama.

Administrator švicarskog registra i središnji administrator Unije osiguravaju ažuriranost prava pristupa i svojim strankama djeluju kao kontaktne točke za upravljanje pristupom. Zahtjevi za pristup obrađuju se u skladu s postupcima za ispunjavanje zahtjeva.

10.7. Upravljanje certifikatima/ključevima

Svaka je stranka odgovorna za upravljanje svojim certifikatima/ključevima (generiranje, registracija, pohrana, instalacija, uporaba, obnavljanje, ukidanje, sigurnosna kopija i povrat certifikata/ključeva). Kako je navedeno u tehničkim standardima za povezivanje (LTS), upotrebljavaju se samo digitalni certifikati koje je izdalo certifikacijsko tijelo koje ima povjerenje obiju stranaka. Postupanje s certifikatima/ključevima i njihova pohrana moraju biti u skladu s odredbama iz uputa o postupanju.

Obje stranke koordiniraju svako ukidanje i/ili obnavljanje certifikata i ključeva. To se odvija u skladu s postupcima za ispunjavanje zahtjeva.

Administrator švicarskog registra i središnji administrator Unije razmjenjivat će certifikate/ključeve sigurnim sredstvima komunikacije u skladu s odredbama utvrđenima u uputama o postupanju.

Svaka provjera certifikata/ključeva bilo kojim sredstvom komunikacije između stranaka provodit će se drugim putem.

PRILOG III.

TEHNIČKI STANDARDI ZA POVEZIVANJE (LTS)

u skladu s člankom 3. stavkom 7. Sporazuma između Europske unije i Švicarske Konfederacije o povezivanju njihovih sustava trgovanja emisijama stakleničkih plinova

Standard za trajnu vezu između registara

Sadržaj

1. Pojmovnik 30
2. Uvod 32
2.1. Područje primjene 32
2.2. Adresati 32
3. Opće odredbe 33
3.1. Struktura komunikacijske veze 33
3.1.1. Razmjena poruka 33
3.1.2. Poruka u XML-u – Detaljan opis 33
3.1.3. Termini prijenosa 33
3.1.4. Tokovi transakcijskih poruka 34
3.2. Sigurnost prijenosa podataka 36
3.2.1. Vatrozid i međumrežna povezanost 36
3.2.2. Virtualna privatna mreža (VPN) 36
3.2.3. Provedba IPSec-a 37
3.2.4. Protokol za siguran prijenos razmjene poruka 37
3.2.5. Šifriranje i potpis sadržaja u XML-u 37
3.2.6. Kriptografski ključevi 37
3.3. Popis funkcija u okviru veze 38
3.3.1. Poslovne transakcije 38
3.3.2. Protokol o usklađivanju 38
3.3.3. Testna poruka 39
3.4. Zahtjevi u pogledu bilježenja podataka 39
3.5. Operativni zahtjevi 40
4. Odredbe o dostupnosti 41
4.1. Oblikovanje dostupnosti komunikacije 41
4.2. Plan pokretanja, komunikacije, ponovne aktivacije i testiranja 41
4.2.1. Interna testiranja infrastrukture IKT-a 42

4.2.2. Komunikacijska testiranja 42
4.2.3. Testiranja cijelog sustava....42
4.2.4. Sigurnosna testiranja....42
4.3. Okruženja za prihvaćanje/testiranje....43
5. Odredbe o povjerljivosti i cjelovitosti 43
5.1. Infrastruktura za testiranje sigurnosti 43
5.2. Odredbe o suspenziji i ponovnoj aktivaciji veze 44
5.3. Odredbe o povredama sigurnosti....44
5.4. Smjernice za testiranje sigurnosti 45
5.4.1. Softver....45
5.4.2. Infrastruktura 45
5.5. Odredbe o procjeni rizika 45

1. POJMOVNIK

Tablica 1.1. Poslovne pokrate i definicije

Pokrata/termin	Definicija
Emisijska jedinica	Dopuštenje za ispuštanje jedne tone ekvivalenta ugljikova dioksida tijekom određenog razdoblja, valjano samo za ispunjavanje zahtjeva u okviru ETS-a EU-a ili ETS-a Švicarske
CH	Švicarska Konfederacija
CHU	Stacionarne emisijske jedinice, poznate i kao CHU2 (odnosi se na 2. obvezujuće razdoblje Kyotskog protokola), koje izdaje CH
CHUA	Švicarske emisijske jedinice za zrakoplovstvo
COP	Zajednički operativni postupci koje su zajednički oblikovale stranke Sporazuma kako bi veza između ETS-a EU-a i ETS-a Švicarske postala operativna
ETR	Registar trgovanja emisijama
ETS	Sustav trgovanja emisijama
EU	Europska unija
EUA	Opća emisijska jedinica EU-a

Pokrata/termin	Definicija
EUAA	Emisijska jedinica EU-a za zrakoplovstvo
EUCR	Konsolidirani registar Europske unije
EUTL	Dnevnik transakcija Europske unije
Registar	Sustav za obračunavanje emisijskih jedinica izdanih u okviru ETS-a, u kojem se prati vlasništvo nad emisijskim jedinicama koje se drže na elektroničkim računima
SSTL	Švicarski dopunski dnevnik transakcija
Transakcija	Postupak u registru koji uključuje prijenos emisijskih jedinica s jednog računa na drugi
Sustav dnevnika transakcija	U dnevniku transakcija bilježe se sve predložene transakcije iz jednog registra u drugi.

Tablica 1.2. Tehničke pokrate i definicije

Pokrata	Definicija
Asimetrična kriptografija	Upotrebljava javne i privatne ključeve za šifriranje i dešifriranje podataka
Certifikacijsko tijelo	Subjekt koji izdaje digitalne certifikate
Kriptografski ključ	Informacija koja određuje funkcionalni rezultat kriptografskog algoritma
Dešifriranje	Proces obrnut od šifriranja
Digitalni potpis	Matematička tehnika koja se upotrebljava za potvrđivanje autentičnosti i cjelovitosti poruke, softvera ili digitalnog dokumenta
Šifriranje	Postupak pretvaranja informacija ili podataka u kôd, posebno kako bi se spriječio neovlašten pristup
Unos datoteke	Proces čitanja datoteke
Vatrozid	Uređaj ili softver za sigurnost mreže koji prati i kontrolira ulazni i izlazni mrežni promet na temelju unaprijed utvrđenih pravila
Praćenje rada sustava	Signal koji se generira u pravilnim vremenskim razmacima, a prati ga hardver ili softver kao pokazatelj normalnog rada ili za usklađivanje drugih dijelova računalnog sustava
IPSec	Sigurnost internetskog protokola. Skup mrežnih protokola koji autentificira i šifrira pakete podataka kako bi se omogućila sigurna šifrirana komunikacija između dvaju računala putem mreže internetskog protokola.
Testiranje na probijanje	Praksa testiranja računalnog sustava, mreže ili mrežne aplikacije kako bi se pronašli sigurnosni nedostaci koje bi napadač mogao iskoristiti
Postupak usklađivanja	Postupak osiguravanja usklađenosti dvaju skupova zapisa
VPN	Virtualna privatna mreža
XML	Proširivi jezik za označivanje podataka. Dizajnerima omogućava da izrade vlastite prilagođene oznake, čime se omogućava definiranje, prijenos, potvrđivanje i tumačenje podataka među aplikacijama i među organizacijama.

2. UVOD

Sporazumom između Europske unije i Švicarske Konfederacije o povezivanju njihovih sustava trgovanja emisijama stakleničkih plinova od 23. studenog 2017. (dalje u tekstu „Sporazum”) omogućava se međusobno priznavanje emisijskih jedinica koje se mogu iskoristiti za ispunjenje obveze u okviru sustava trgovanja emisijskim jedinicama stakleničkih plinova Europske unije („ETS EU-a”) ili sustava trgovanja emisijskim jedinicama Švicarske („ETS Švicarske”). Kako bi veza između ETS-a EU-a i ETS-a Švicarske postala operativna, uspostavlja se izravna veza između dnevnika transakcija Europske unije (EUTL) u okviru registra Unije i Švicarskog dopunskog dnevnika transakcija (SSTL) u okviru švicarskog registra, čime će se omogućiti prijenos emisijskih jedinica izdanih u okviru tih ETS-ova iz jednog registra u drugi (članak 3. stavak 2. Sporazuma). Privremeno rješenje koje je omogućilo operativnost veze između ETS-a EU-a i ETS-a Švicarske uvedeno je 2020. Od 2023. veza između registara tih dvaju sustava trgovanja emisijama postupno će se razvijati u trajnu vezu između registara. Očekuje se da će se uspostaviti najkasnije 2024., čime se omogućuje funkcioniranje povezanih tržišta s obzirom na koristi od likvidnosti tržišta i izvršenja transakcija između dvaju povezanih sustava na način koji je istovjetan jednom tržištu koje čine dva sustava i koji sudionicima na tržištu omogućuje da djeluju kao da su na jednom tržištu, podložno samo pojedinačnim regulatornim odredbama stranaka (Prilog II. Sporazumu).

U skladu s člankom 3. stavkom 7. Sporazuma, administrator švicarskog registra i središnji administrator registra Unije izrađuju tehničke standarde za povezivanje (LTS), koji se temelje na načelima iz Priloga II. Sporazumu i u kojima se opisuju detaljni zahtjevi za uspostavu pouzdane i sigurne veze između SSTL-a i EUTL-a. Tehnički standardi za povezivanje koje izrade administratori počinju proizvoditi učinke kad se donesu odlukom Zajedničkog odbora.

Tehničke standarde za povezivanje donio je Zajednički odbor Odlukom br. 2/2020. Kako je navedeno u tom dokumentu, ažurirane tehničke standarde za povezivanje donijet će Zajednički odbor Odlukom br. 1/2024. U skladu s tom odlukom i zahtjevima Zajedničkog odbora administrator švicarskog registra i središnji administrator Unije izradili su i ažurirat će daljnje tehničke smjernice kako bi veza postala operativna i kako bi se osiguralo da se zajednički operativni postupci stalno prilagođavaju tehničkom napretku i/ili novim zahtjevima u pogledu sigurnosti i zaštite veze te njezina djelotvornog i učinkovitog funkcioniranja.

2.1. Područje primjene

Ovaj dokument predstavlja zajednički dogovor stranaka Sporazuma u pogledu utvrđivanja tehničkih temelja veze između registara ETS-a EU-a i ETS-a Švicarske. Iako se u njemu navode osnovne tehničke specifikacije u pogledu arhitektonskih, uslužnih i sigurnosnih zahtjeva, bit će potrebne daljnje detaljne smjernice kako bi veza postala operativna.

Potrebno je utvrditi procese i postupke kojima će se osiguravati daljnje pravilno funkcioniranje veze. U skladu s člankom 3. stavkom 6. Sporazuma ta su pitanja detaljno razrađena u zasebnom dokumentu o zajedničkim operativnim postupcima (COP), koji treba biti donesen odlukom Zajedničkog odbora.

2.2. Adresati

Ovaj je dokument upućen administratoru švicarskog registra i središnjem administratoru registra Unije.

3. OPĆE ODREDBE

3.1. Struktura komunikacijske veze

Svrha je ovog odjeljka opisati opću strukturu za postizanje operativnosti veze između ETS-a EU-a i ETS-a Švicarske te njezine različite sastavne dijelove.

Budući da je sigurnost ključna u utvrđivanju strukture, poduzete su sve mjere kako bi se postigla stabilna struktura. U okviru trajne veze između registara upotrebljava se mehanizam razmjene datoteka, čime se osigurava sigurnost veze na temelju fizičke odvojenosti od nezaštićenih mreža (eng. *air gap*).

Tehničko rješenje koristi:

- protokol za siguran prijenos razmjene poruka,
- poruke u XML-u,
- digitalni potpis i šifriranje na temelju XML-a,
- VPN.

U nastavku je prikazan opći pregled strukture stalne veze između registara.

3.1.1. Razmjena poruka

Komunikacija između registra Unije i švicarskog registra temelji se na mehanizmu razmjene poruka sigurnim kanalima. Svaka strana oslanja se na vlastiti repozitorij primljenih poruka.

Obje stranke vode evidenciju primljenih poruka zajedno s pojedinostima o obradi.

Pogreške ili neočekivani status potrebno je prijaviti kao upozorenje te bi trebalo uspostaviti osobni kontakt između timova za potporu.

S pogreškama i neočekivanim događajima postupa se u skladu s operativnim postupcima utvrđenima u postupku upravljanja incidentima u okviru zajedničkih operativnih postupaka.

3.1.2. Poruka u XML-u – Detaljan opis

Poruka u XML-u sadržava jedno od sljedećeg:

- jedan ili više zahtjeva za transakciju i/ili jedan ili više odgovora na transakciju,
- jednu operaciju/odgovor povezan s usklađivanjem,
- jednu testnu poruku.

Svaka poruka sadrži zaglavlje s:

- ETS-om iz kojeg dolazi,
- rednim brojem.

3.1.3. Termini prijenosa

Trajna veza između registara temelji se na unaprijed definiranim terminima prijenosa, nakon kojih slijedi niz imenovanih radnji. Zahtjevi za transakcije pristigli putem veze primaju se samo u unaprijed utvrđenim intervalima i uključuju tehničku potvrdu izlaznih i ulaznih transakcija. Osim toga, usklađivanje se može provoditi svakodnevno i može se aktivirati ručno.

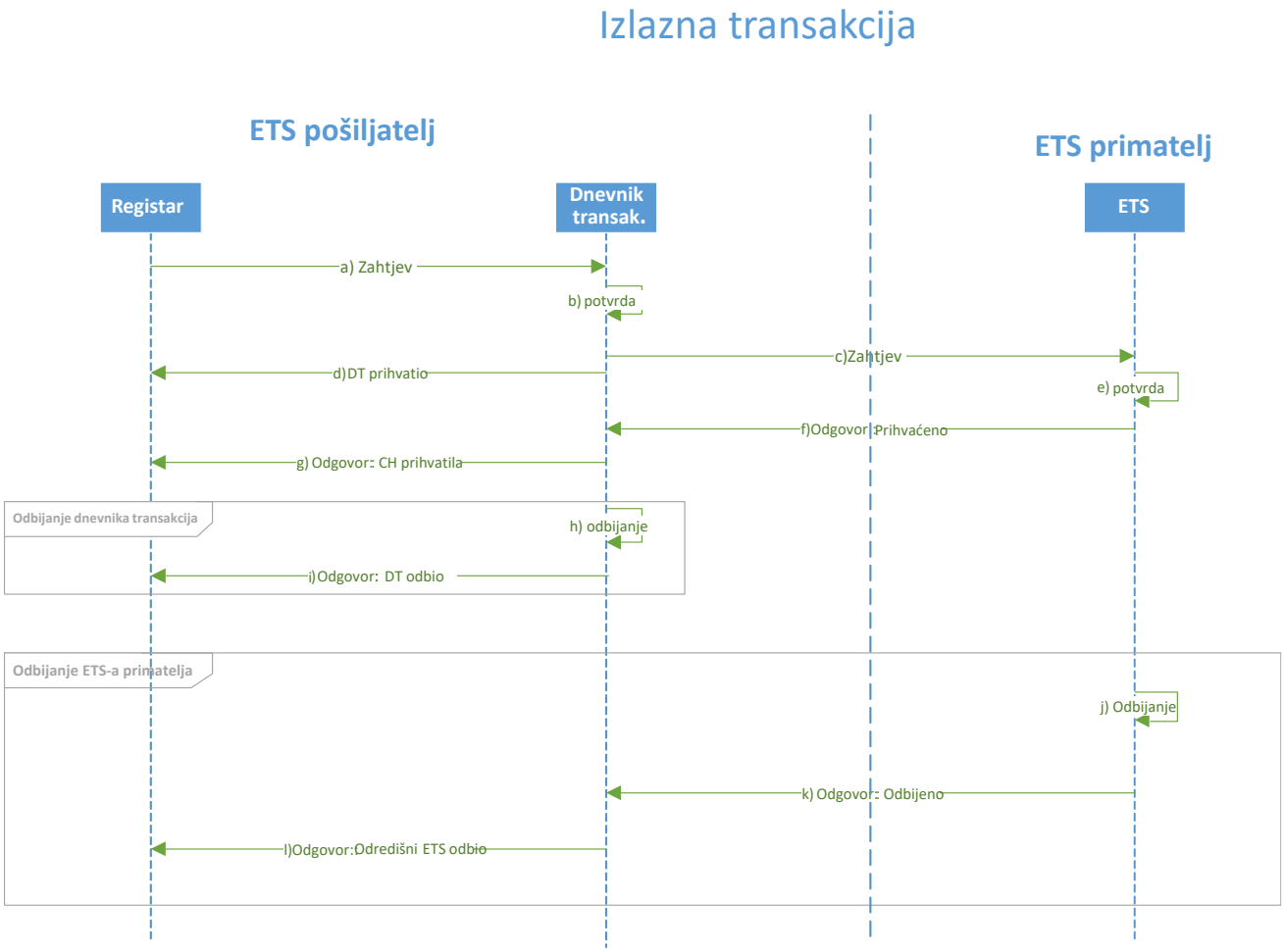
Promjene učestalosti i/ili vremena bilo koje od tih radnji provodit će se u skladu s operativnim

postupcima utvrđenima u postupku ispunjavanja zahtjeva u okviru zajedničkih operativnih postupaka.

3.1.4. Tokovi transakcijskih poruka

Izlazne transakcije

Postupak je opisan iz perspektive ETS-a pošiljatelja. Specifični tok prikazan je na shemi:



Glavni tok prikazuje sljedeće korake (kao u prethodnom grafičkom prikazu):

(a) kad je riječ o ETS-u pošiljatelju, zahtjev za transakciju šalje se iz registra u dnevnik transakcija nakon što se završe sve poslovne odgode (prema potrebi 24 sata);
(b) dnevnik transakcija potvrđuje zahtjev za transakciju;
(c) zahtjev za transakciju šalje se u odredišni ETS;
(d) odgovor o prihvaćanju šalje se u registar ishodišnog ETS-a;
(e) odredišni ETS potvrđuje zahtjev za transakciju;
(f) odredišni ETS šalje odgovor o prihvaćanju u dnevnik transakcija ishodišnog ETS-a;
(g) dnevnik transakcija šalje odgovor o prihvaćanju u registar.

Alternativni tok „Odbijanje dnevnika transakcija” (kao u prethodnom grafičkom prikazu, počevši od točke (a) u glavnom toku):

(a) zahtjev za transakciju šalje se u ishodišnom sustavu iz registra u dnevnik transakcija nakon što se završe sve poslovne odgode (prema potrebi 24 sata);

(b) dnevnik transakcija ne potvrđuje zahtjev:

(c) poruka o odbijanju zahtjeva šalje se u ishodišni registar.

Alternativni tok „Odbijanje ETS-a” (kao u prethodnom grafičkom prikazu, počevši od točke (d) u glavnom toku):

(a) zahtjev za transakciju šalje se u ishodišnom ETS-u iz registra u dnevnik transakcija nakon što se završe sve poslovne odgode (prema potrebi 24 sata);

(b) dnevnik transakcija potvrđuje transakciju;

(c) zahtjev za transakciju šalje se u odredišni ETS;

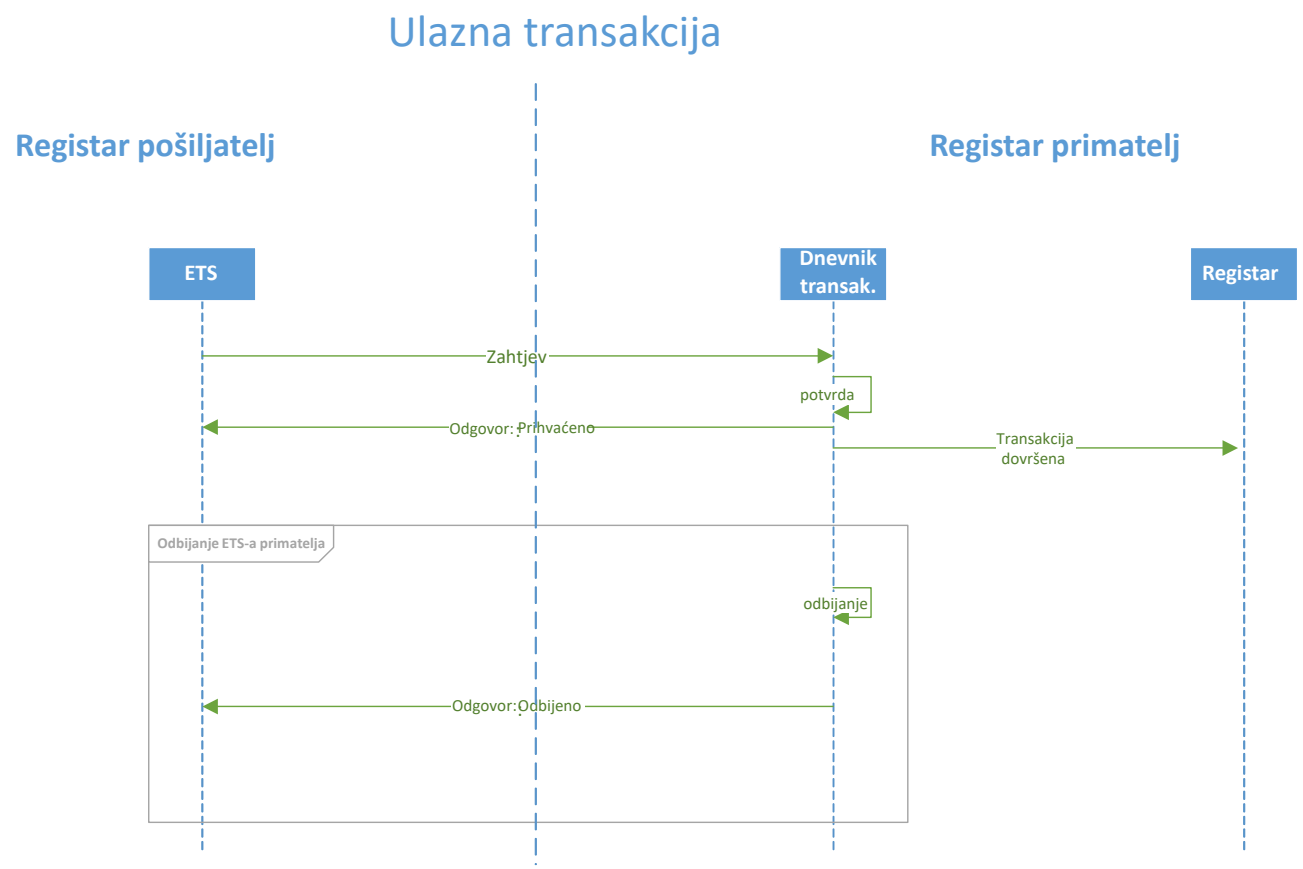
(d) poruka o prihvaćanju šalje se u registar ishodišnog ETS-a;

(e) u dnevniku transakcija u okviru ETS-a primatelja transakcija se ne potvrđuje;

(f) ETS primatelj šalje odgovor o odbijanju u dnevnik transakcija ETS-a pošiljatelja;

(g) dnevnik transakcija šalje odbijanje u registar.

Ulazne transakcije



Postupak je opisan iz perspektive ETS-a primatelja. Specifični tok prikazan je na shemi.

Na shemi se prikazuje sljedeće:

(1) kad dnevnik transakcija u okviru ETS-a primatelja potvrdi zahtjev, šalje poruku o prihvaćanju ETS-u pošiljatelju i poruku o dovršetku transakcije registru ETS-a primatelja;

(2) ako je ulazni zahtjev odbijen u dnevniku transakcija primatelja, zahtjev za transakciju ne šalje se registru ETS-a primatelja.

Protokol

Ciklus poruka o transakciji uključuje samo dvije poruke:

- ETS pošiljatelj → ETS primatelj: prijedlog transakcije,
- ETS primatelj → ETS pošiljatelj: odgovor o transakciji, koja se prihvaća ili odbija (uključujući razlog odbijanja)
  - prihvaćeno: transakcija je dovršena,
  - odbijeno: transakcija je prekinuta.

Status transakcije

- U ETS-u pošiljatelju transakcija će imati status „predloženo” kad se pošalje zahtjev za tu transakciju.
- U ETS-u primatelju transakcija će imati status „predloženo” nakon primitka i tijekom obrade zahtjeva.
- U ETS-u primatelju transakcija će dobiti status „dovršeno”/„prekinuto” nakon obrade zahtjeva. ETS primatelj zatim šalje odgovarajuću poruku o prihvaćanju/odbijanju.
- U ETS-u pošiljatelju transakcija dobiva status „dovršeno”/„prekinuto” nakon primitka i obrade poruke o prihvaćanju/odbijanju.
- Ako ne bude nikakvog odgovora, status transakcije u ETS-u pošiljatelju ostat će „predloženo”.
- Sve transakcije koje ostanu predložene dulje od 30 minuta ETS primatelj označava kao prekinute.

Incidenti povezani s transakcijama rješavat će se u skladu s operativnim postupcima utvrđenima u postupku upravljanja incidentima u okviru zajedničkih operativnih postupaka.

3.2. Sigurnost prijenosa podataka

Na podatke o prijenosu primjenjivat će se četiri razine zaštite:

(1) kontrola pristupa mreži: vatrozid i sloj međumrežne povezanosti;

(2) šifriranje na razini prijenosa: VPN;

(3) šifriranje na razini sesije: protokol za siguran prijenos razmjene poruka;

(4) šifriranje na razini aplikacije: šifriranje i potpis sadržaja u XML-u.

3.2.1. Vatrozid i međumrežna povezanost

Veza se uspostavlja putem mreže zaštićene hardverskim vatrozidom. Vatrozid mora biti konfiguriran tako da se samo „registrirani” klijenti mogu spajati na poslužitelj za VPN.

3.2.2. Virtualna privatna mreža (VPN)

Sva komunikacija između stranaka zaštićena je tehnologijom virtualne privatne mreže (VPN). Tehnologije VPN-a pružaju mogućnost „tunela” kroz mrežu kao što je internet od jedne do druge

točke, štiteći pritom svu komunikaciju. Prije stvaranja tunela VPN-a potencijalnom krajnjem klijentu izdaje se digitalni certifikat, čime se tom klijentu omogućava da dostavi dokaz identiteta tijekom pregovora o spajanju. Svaka je stranka odgovorna za ugradnju certifikata u svoju krajnju točku VPN-a. Upotrebom digitalnih certifikata svaki krajnji poslužitelj VPN-a pristupit će središnjem tijelu kako bi se utvrdili podaci za autentifikaciju. Tijekom postupka stvaranja tunela pregovara se o šifriranju, čime se osigurava zaštita sve komunikacije putem tunela.

Krajnje točke VPN-a klijenata moraju biti konfigurirane tako da trajno održavaju tunel VPN-a kako bi u svakom trenutku bila moguća pouzdana dvosmjerna komunikacija između stranaka u stvarnom vremenu.

Općenito, Europska unija upotrebljava mrežu STESTA (sigurne transeuropske telematske usluge među upravama) kao privatnu IP mrežu. Stoga je ta mreža prikladna i za trajnu vezu između registara.

3.2.3. Provedba IPSec-a

Upotrebom protokola IPSec za oblikovanje infrastrukture VPN-a između lokacija krajnjih korisnika osigurat će se autentifikacija te cjelovitost i šifriranje podataka između lokacija krajnjih korisnika. Konfiguracije IPSec VPN-a osiguravaju pravilnu autentifikaciju između dviju krajnjih točaka povezanih VPN-om. Stranke identificiraju i autentificiraju udaljenog klijenta putem veze IPSec upotrebom digitalnih certifikata koje dostavlja certifikacijsko tijelo koje priznaje druga strana.

IPsec osigurava i cjelovitost podataka u svoj komunikaciji koja se prenosi kroz tunel VPN-a. Podatkovni paketi raspršuju se (eng. *hash*) i potpisuju upotrebom podataka za autentifikaciju koje je utvrdio VPN. Povjerljivost podataka osigurava se i omogućavanjem šifriranja IPSec.

3.2.4. Protokol za siguran prijenos razmjene poruka

Trajna veza između registara temelji se na više slojeva šifriranja kako bi se postigla sigurna razmjena podataka između stranaka. Oba sustava i njihova različita okruženja međusobno su povezana na razini mreže s pomoću tunela VPN-a. Na razini aplikacije datoteke se prenose putem protokola za sigurnu razmjenu poruka na razini sesije.

3.2.5. Šifriranje i potpis sadržaja u XML-u

Potpisivanje i šifriranje u XML datotekama odvijaju se na dvije razine. Svaki zahtjev za transakciju, odgovor na transakciju i poruka o usklađivanju pojedinačno se digitalno potpisuju.

U drugom se koraku svaki podelement elementa „poruka” pojedinačno šifrira.

Uz to, kako bi se osiguralo da poruka bude cjelovita i da cijela poruka ne bude odbačena, u trećem se koraku digitalno potpisuje korijenski element poruke. Tako se dobiva visoka razina zaštite ugrađenih podataka u XML-u. U tehničkoj provedbi poštuju se standardi konzorcija World Wide Web.

Za dešifriranje i provjeru poruke postupak se provodi obrnutim redoslijedom.

3.2.6. Kriptografski ključevi

Kriptografija javnih ključeva upotrebljavat će se za šifriranje i potpisivanje.

Za poseban slučaj IPSec-a upotrebljava se digitalni certifikat koji je izdalo certifikacijsko tijelo koje ima povjerenje obiju stranaka. To certifikacijsko tijelo provjerava identitet i izdaje certifikate koji se upotrebljavaju za točnu identifikaciju organizacije i uspostavu kanala za sigurnu podatkovnu komunikaciju između stranaka.

Kriptografski ključevi upotrebljavaju se za potpisivanje i šifriranje komunikacijskih kanala i podatkovnih datoteka. Javne certifikate u digitalnom obliku stranke razmjenjuju sigurnim kanalima, a provjeravaju se drugim putem (eng. *out of band*). Taj je postupak dio postupka upravljanja sigurnošću informacija u okviru zajedničkih operativnih postupaka.

3.3. Popis funkcija u okviru veze

Veza određuje sustav prijenosa za niz funkcija kojima se provode poslovni procesi koji proizlaze iz Sporazuma. Veza uključuje i specifikaciju za postupak usklađivanja i za testne poruke koje će omogućiti praćenje rada sustava.

3.3.1. Poslovne transakcije

Iz poslovne perspektive veza omogućava četiri (4) vrste zahtjeva za transakciju:

- vanjski prijenos:
  - Nakon stupanja na snagu povezivanja ETS-ova, emisijske jedinice EU-a i Švicarske zamjenjive su i stoga u potpunosti prenosive između stranaka.
  - Prijenos putem veze uključivat će pošiljateljski račun u jednom ETS-u i primateljski račun u drugome.
  - prijenos može uključivati bilo koju količinu četiriju (4) vrsta jedinica:
    - švicarskih općih emisijskih jedinica (CHU),
    - švicarskih emisijskih jedinica za zrakoplovstvo (CHUA),
    - općih emisijskih jedinica EU-a (EUA),
    - emisijskih jedinica EU-a za zrakoplovstvo (EUAA).
- međunarodnu dodjelu:

operatori zrakoplova za koje je nadležan jedan ETS, a imaju obveze prema drugom ETS-u i imaju pravo na besplatne emisijske jedinice iz tog drugog ETS-a dobit će besplatne emisijske jedinice za zrakoplovstvo iz drugog ETS-a putem transakcije za međunarodnu dodjelu,

- poništavanje međunarodne dodjele:

Ta će transakcija biti izvršena ako se besplatne emisijske jedinice koje je drugi ETS dodijelio vlasničkom računu operatora zrakoplova moraju u potpunosti poništiti.

- povrat viška dodijeljenih jedinica:

Slično poništenju, ali se odnosi na slučajeve u kojima dodjela ne treba biti u potpunosti poništena, već se ETS-u koji je izvršio dodjelu treba vratiti samo višak dodijeljenih emisijskih jedinica.

3.3.2. Protokol o usklađivanju

Usklađivanje će se provoditi tek nakon što se završe primanje, potvrđivanje i obrada poruka.

Usklađivanje je sastavni dio mjera zaštite i ujednačenosti povezivanja. Stranke će se prije izrade rasporeda usuglasiti o točnom vremenu usklađivanja. Dnevno planirano usklađivanje može se provoditi ako se o tome slože obje stranke. No nakon primanja provest će se barem jedno planirano usklađivanje.

Međutim, svaka stranka može u bilo kojem trenutku pokrenuti ručno usklađivanje.

Vrijeme i učestalost planiranog usklađivanja mijenjat će se u skladu s operativnim postupcima utvrđenima u postupku ispunjavanja zahtjeva u okviru zajedničkih operativnih postupaka.

3.3.3. Testna poruka

Svrha testne poruke jest testirati komunikaciju između krajnjih korisnika. Poruka će sadržavati podatke koji će je identificirati kao testnu i druga će strana nakon primitka odgovoriti na nju.

3.4. Zahtjevi u pogledu bilježenja podataka

Kako bi obje stranke raspolagale točnim i dosljednim informacijama te kako bi se pružili alati za rješavanje nedosljednosti putem postupka usklađivanja, obje stranke čuvaju četiri (4) vrste podataka:

- dnevnike transakcija,
- dnevnike usklađivanja,
- arhivu poruka,
- dnevnike unutarnje revizije.

Svi navedeni podaci čuvaju se najmanje tri (3) mjeseca za potrebe otklanjanja problema, a njihovo daljnje čuvanje ovisit će o primjenjivom pravu svake stranke za potrebe revizije. Datoteke s podacima starije od tri (3) mjeseca mogu se pohraniti na sigurnu lokaciju u neovisnom IT sustavu pod uvjetom da ih se može dobiti ili im se može pristupiti u razumnom roku.

Dnevnici transakcija

Podsustavi EUTL i SSTL sadržavaju provedbu dnevnika transakcija. Oba su sustava ETS-a povezana.

Točnije, u dnevnicima transakcija evidentirat će se svaka predložena transakcija poslana drugom ETS-u. Svaki zapis uključuje sva polja sadržaja transakcije i naknadni ishod transakcije (odgovor ETS-a primatelja). U dnevnicima transakcija evidentirat će se i ulazne transakcije, kao i odgovori poslani ishodišnom ETS-u.

Dnevnici usklađivanja

U dnevniku usklađivanja evidentira se svaka poruka o usklađivanju koju su razmijenile stranke, uključujući identifikacijsku oznaku usklađivanja, vremenski žig i rezultat usklađivanja: status usklađivanja „Uspješno” ili „Nepodudarnosti”. Poruke o usklađivanju u okviru trajne veze između registara sastavni su dio razmijenjenih poruka i stoga se pohranjuju kako je opisano u odjeljku „Arhiva poruka”.

Svaka stranka u dnevniku usklađivanja evidentira svaki zahtjev i svoj odgovor. Iako se informacije u dnevniku usklađivanja ne dijele izravno u okviru samog usklađivanja, pristup tim informacijama može biti nužan kako bi se uklonile nepodudarnosti.

Arhiva poruka

Obje stranke moraju pohraniti kopiju razmijenjenih podataka (XML datoteke), poslanih i primljenih, uz navod jesu li te poruke u XML-u bile ispravne u svojem formatu.

Arhiva se uglavnom čuva za potrebe revizije, kako bi postojali dokazi o tome što je poslano drugoj stranci i primljeno od nje. S obzirom na to, osim datoteka potrebno je pohraniti i povezane certifikate.

U tim će se datotekama nalaziti i dodatne informacije za otklanjanje problema.

Dnevnik unutarnje revizije

Svaka stranka samostalno definira i upotrebljava te dnevnike.

3.5. Operativni zahtjevi

Razmjena podataka između dvaju sustava nije u potpunosti neovisna u okviru trajne veze između registara, što znači da su potrebni operatori i postupci da bi veza bila operativna. U tu je svrhu detaljno opisano nekoliko uloga i alata u tom procesu.

4. ODREDBE O DOSTUPNOSTI

4.1. Oblikovanje dostupnosti komunikacije

Struktura trajne veze između registara u osnovi je infrastruktura i softver IKT-a koji omogućavaju komunikaciju između ETS-a Švicarske i ETS-a EU-a. Osiguravanje visoke razine dostupnosti, cjelovitosti i povjerljivosti tog toka podataka postaje ključan aspekt koji treba uzeti u obzir pri oblikovanju trajne veze između registara. Budući da je riječ o projektu u kojem infrastruktura IKT-a, namjenski izrađen softver i procesi imaju važnu ulogu, sva se ta tri elementa moraju uzeti u obzir kako bi se oblikovao otporan sustav.

Otpornost infrastrukture IKT-a

U poglavlju o općim odredbama u ovom dokumentu detaljno su opisani strukturni sastavni dijelovi. Kad je riječ o infrastrukturi IKT-a, trajnom vezom između registara uspostavlja se otporna mreža VPN u kojoj se stvaraju tuneli za sigurnu komunikaciju, preko kojih se može odvijati sigurna razmjena poruka. Drugi infrastrukturni elementi konfigurirani su kao visokodostupni i/ili se oslanjaju na zamjenske mehanizme.

Otpornost namjenskog softvera

Namjenski izrađeni softverski moduli povećavaju otpornost tako što tijekom određenog vremenskog razdoblja pokušavaju uspostaviti komunikaciju s drugom stranom ako ona zbog bilo kojeg razloga nije dostupna.

Otpornost usluga

U trajnoj vezi između registara razmjena podataka između stranaka odvija se u unaprijed utvrđenim intervalima. Za neke od koraka u planiranoj razmjeni podataka potrebna je ručna intervencija operatora sustava i/ili administratora registara. S obzirom na to te kako bi se povećala dostupnost i uspjeh razmjena:

- u okviru operativnih postupaka predviđena su vremenska razdoblja za provedbu svake faze,
- softverski moduli za trajnu vezu između registara provode asinkronu komunikaciju,
- postupkom automatskog usklađivanja otkrit će se postoje li problemi pri primanju podatkovnih datoteka na bilo kojoj strani,
- postupci praćenja (infrastruktura IKT-a i namjenski softverski moduli) uzimaju se u obzir i pokreću postupke upravljanja incidentima (kako su definirani u dokumentu o zajedničkim operativnim postupcima). Ti postupci, čiji je cilj brža ponovna uspostava normalnog rada nakon incidenata, ključni su za osiguravanje visokih omjera dostupnosti.

4.2. Plan pokretanja, komunikacije, ponovne aktivacije i testiranja

Svi elementi uključeni u strukturu trajne veze između registara prolaze niz pojedinačnih i kolektivnih testova kako bi se potvrdilo da je platforma spremna na razini infrastrukture IKT-a i informacijskog sustava. Ti su operativni testovi obvezni svaki put kad se na platformi trajnoj vezi između registara status promijeni iz suspendiranog u operativni.

Za aktivaciju operativnog statusa veze potrebna je uspješna provedba unaprijed definiranog plana testiranja. Time se potvrđuje da je svaki registar najprije proveo niz internih testova, nakon čega je uslijedila potvrda povezivosti između krajnjih korisnika prije početka podnošenja proizvodnih transakcija između stranaka.

U planu testiranja treba navesti opću strategiju testiranja i pojedinosti o infrastrukturi za testiranje. Konkretno, svaki element u svakom testnom bloku trebao bi uključivati:

- kriterije i alate za testiranje,
- uloge dodijeljene za provođenje testiranja,
- očekivane rezultate (pozitivne i negativne),
- raspored testiranja,
- evidenciju zahtjeva u pogledu rezultata testiranja,
- dokumentaciju o otklanjanju problema,
- odredbe o upućivanju na više razine.

Kao proces, testiranja za aktivaciju operativnog statusa mogu se podijeliti na četiri (4) konceptualna bloka ili faze, kako je navedeno u nastavku.

4.2.1. Interna testiranja infrastrukture IKT-a

Ta bi testiranja administratori registara trebali provoditi i/ili provjeravati pojedinačno.

Svaki element infrastrukture IKT-a sa svake strane testira se pojedinačno. To uključuje svaku pojedinu komponentu infrastrukture. Ta se testiranja mogu provoditi automatski ili ručno, ali se njima mora provjeriti je li svaki element infrastrukture operativan.

4.2.2. Komunikacijska testiranja

Ta testiranja započinju pojedinačno u svakoj stranci i zaključuju se u suradnji s drugom stranom.

Nakon što pojedini elementi postanu operativni, potrebno je testirati komunikacijske kanale između dvaju registara. U tu svrhu svaka stranka provjerava je li omogućen pristup internetu, jesu li uspostavljeni tuneli VPN-a te postoji li IP povezanost između lokacija krajnjih korisnika. Druga strana zatim treba potvrditi dostupnost lokalnih i udaljenih infrastrukturnih elemenata i IP povezanost.

4.2.3. Testiranja cijelog sustava

Ta bi se ispitivanja trebala provoditi na obje strane, a rezultati dijeliti s drugom strankom.

Nakon što se testiraju komunikacijski kanali i svaki pojedini sastavni dio obaju registara, svaka strana priprema niz simuliranih transakcija i usklađivanja reprezentativnih za sve funkcije koje se provode putem veze.

4.2.4. Sigurnosna testiranja

Ta bi testiranja administratori registara trebali provesti i/ili pokrenuti sa svoje strane kako je detaljno opisano u odjeljcima „Smjernice za testiranje sigurnosti” i „Odredbe o procjeni rizika”.

Tek nakon završetka svake od četiri faze/bloka s predvidivim rezultatima može se smatrati da je trajna veza između registara operativna.

Resursi za testiranje

Svaka stranka računa na posebne resurse za testiranje (posebni softver i hardver za infrastrukturu IKT-a) i u svojem sustavu razvija funkcije testiranja kako bi poduprla ručno i kontinuirano potvrđivanje platforme. Administratori registara u svakom trenutku mogu provesti ručna pojedinačna ili kooperativna testiranja. Operativni status aktivira se ručno.

Isto je tako predviđeno da platforma redovito provodi automatske provjere. Cilj je tih provjera povećati dostupnost platforme ranim otkrivanjem mogućih problema povezanih s infrastrukturom ili softverom. Plan praćenja platforme sastoji se od dva elementa:

- praćenja infrastrukture IKT-a: infrastrukturu će sa svake strane pratiti pružatelji usluga infrastrukture IKT-a. Automatskim testiranjima bit će obuhvaćeni razni infrastrukturni elementi i dostupnost komunikacijskih kanala,
- praćenja aplikacija: softverski moduli za trajno povezivanje registara pratit će komunikaciju u sustavu na razini aplikacija (ručno i/ili u redovitim vremenskim razmacima), čime će se testirati dostupnost povezivanja krajnjih korisnika simuliranjem nekih transakcija preko veze.

4.3. Okruženja za prihvaćanje/testiranje

Struktura registra Unije i švicarskog registra sastoji se od sljedeća tri okruženja:

- proizvodnja (PROD): u tom se okruženju nalaze stvarni podaci i obrađuju stvarne transakcije,
- prihvaćanje (ACC): u tom se okruženju nalaze podaci koji nisu stvarni ili koji su anonimizirani i reprezentativni; u tom okruženju operatori sustava obiju stranaka potvrđuju nova izdanja,
- testiranje (TEST): u tom se okruženju nalaze podaci koji nisu stvarni ili koji su anonimizirani i reprezentativni; tom okruženju mogu pristupiti samo administratori registara te bi ga obje stranke trebale koristiti za provođenje integracijskih testova.

Osim VPN-a, navedena tri okruženja potpuno su neovisna jedno o drugome, što znači da su im hardver, softver, baze podataka, virtualna okruženja, IP adrese i ulazi uspostavljeni i djeluju neovisno jedni o drugima.

Kad je riječ o planu VPN-a, komunikacija između triju okruženja mora biti potpuno neovisna, što se osigurava upotrebom STESTA-e.

5. ODREDBE O POVJERLJIVOSTI I CJELOVITOSTI

Sigurnosnim mehanizmima i postupcima predviđena je uloga dviju osoba (načelo dvije kontrole) za operacije koje se odvijaju u vezi između registra Unije i švicarskog registra. Uloga dviju osoba primjenjuje se kad god je to potrebno, no možda nije primjenjiva na sve korake koje poduzimaju administratori registara.

Sigurnosni zahtjevi razmatraju se i analiziraju u planu upravljanja sigurnošću, koji uključuje i procese povezane s rješavanjem sigurnosnih incidenata nakon moguće povrede sigurnosti. Operativni dio tih procesa opisan je u zajedničkim operativnim postupcima.

5.1. Infrastruktura za testiranje sigurnosti

Svaka se stranka obvezuje uspostaviti infrastrukturu za testiranje sigurnosti (upotrebom zajedničkog softvera i hardvera koji se upotrebljavaju za otkrivanje nedostataka u fazama razvoja i rada):

- odvojeno od proizvodnog okruženja,
- ako sigurnost analizira tim neovisan o razvoju i radu sustava.

Svaka se stranka obvezuje provesti statičku i dinamičku analizu.

U slučaju dinamičke analize (kao što je testiranje na probijanje), obje se stranke obvezuju da će evaluacije u pravilu ograničavati na okruženja za testiranje i prihvaćanje (kako je definirano u odjeljku „Okruženja za prihvaćanje/testiranje”). Iznimke od tog načela trebaju odobriti obje stranke.

Prije uvođenja u proizvodno okruženje svaki softverski modul veze (kako je definirano u odjeljku „Struktura komunikacijske veze”) testira se u pogledu sigurnosti.

Infrastruktura za testiranje mora biti odvojena i na razini mreže i na razini infrastrukture od one za proizvodnju i omogućavati provedbu sigurnosnih testiranja potrebnih za provjeru usklađenosti sa sigurnosnim zahtjevima.

5.2. Odredbe o suspenziji i ponovnoj aktivaciji veze

Ako se posumnja da je sigurnost švicarskog registra, SSTL-a, registra Unije ili EUTL-a ugrožena, obje stranke odmah o tome obavješćuju jedna drugu te suspendiraju vezu između SSTL-a i EUTL-a.

Postupci razmjene informacija te odlučivanja o suspenziji i ponovnoj aktivaciji dio su procesa ispunjavanja zahtjeva u okviru zajedničkih operativnih postupaka.

Suspenzije

Do suspenzije veze između registara u skladu s Prilogom II. sporazumu može doći zbog:

- administrativnih razloga (održavanje itd.) – tada se radi o planiranoj suspenziji,
- razloga povezanih sa sigurnošću (ili kvarom informatičke infrastrukture) – tada se radi o neplaniranoj suspenziji.

U hitnim slučajevima svaka stranka obavješćuje drugu stranku i jednostrano suspendira vezu između registara.

Ako se donese odluka o suspenziji veze između registara, svaka će stranka osigurati prekid veze na razini mreže (blokiranjem nekih ili svih ulaznih i izlaznih povezivanja).

Odluka o suspenziji veze između registara, bez obzira na to je li planirana ili neplanirana, donosi se u skladu s postupkom upravljanja promjenama ili upravljanja incidentima u području sigurnosti u okviru zajedničkih operativnih postupaka.

Ponovna aktivacija komunikacije

Odluka o ponovnoj aktivaciji donosi se kako je detaljno opisano u zajedničkim operativnim postupcima, ali u svakom slučaju ne prije uspješnog završetka postupaka testiranja sigurnosti kako je navedeno u odjeljcima „Smjernice za testiranje sigurnosti” i „Plan pokretanja, komunikacije, ponovne aktivacije i testiranja”.

5.3. Odredbe o povredama sigurnosti

Povreda sigurnosti smatra se incidentom u području sigurnosti koji utječe na povjerljivost i cjelovitost osjetljivih informacija i/ili dostupnost sustava u kojem se one obrađuju.

Osjetljive informacije navedene su na popisu osjetljivih informacija i može ih se obrađivati u sustavu ili bilo kojem njegovu povezanom dijelu.

Informacije koje su izravno povezane s povredom sigurnosti smatrat će se osjetljivima, bit će označene kao „SPECIAL HANDLING (POSEBNO POSTUPANJE): *ETS Critical (ETS kritično)*” i s njima će se postupati u skladu s uputama o postupanju, osim ako je određeno drukčije.

Svaka povreda sigurnosti obrađivat će se u skladu s poglavljem „Upravljanje incidentima u području

sigurnosti” u okviru zajedničkih operativnih postupaka.

5.4. Smjernice za testiranje sigurnosti

5.4.1. Softver

Testiranje sigurnosti, uključujući testiranje na probijanje ako je primjenjivo, provodi se barem na svim većim novim izdanjima softvera u skladu sa sigurnosnim zahtjevima utvrđenima u tehničkim standardima za povezivanje kako bi se procijenila sigurnost povezivanja i povezani rizici.

Ako u posljednjih 12 mjeseci nije bilo velikog novog izdanja, provodi se testiranje sigurnosti postojećeg sustava s obzirom na razvoj kiberprijetnji u posljednjih 12 mjeseci.

Testiranje sigurnosti veze između registara provodi se u okruženju za prihvaćanje i, ako je potrebno, u proizvodnom okruženju te uz koordinaciju i uzajamnu suglasnost obiju stranaka.

Testiranjem mrežnih aplikacija poštovat će se međunarodni otvoreni standardi poput onih razvijenih u okviru projekta OWASP (eng. *Open Web Application Security Project*).

5.4.2. Infrastruktura

Infrastruktura koja podupire proizvodni sustav redovito se pregledava kako bi se nedostaci otkrili (najmanje jednom mjesečno) i otkriveni nedostaci uklonili u skladu s istim načelom kako je utvrđeno u prethodnom odjeljku uz upotrebu ažurirane baze podataka o nedostacima.

5.5. Odredbe o procjeni rizika

Ako je testiranje na probijanje primjenjivo, mora se uključiti u testiranje sigurnosti.

Svaka stranka može sklopiti ugovor sa specijaliziranim poduzećem za testiranje sigurnosti, pod uvjetom da to poduzeće:

- raspolaže vještinama i iskustvom za takvo testiranje sigurnosti,
- ne izvješćuje izravno poduzeće koje je razvilo predmetni softver i/ili njegova podizvođača niti je uključeno u razvoj softvera za vezu niti je podizvođač poduzeća koje je razvilo predmetni softver,
- ima potpisan ugovor o povjerljivosti podataka kako bi rezultati ostali povjerljivi i kako bi se njima postupalo na razini „SPECIAL HANDLING (POSEBNO POSTUPANJE): ETS Critical (ETS kritično)” u skladu s uputama o postupanju.