2024/1873

5.7.2024

DECIZIA (UE) 2024/1873 A CONSILIULUI

din 24 iunie 2024

privind poziția care urmează să fie adoptată în numele Uniunii Europene în cadrul comitetului mixt constituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră, în ceea ce privește modificarea anexei II la acord și a procedeelor comune de funcționare și a standardelor tehnice de creare a legăturii

(Text cu relevanță pentru SEE)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 192 alineatul (1), coroborat cu articolul 218 alineatul (9),

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră ([1]) (denumit în continuare „acordul") a fost semnat la 23 noiembrie 2017 în conformitate cu Decizia (UE) 2017/2240 a Consiliului ([2]).

(2) Acordul a fost încheiat prin Decizia (UE) 2018/219 a Consiliului ([3]) și a intrat în vigoare la 1 ianuarie 2020.

(3) În temeiul articolului 12 alineatul (3) din acord, comitetul mixt poate adopta decizii care, de la data intrării lor în vigoare, sunt obligatorii pentru părți.

(4) Articolul 13 alineatul (2) din acord prevede posibilitatea modificării de către Comitetul mixt a anexelor la acord.

(5) Articolul 3 alineatele (6) și (7) prevăd că procedurile comune de funcționare și standardele tehnice de creare a legăturii intră în vigoare atunci când sunt adoptate printr-o decizie a comitetului mixt. Prin Deciziile sale nr. 1/2020 ([4]) și nr. 2/2020 ([5]), comitetul mixt a adoptat procedurile comune de funcționare și, respectiv, standardele tehnice de creare a legăturii.

(6) Este oportun să se modifice anexa II la acord pentru a reflecta evoluția legăturii dintre registre între schema UE de comercializare a certificatelor de emisii și schema Elveției de comercializare a certificatelor de emisii și pentru a raționaliza dispozițiile anexei II în lumina evoluțiilor tehnologice. Pentru a asigura coerența procedeelor comune de funcționare și a standardelor tehnice de creare a legăturii cu anexa II, documentele respective ar trebui să fie de asemenea modificate.

([1]) JO L 322, 7.12.2017, p. 3.

([2]) Decizia (UE) 2017/2240 a Consiliului din 10 noiembrie 2017 privind semnarea, în numele Uniunii, și aplicarea cu titlu provizoriu a Acordului dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră (JO L 322, 7.12.2017, p. 1).

([3]) Decizia (UE) 2018/219 a Consiliului din 23 ianuarie 2018 privind încheierea Acordului dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră (JO L 43, 16.2.2018, p. 1).

([4]) Decizia nr. 1/2020 a Comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 5 noiembrie 2020 în ceea ce privește adoptarea unor procedee comune de funcționare [2021/1033] (JO L 226, 25.6.2021, p. 2).

([5]) Decizia nr. 2/2020 a comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 5 noiembrie 2020 privind modificarea anexelor I și II la acord și adoptarea standardelor tehnice de creare a legăturii (LTS) [2021/1034] (JO L 226, 25.6.2021, p. 16).

(7) În cadrul celei de a șaptea reuniuni a comitetului mixt, sau mai devreme, prin intermediul procedurii scrise în temeiul articolului 8 alineatul (4) din Regulamentul de procedură al comitetului mixt ([6]), acesta adoptă o decizie privind modificarea anexei II la acord și modificarea procedeelor comune de funcționare și a standardelor tehnice de creare a legăturii.

(8) Este oportun să se stabilească poziția care urmează să fie adoptată în numele Uniunii în cadrul comitetului mixt, în ceea ce privește modificarea anexei II la acord și modificarea procedeelor comune de funcționare și a standardelor tehnice de creare a legăturii, întrucât decizia va avea caracter obligatoriu pentru Uniune.

(9) Prin urmare, poziția Uniunii în cadrul comitetului mixt ar trebui să se bazeze pe proiectul de decizie atașat,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Poziția care urmează să fie adoptată în numele Uniunii în cadrul celei de-a șaptea reuniuni a comitetului mixt, sau mai devreme, prin intermediul procedurii scrise în temeiul articolului 8 alineatul (4) din Regulamentul de procedură al comitetului mixt, se bazează pe proiectul de decizie a comitetului mixt atașat la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare la data adoptării.

Adoptată la Luxemburg, 24 iunie 2024.

Pentru Consiliu

Președintele

D. CLARINVAL

([6]) Decizia nr. 1/2019 a comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 25 ianuarie 2019 privind adoptarea regulamentului său de procedură și Decizia (UE) 2018/1279 a Consiliului din 18 septembrie 2018 privind poziția care urmează să fie adoptată în numele Uniunii Europene în cadrul comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră în ceea ce privește adoptarea regulamentului său de procedură (JO L 239, 24.9.2018, p. 8).

DECIZIA NR. 1/2024 A COMITETULUI MIXT INSTITUIT PRIN ACORDUL DINTRE UNIUNEA EUROPEANĂ ȘI CONFEDERAȚIA ELVEȚIANĂ PENTRU CREAREA UNEI LEGĂTURI ÎNTRE RESPECTIVELE LOR SCHEME DE COMERCIALIZARE A CERTIFICATELOR DE EMISII DE GAZE CU EFECT DE SERĂ

din …

privind modificarea anexei II la acord și a procedeelor comune de funcționare și a standardelor tehnice de creare a legăturii

COMITETUL MIXT,

având în vedere Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră ([1]) (denumit în continuare „acordul"), în special articolul 9 și articolul 13 alineatul (2),

întrucât:

(1) Decizia nr. 2/2019 a Comitetului mixt ([2]) a prevăzut o soluție provizorie pentru operaționalizarea legăturii dintre EU ETS și ETS-ul Elveției.

(2) În cadrul celei de a treia reuniuni, Comitetul mixt a convenit asupra necesității de a analiza raportul cost-eficacitate al unei legături permanente între registrul Uniunii și registrul elvețian.

(3) În cadrul celei de a cincea reuniuni, Comitetul mixt a convenit asupra raportului prezentat de grupul de lucru constituit prin Deciziile 1/2020 ([3]) și 2/2020 ([4]) ale Comitetului mixt. În raportul respectiv grupul de lucru a analizat și a recomandat o abordare pentru punerea în aplicare a legăturii permanente dintre registrul Uniunii și registrul elvețian.

(4) Pentru a reflecta cerințele tehnice ale legăturii permanente dintre registrul Uniunii și registrul elvețian, precum și pentru a raționaliza dispozițiile anexei II la acord în lumina evoluțiilor tehnologice, anexa II la acord ar trebui modificată.

(5) Pentru a asigura coerența procedeelor comune de funcționare și a standardelor tehnice de creare a unei legături cu anexa II la acord, documentele respective ar trebui, de asemenea, modificate,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

(1) Anexa II la acord se înlocuiește cu textul prevăzut în anexa I la prezenta decizie.

(2) Procedeele comune de funcționare menționate la articolul 3 alineatul (6) din acord sunt prevăzute în anexa II la prezenta decizie. Acestea înlocuiesc procedeele comune de funcționare prevăzute în anexa la Decizia nr. 1/2020.

(3) Standardele tehnice de creare a legăturii menționate la articolul 3 alineatul (7) din acord sunt stabilite în anexa III la prezenta decizie. Acestea înlocuiesc standardele tehnice de creare a legăturii prevăzute în anexa la Decizia nr. 2/2020.

([1]) JO L 322, 7.12.2017, p. 3.

([2]) Decizia nr. 2/2019 a Comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 5 decembrie 2019 de modificare a anexelor I și II la Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră [2020/1359] (JO L 314, 29.9.2020, p. 68).

([3]) Decizia nr. 1/2020 a Comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 5 noiembrie 2020 în ceea ce privește adoptarea unor procedee comune de funcționare [2021/1033] (JO L 226, 25.6.2021, p. 2).

([4]) Decizia nr. 2/2020 a comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 5 noiembrie 2020 privind modificarea anexelor I și II la acord și adoptarea standardelor tehnice de creare a legăturii (LTS) [2021/1034] (JO L 226, 25.6.2021, p. 16).

Articolul 2

Prezenta decizie intră în vigoare la data adoptării.

Adoptată la …, la …

Pentru Comitetul mixt

Secretarul pentru Uniunea Europeană	*Președintele*	*Secretarul pentru Elveția*

ANEXA I

„ANEXA II

STANDARDE TEHNICE DE CREARE A LEGĂTURII

Pentru a operaționaliza legătura dintre EU ETS și ETS-ul Elveției, în 2020 a fost pusă în aplicare o soluție provizorie. Începând din 2023, legătura dintre cele două sisteme de comercializare a certificatelor de emisii se va transforma treptat într-o legătură permanentă între registre, a cărei implementare este preconizată a avea loc cel târziu în 2024, care va permite funcționarea piețelor legate în ceea ce privește beneficiile oferite de lichiditatea pieței și de executarea tranzacțiilor între cele două sisteme conectate într-un mod echivalent cu o piață formată din două sisteme și care va permite participanților la piață să acționeze ca și cum ar fi pe o singură piață, sub rezerva unor dispoziții de reglementare individuale ale părților.

Standardele tehnice de creare a legăturii (LTS) specifică:

— arhitectura legăturii de comunicare;

— comunicările dintre SSTL și EUTL;

— securitatea transferului de date;

— lista funcțiilor (tranzacții, reconciliere etc.);

— definiția nivelului de transport;

— cerințele referitoare la arhivarea datelor;

— aranjamentele operaționale (serviciul de asistență, sprijinul);

— planul de activare a comunicării și procedura de testare;

— procedura de testare a securității.

LTS precizează că administratorii trebuie să ia toate măsurile rezonabile pentru a se asigura că SSTL, EUTL și legătura sunt operaționale 24 de ore pe zi și 7 zile pe săptămână și că orice întreruperi ale funcționării SSTL, a EUTL și a legăturii sunt menținute la un nivel minim.

LTS stabilesc cerințe de securitate suplimentare pentru registrul elvețian, SSTL, registrul Uniunii și EUTL și sunt consemnate într-un «plan de gestionare a securității». LTS precizează în special că:

— dacă există suspiciunea că securitatea registrului elvețian, a SSTL, a registrului Uniunii sau a EUTL a fost compromisă, părțile se informează reciproc imediat și suspendă legătura dintre SSTL și EUTL;

— în caz de încălcare a securității, părțile se angajează să facă imediat schimb de informații. În măsura în care se cunosc detaliile tehnice, administratorul registrului elvețian și administratorul central al Uniunii își transmit, în termen de 24 de ore după ce un incident de securitate este identificat drept o încălcare a securității, un raport în care este descris incidentul (data, cauza, impactul, soluțiile de remediere).

Procedura de testare a securității prevăzută în LTS se aplică înainte de stabilirea legăturii de comunicare dintre SSTL și EUTL și ori de câte ori este necesară o nouă versiune sau ediție a SSTL sau a EUTL.

LTS prevăd două medii de testare în plus față de mediul de producție: un mediu de testare pentru dezvoltator și un mediu de acceptare.

Părțile prezintă dovezi, prin intermediul administratorului registrului elvețian și al administratorului central al Uniunii, că a fost efectuată în precedentele 12 luni o evaluare independentă a securității sistemelor lor în conformitate cu cerințele de securitate prevăzute în LTS. Toate noile ediții importante de software sunt supuse, în conformitate cu cerințele de securitate prevăzute în LTS, unor teste de securitate, în special testului de rezistență la intruziuni. Testul de rezistență la intruziuni nu se efectuează de către dezvoltatorul software-ului sau un subcontractant al acestuia.”

ANEXA II

PROCEDEELE COMUNE DE FUNCȚIONARE ÎN TEMEIUL ARTICOLULUI 3 ALINEATUL (6) DIN ACORDUL DINTRE UNIUNEA EUROPEANĂ ȘI CONFEDERAȚIA ELVEȚIANĂ PENTRU CREAREA UNEI LEGĂTURI ÎNTRE RESPECTIVELE LOR SCHEME DE COMERCIALIZARE A CERTIFICATELOR DE EMISII DE GAZE CU EFECT DE SERĂ

Proceduri pentru legătura permanentă între registre

Cuprins

1. GLOSAR . . . 9
2. INTRODUCERE . . . 9
2.1. Domeniul de aplicare . . . 10
2.2. Destinatari . . . 10
3. ABORDARE ȘI STANDARDE . . . 10
4. GESTIONAREA INCIDENTELOR . . . 11
4.1. Identificarea și înregistrarea incidentelor . . . 11
4.2. Clasificarea și asistența inițială . . . 11
4.3. Investigarea și diagnosticarea . . . 12
4.4. Rezolvarea și restabilirea sistemului . . . 12
4.5. Închiderea incidentului . . . 12
5. GESTIONAREA PROBLEMELOR . . . 13
5.1. Identificarea și înregistrarea problemelor . . . 13
5.2. Ierarhizarea problemelor . . . 13
5.3. Investigarea și diagnosticarea problemelor . . . 13
5.4. Rezoluția . . . 13
5.5. Închiderea problemei . . . 13
6. SOLUȚIONAREA CERERILOR . . . 13
6.1. Inițierea cererii . . . 13
6.2. Înregistrarea și analiza cererilor . . . 14
6.3. Aprobarea cererilor . . . 14
6.4. Soluționarea cererilor . . . 14
6.5. Transmiterea cererilor . . . 14
6.6. Verificarea procesului de soluționare a cererii . . . 14
6.7. Închiderea cererii . . . 14
7. GESTIONAREA MODIFICĂRILOR . . . 14
7.1. Cererea de modificare . . . 15
7.2. Evaluarea și planificarea modificărilor . . . 15
7.3. Aprobările modificărilor . . . 15
7.4. Implementarea modificărilor . . . 15
8. GESTIONAREA VERSIUNILOR . . . 15
8.1. Planificarea versiunii . . . 15
8.2. Conceperea și testarea pachetului de versiuni . . . 16
8.3. Pregătirea implementării . . . 16

8.4. Readucerea versiunii la starea anterioară . . . 16
8.5. Evaluarea și finalizarea versiunii . . . 16
9. GESTIONAREA INCIDENTELOR DE SECURITATE . . . 17
9.1. Clasificarea incidentelor de securitate a informațiilor . . . 17
9.2. Gestionarea incidentelor de securitate a informațiilor . . . 17
9.3. Identificarea incidentelor de securitate . . . 17
9.4. Analiza incidentelor de securitate . . . 17
9.5. Evaluarea gravității incidentelor de securitate, transmiterea și raportarea acestora . . . 17
9.6. Raportarea răspunsurilor la incidentele de securitate . . . 18
9.7. Monitorizarea, consolidarea capacităților și îmbunătățirea continuă . . . 18
10. MANAGEMENTUL SECURITĂȚII INFORMAȚIILOR . . . 18
10.1. Identificarea informațiilor sensibile . . . 18
10.2. Nivelurile de sensibilitate ale activelor informaționale . . . 18
10.3. Desemnarea proprietarului activelor informaționale . . . 18
10.4. Înregistrarea informațiilor sensibile . . . 19
10.5. Gestionarea informațiilor sensibile . . . 19
10.6. Gestionarea accesului . . . 19
10.7. Gestionarea certificatelor/cheilor . . . 19

1. GLOSAR

Tabelul 1-1 Acronime și definiții

Acronim/termen	Definiție
Autoritate de certificare (CA)	Entitatea care emite certificate digitale
CH	Confederația Elvețiană
ETS	Schema de comercializare a certificatelor de emisii
UE	Uniunea Europeană
IMT	Echipa de gestionare a incidentelor
Activ informațional	O informație care prezintă valoare pentru o societate sau o organizație
IT	Instrucțiuni de securitate pentru program/proiect
ITIL	Bibliotecă pentru infrastructura tehnologiei informației
ITSM	Gestionarea serviciilor IT
LTS	Standarde tehnice de creare a legăturii
Registrul	Un sistem de contabilizare a certificatelor emise în cadrul ETS, care ține evidența drepturilor de proprietate asupra certificatelor deținute în conturile electronice.
RFC	Cererea de modificare
SIL	Evidența informațiilor sensibile
SR	Cerere de servicii
Wiki	Site web care permite utilizatorilor să facă schimb de informații și de cunoștințe prin adăugarea sau adaptarea conținutului în mod direct prin intermediul unui browser web.

2. INTRODUCERE

Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 23 noiembrie 2017 (denumit în continuare „acordul”) prevede recunoașterea reciprocă a certificatelor de emisii care pot fi utilizate pentru asigurarea conformității în cadrul sistemului de comercializare a certificatelor de emisii (denumit în continuare „EU ETS”) sau în cadrul sistemului Elveției de comercializare a certificatelor de emisii (denumit în continuare „ETS-ul Elveției”). În vederea activării legăturii dintre EU ETS și ETS-ul Elveției, se va crea o legătură directă între Registrul de tranzacții al Uniunii Europene (EUTL) din cadrul registrului Uniunii și Registrul suplimentar de tranzacții al Elveției (SSTL) din cadrul registrului elvețian, ceea ce va permite transferul dintr-un registru în altul al certificatelor de emisii emise în cadrul oricăruia dintre ETS-uri [articolul 3 alineatul (2) din acord]. Pentru a operaționaliza legătura dintre EU ETS și ETS-ul Elveției, în 2020 a fost pusă în aplicare o soluție provizorie. Începând din 2023, legătura dintre cele două sisteme de comercializare a certificatelor de emisii se va transforma treptat într-o legătură permanentă între registre, a cărei implementare este preconizată a avea loc cel târziu în 2024, care va permite funcționarea piețelor legate în ceea ce privește beneficiile oferite de lichiditatea pieței și de executarea tranzacțiilor între cele două sisteme conectate într-un mod echivalent cu o piață formată din două sisteme și care va permite participanților la piață să acționeze ca și cum ar fi pe o singură piață, sub rezerva unor dispoziții de reglementare individuale ale părților (Anexa II la acord).

În temeiul articolului 3 alineatul (6) din acord, administratorul registrului elvețian și administratorul central al Uniunii stabilesc procedeele comune de funcționare pentru aspectele tehnice sau alte aspecte care sunt necesare pentru funcționarea legăturii, ținând cont de prioritățile din legislația națională. Procedeele comune de funcționare elaborate de administratori produc efecte după ce sunt adoptate prin decizia comitetului mixt.

Procedeele comune de funcționare au fost adoptate de comitetul mixt prin Decizia nr. 1/2020. Procedeele comune de funcționare actualizate, astfel cum sunt specificate în prezentul document, vor fi adoptate prin Decizia nr. 1/2024 a comitetului mixt. În conformitate cu prezenta decizie și cu solicitările Comitetului mixt, administratorul registrului elvețian și administratorul central al Uniunii au elaborat și vor actualiza orientări tehnice suplimentare pentru activarea legăturii și pentru a garanta că acestea sunt adaptate permanent la progresul tehnic și la noile cerințe privind siguranța și securitatea legăturii și funcționarea efectivă și eficientă a acesteia.

2.1. Domeniul de aplicare

Prezentul document reprezintă înțelegerea comună dintre părțile la acord cu privire la stabilirea fundamentelor procedurale ale legăturii dintre registrele EU ETS și ETS-ul Elveției. Acesta prezintă cerințele procedurale generale în ceea ce privește operațiunile, însă vor fi necesare unele orientări tehnice suplimentare pentru activarea legăturii.

Pentru funcționarea corespunzătoare, legătura va necesita specificații tehnice pentru operaționalizarea în continuare a acesteia. În temeiul articolului 3 alineatul (7) din acord, aceste aspecte sunt prezentate în detaliu în documentul privind standardele tehnice de creare a legăturii (LTS), care urmează să fie adoptat separat prin decizia comitetului mixt.

Obiectivul procedeelor comune de funcționare este de a asigura prestarea efectivă și eficientă a serviciilor IT asociate cu funcționarea legăturii dintre registrele EU ETS și ETS al Elveției, în special în ceea ce privește soluționarea cererilor de servicii, rezolvarea cazurilor de întrerupere a serviciului, remedierea problemelor, precum și îndeplinirea sarcinilor operaționale de rutină în conformitate cu standardele internaționale privind gestionarea serviciilor IT.

Pentru legătura permanentă între registre, vor fi necesare doar următoarele procedee comune de funcționare, incluse în prezentul document:

— gestionarea incidentelor;

— gestionarea problemelor;

— soluționarea cererilor;

— gestionarea modificărilor;

— gestionarea versiunilor;

— gestionarea incidentelor de securitate;

— managementul securității informațiilor.

2.2. Destinatari

Beneficiarii vizați ai prezentelor procedee comune de funcționare sunt echipele de asistență ale registrelor din UE și Elveția.

3. ABORDARE ȘI STANDARDE

Următorul principiu se aplică tuturor procedeelor comune de funcționare:

— UE și CH convin asupra definirii procedeelor comune de funcționare pe baza ITIL (Biblioteca pentru infrastructura tehnologiei informației, versiunea 4). Practicile specificate în acest standard sunt reutilizate și adaptate necesităților specifice legăturii permanente între registre;

— Comunicarea și coordonarea necesare pentru prelucrarea procedeelor comune de funcționare dintre cele două părți se realizează prin intermediul serviciilor de asistență ale registrelor din CH și UE. Sarcinile sunt întotdeauna atribuite în cadrul unei singure părți.

— În cazul unui dezacord cu privire la gestionarea unui procedeu comun de funcționare, acesta va fi analizat și soluționat între cele două servicii de asistență. În cazul în care nu se poate ajunge la niciun acord, găsirea unei soluții comune este transmisă la nivelul următor.

Niveluri de transmitere	UE	CH
Nivelul 1	Serviciul de asistență UE	Serviciul de asistență CH
Nivelul 2	Managerul pentru operațiuni al UE	Managerul pentru aplicații din cadrul registrului CH
Nivelul 3	Comitetul mixt [care poate delega această responsabilitate în temeiul articolului 12 alineatul (5) din acord]	
Nivelul 4	Comitetul mixt, în cazul delegării responsabilității de la nivelul 3	

— Fiecare parte poate stabili procedeele de funcționare pentru propriul sistem de registre, ținând cont de cerințele și interfețele asociate cu prezentele procedee comune de funcționare.

— Se utilizează un instrument de gestionare a serviciilor IT (ITSM) în vederea furnizării de asistență în ceea ce privește procedeele comune de funcționare, în special gestionarea incidentelor, gestionarea problemelor și soluționarea cererilor, precum și comunicarea între cele două părți.

— În plus, este permis schimbul de informații prin e-mail.

— Ambele părți se asigură că sunt respectate cerințele privind securitatea informațiilor, în conformitate cu Instrucțiunile de gestionare.

4. GESTIONAREA INCIDENTELOR

Obiectivul procesului de gestionare a incidentelor este de a readuce serviciile IT la un nivel normal cât mai repede posibil și cu o perturbare minimă a activității în urma producerii unui incident.

În cadrul procesului de gestionare a incidentelor ar trebui, de asemenea, să se țină o evidență a incidentelor în scopul raportării, care să fie integrată în alte procese pentru favorizarea unei îmbunătățiri continue.

În general, procesul de gestionare a incidentelor cuprinde următoarele activități:

— identificarea și înregistrarea incidentelor;

— clasificarea și asistența inițială;

— investigarea și diagnosticarea;

— rezolvarea și restabilirea sistemului;

— închiderea incidentului.

Pe parcursul ciclului de viață al unui incident, procesul de gestionare a incidentelor este responsabil pentru gestionarea permanentă a drepturilor de proprietate, pentru monitorizare, urmărire și comunicare.

4.1. Identificarea și înregistrarea incidentelor

Un incident poate fi identificat de un grup de asistență, prin intermediul unor instrumente de monitorizare automatizate sau de către personalul tehnic care asigură supravegherea de rutină.

Odată identificat, un incident trebuie înregistrat, fiindu-i atribuit un identificator unic care permite urmărirea și monitorizarea corespunzătoare a acestuia. Identificatorul unic al unui incident este identificatorul atribuit în sistemul comun de tichete de către serviciul de asistență al părții (fie UE, fie CH) care a semnalat incidentul și trebuie utilizat în toate comunicările referitoare la respectivul incident.

Pentru toate incidentele, punctul de contact ar trebui să fie serviciul de asistență al părții care a introdus tichetul.

4.2. Clasificarea și asistența inițială

Clasificarea incidentelor are ca scop înțelegerea și identificarea sistemului și/sau a serviciului afectat de un incident și a măsurii în care este afectat acesta. Pentru a fi eficientă, clasificarea ar trebui să direcționeze de prima dată soluționarea incidentului către resursa corectă, pentru a accelera rezolvarea acestuia.

Faza de clasificare ar trebui să includă clasificarea și ierarhizarea incidentului în funcție de impactul și de nivelul de urgență al acestuia, pentru a fi tratat în intervalul de timp stabilit în funcție de priorități.

Dacă incidentul are un potențial impact asupra confidențialității sau integrității datelor sensibile și/sau are un impact asupra disponibilității sistemului, este, de asemenea, declarat drept incident de securitate și, ulterior, va fi gestionat conform procesului definit în capitolul „Gestionarea incidentelor de securitate” din prezentul document.

Dacă este posibil, serviciul de asistență care a introdus tichetul efectuează o diagnosticare inițială. În acest scop, serviciul de asistență va analiza dacă incidentul reprezintă o eroare cunoscută. În caz afirmativ, calea de rezolvare sau soluția alternativă este deja cunoscută și documentată.

Dacă serviciul de asistență reușește să rezolve incidentul, atunci va închide efectiv incidentul în această fază, întrucât scopul principal al procesului de gestionare a incidentelor a fost atins (și anume restaurarea rapidă a serviciului pentru utilizatorul final). În caz contrar, serviciul de asistență va transmite incidentul grupului de rezolvare corespunzător pentru o investigare și o diagnosticare suplimentare.

4.3. Investigarea și diagnosticarea

Procesul de investigare și diagnosticare a incidentelor se aplică atunci când un incident nu poate fi rezolvat de către serviciul de asistență în cadrul diagnosticării inițiale și, prin urmare, este transmis în mod corespunzător. Transmiterea incidentelor constituie o parte integrantă din procesul de investigare și diagnosticare.

O practică comună în faza de investigare și diagnosticare este încercarea de a recrea incidentul în condiții controlate. Atunci când se efectuează investigarea și diagnosticarea incidentului, este important să se înțeleagă ordinea corectă a evenimentelor care au cauzat incidentul.

Transmiterea reprezintă recunoașterea faptului că un incident nu poate fi rezolvat la nivelul curent de asistență și trebuie transmis unui grup de asistență de nivel superior sau celeilalte părți. Transmiterea poate urma două căi: orizontală (funcțională) sau verticală (ierarhică).

Serviciul de asistență care a înregistrat și a declanșat incidentul este responsabil pentru transmiterea acestuia către resursa corespunzătoare și pentru urmărirea stadiului general și atribuirea incidentului.

Partea căreia i s-a atribuit incidentul este responsabilă pentru asigurarea efectuării în timp util a acțiunilor solicitate și pentru furnizarea de feedbackuri propriului serviciu de asistență.

4.4. Rezolvarea și restabilirea sistemului

Rezolvarea incidentului și restabilirea sistemului se efectuează după înțelegerea în totalitate a acestuia. Găsirea unei soluții de rezolvare a unui incident înseamnă că a fost identificată o modalitate de a remedia problema. Aplicarea soluției de rezolvare reprezintă faza de restabilire a sistemului.

După remedierea întreruperii serviciului de către resursele corespunzătoare, incidentul este redirecționat către serviciul de asistență competent care a înregistrat incidentul și serviciul respectiv confirmă, împreună cu inițiatorul incidentului, că eroarea a fost remediată și că incidentul poate fi închis. Elementele identificate în timpul procesării incidentului trebuie înregistrate pentru a fi utilizate ulterior.

Restabilirea sistemului poate fi efectuată de către personalul de asistență IT sau prin punerea la dispoziția utilizatorului final a unui set de instrucțiuni care trebuie urmate.

4.5. Închiderea incidentului

Închiderea este ultima etapă a procesului de gestionare a incidentelor și se efectuează la scurt timp după rezolvarea acestora.

Printre activitățile din lista de verificare care trebuie desfășurate în faza de închidere, se evidențiază următoarele:

— verificarea clasificării inițiale care a fost atribuită incidentului;

— colectarea corespunzătoare a tuturor informațiilor referitoare la incident;

— documentarea corespunzătoare a incidentului și actualizarea bazei de informații;

— informarea corespunzătoare a fiecărei părți interesate afectate în mod direct sau indirect de incident.

Un incident este închis în mod oficial după executarea fazei de închidere a incidentului de către serviciul de asistență și după informarea în acest sens a celeilalte părți.

Odată închis un incident, acesta nu mai este redeschis. Dacă un incident reapare într-un interval scurt de timp, incidentul inițial nu este redeschis, ci trebuie înregistrat un nou incident.

Dacă incidentul este urmărit atât de serviciul de asistență al UE, cât și de cel al CH, responsabilitatea închiderii finale a acestuia îi revine serviciului de asistență care a introdus tichetul.

5. GESTIONAREA PROBLEMELOR

Această procedură ar trebui urmată ori de câte ori este identificată o problemă și se declanșează procesul de gestionare a problemelor. Procesul de gestionare a problemelor se axează pe îmbunătățirea calității și pe reducerea volumului de incidente semnalate. O problemă poate fi cauza unuia sau a mai multor incidente. Atunci când este raportat un incident, obiectivul procesului de gestionare a incidentelor este de a restabili serviciul cât mai repede posibil, ceea ce poate implica soluții alternative. Atunci când se creează o problemă, obiectivul este de a investiga cauza principală a problemei pentru a identifica o modificare care să garanteze faptul că problema și incidentele conexe nu vor mai apărea.

5.1. Identificarea și înregistrarea problemelor

În funcție de partea care a introdus tichetul, fie serviciul de asistență al UE, fie cel al CH va fi punctul de contact pentru aspectele legate de problema în cauză.

Identificatorul unic al unei probleme reprezintă identificatorul atribuit de echipa de gestionare a serviciilor IT (ITSM). Acesta trebuie utilizat în toate comunicările referitoare la respectiva problemă.

O problemă poate fi declanșată de un incident sau poate fi deschisă din proprie inițiativă pentru a remedia problemele descoperite în cadrul sistemului în orice moment.

5.2. Ierarhizarea problemelor

Problemele pot fi clasificate în funcție de gravitatea și prioritatea acestora, în același mod ca incidentele, pentru a facilita urmărirea lor, luând în considerare impactul incidentelor asociate și frecvența de apariție a acestora.

5.3. Investigarea și diagnosticarea problemelor

Fiecare parte poate semnala o problemă, iar serviciul de asistență al părții inițiatoare va fi responsabil pentru înregistrarea problemei, pentru atribuirea acesteia resursei corespunzătoare și pentru monitorizarea stadiului general al problemei.

Grupul de rezolvare căruia i-a fost transmisă problema este responsabil pentru gestionarea în timp util a acesteia și pentru comunicarea cu serviciul de asistență.

La cerere, ambele părți sunt responsabile pentru asigurarea executării acțiunilor atribuite și pentru transmiterea de feedbackuri propriului serviciu de asistență.

5.4. Rezoluția

Grupul de rezolvare căruia i se atribuie problema este responsabil pentru soluționarea acesteia și pentru furnizarea de informații relevante propriului serviciu de asistență.

Elementele identificate în timpul procesării problemei trebuie înregistrate pentru a fi utilizate ulterior.

5.5. Închiderea problemei

O problemă este închisă oficial după soluționarea sa prin implementarea modificării. Faza de închidere a problemei va fi executată de serviciul de asistență care a semnalat problema și a informat în acest sens serviciul de asistență al celeilalte părți.

6. SOLUȚIONAREA CERERILOR

Procesul de soluționare a cererilor reprezintă gestionarea integrală a unei cereri vizând un serviciu nou sau existent din momentul înregistrării și aprobării acesteia și până la închiderea sa. Cererile de servicii sunt de obicei solicitări minore, predefinite, repetabile, frecvente, aprobate în prealabil și procedurale.

Principalele etape care trebuie parcurse sunt enumerate mai jos.

6.1. Inițierea cererii

Informațiile cu privire la o cerere de servicii sunt transmise către serviciul de asistență al UE sau al CH prin e-mail, telefon sau prin instrumentul de gestionare a serviciilor IT (ITSM) sau prin orice alt canal de comunicare convenit.

6.2. Înregistrarea și analiza cererilor

Pentru toate cererile de servicii, punctul de contact ar trebui să fie serviciul de asistență al UE sau al CH, în funcție de partea care a transmis cererea de servicii. Respectivul serviciu de asistență va fi responsabil pentru înregistrarea și analizarea cererii de servicii cu diligența corespunzătoare.

6.3. Aprobarea cererilor

Agentul din cadrul serviciului de asistență al părții care a transmis cererea de servicii verifică dacă sunt necesare aprobări din partea celeilalte părți și, dacă este cazul, face demersurile necesare pentru obținerea acestora. Dacă cererea de servicii nu este aprobată, serviciul de asistență actualizează și închide tichetul.

6.4. Soluționarea cererilor

Această etapă se referă la gestionarea efectivă și eficientă a cererilor de servicii. Trebuie să se facă distincție între următoarele cazuri:

— soluționarea cererii de servicii afectează doar una dintre părți. În acest caz, respectiva parte emite ordinele de lucru și coordonează executarea acestora;

— soluționarea cererii de servicii afectează atât UE, cât și CH. În acest caz, serviciile de asistență emit ordine de lucru în sfera lor de responsabilitate. Derularea procesului de soluționare cererii de servicii este coordonată de ambele servicii de asistență. Responsabilitatea generală îi revine serviciului de asistență care a primit și a inițiat cererea de servicii.

Când cererea de servicii a fost soluționată, stadiul acesteia trebuie modificat în „Rezolvată”.

6.5. Transmiterea cererilor

Serviciul de asistență poate transmite cererea de servicii nesoluționată către resursa corespunzătoare (o terță parte), dacă este necesar.

Transmiterile sunt efectuate către părțile terțe corespunzătoare, și anume serviciul de asistență al UE va trebui să apeleze la serviciul de asistență al CH pentru transmiterea către o terță parte a CH și viceversa.

Terța parte către care a fost transmisă cererea de servicii este responsabilă pentru gestionarea în timp util a cererii de servicii și pentru comunicarea cu serviciul de asistență care a transmis cererea de servicii.

Serviciul de asistență care a înregistrat cererea de servicii este responsabil pentru monitorizarea stadiului general și atribuirea unei cereri de servicii.

6.6. Verificarea procesului de soluționare a cererii

Serviciul de asistență responsabil supune evidențele privind cererea de servicii unui control al calității final înainte de închiderea cererii. Scopul este de a se asigura că cererea de servicii este efectiv prelucrată și că toate informațiile necesare pentru descrierea ciclului de viață al cererii sunt suficient de detaliate. În plus, elementele identificate în timpul prelucrării cererii trebuie înregistrate pentru a fi utilizate ulterior.

6.7. Închiderea cererii

Dacă părțile desemnate sunt de acord cu faptul că cererea de servicii a fost soluționată și solicitantul consideră cazul rezolvat, stadiul cererii devine „Închisă”.

O cerere de servicii este oficial închisă după ce serviciul de asistență care a înregistrat cererea de servicii a executat faza de închidere a acesteia și a informat în acest sens serviciul de asistență al celeilalte părți.

7. GESTIONAREA MODIFICĂRILOR

Obiectivul acestui proces de a asigura faptul că sunt utilizate metode și proceduri standardizate pentru o gestionare eficientă și promptă a tuturor modificărilor legate de controlul infrastructurii IT, în scopul reducerii la minimum a numărului și a impactului oricăror incidente conexe asupra serviciului. Modificări ale infrastructurii IT pot apărea reactiv ca răspuns la probleme sau cerințe impuse din exterior, de exemplu, modificări legislative, sau proactiv, rezultate din încercarea de a îmbunătăți eficiența și eficacitatea ori pentru a permite sau a reflecta inițiative antreprenoriale.

Procesul de gestionare a modificărilor include diferite etape care surprind fiecare detaliu cu privire la o cerere de modificare în vederea monitorizării ulterioare. Aceste procese asigură faptul că modificarea este validată și testată înainte de a fi implementată. Procesul de gestionare a versiunilor este responsabil pentru implementarea cu succes a acestora.

7.1. Cererea de modificare

O cerere de modificare (RFC) este prezentată echipei de gestionare a modificărilor, pentru validare și aprobare. Pentru toate cererile de modificare, punctul de contact ar trebui să fie serviciul de asistență al UE sau al CH, în funcție de partea care a transmis cererea. Respectivul serviciu de asistență va fi responsabil pentru înregistrarea și analizarea cererii cu diligența corespunzătoare.

Cererile de modificare pot fi determinate de:

— un incident care a cauzat o modificare;

— o problemă existentă care are ca rezultat o modificare;

— un utilizator final care solicită o nouă modificare;

— o modificare ca urmare a întreținerii continue;

— o modificare legislativă.

7.2. Evaluarea și planificarea modificărilor

Această etapă implică activitățile de evaluare și de planificare a modificărilor. Aceasta include activități de ierarhizare și de planificare pentru a reduce la minimum riscul și impactul.

Dacă implementarea cererii de modificare afectează atât UE, cât și CH, partea care a înregistrat cererea de modificare verifică împreună cu cealaltă parte procesul de evaluare și de planificare a modificărilor.

7.3. Aprobările modificărilor

Orice cerere de modificare înregistrată trebuie să fie aprobată de nivelul de transmitere competent.

7.4. Implementarea modificărilor

Implementarea modificărilor este operată în cadrul procesului de gestionare a versiunilor. Echipele de gestionare a versiunilor ale ambelor părți urmează propriile procese care implică planificarea și testarea. Revizuirea modificărilor se efectuează după ce modificarea a fost implementată. Pentru a asigura aplicarea modificărilor conform planului, procesul de gestionare a modificărilor este revizuit și actualizat în mod constant, dacă este necesar.

8. GESTIONAREA VERSIUNILOR

O versiune reprezintă una sau mai multe modificări ale unui serviciu IT, incluse într-un plan de lansare a versiunii, care vor trebui autorizate, pregătite, concepute, testate și implementate în același timp. O versiune poate reprezenta remedierea unor erori, o modificare a hardware-ului sau a altor componente, modificări ale software-ului, actualizări ale versiunilor de aplicații, modificări ale documentației și/sau ale unor procese. Conținutul fiecărei versiuni este gestionat, testat și implementat ca un tot unitar.

Procesul de gestionare a versiunilor vizează planificarea, conceperea, testarea și validarea, precum și asigurarea capacității de furnizare a serviciilor concepute, care să răspundă cerințelor părților interesate și să îndeplinească obiectivele propuse. Criteriile de acceptare pentru toate modificările aduse serviciului vor fi definite și documentate pe parcursul etapei de coordonare a procesului de concepere și vor fi furnizate echipelor de gestionare a versiunilor.

Versiunea va consta, în mod obișnuit, dintr-o serie de soluționări de probleme și de îmbunătățiri aduse unui serviciu. Aceasta conține software-ul nou sau modificat necesar și orice hardware nou sau modificat necesar pentru implementarea modificărilor aprobate.

8.1. Planificarea versiunii

Prima etapă a procesului include alocarea modificărilor autorizate pachetelor de versiuni și definirea domeniului de aplicare și a conținutului versiunilor. Pe baza acestor informații, în cadrul subprocesului de planificare a versiunilor se elaborează un calendar pentru conceperea, testarea și implementarea versiunii.

În cadrul planificării ar trebui definite următoarele:

— domeniul de aplicare și conținutul versiunii;

— evaluarea riscurilor și profilul de risc al versiunii;

— clienții/utilizatorii afectați de versiune;

— echipa responsabilă pentru versiune;

— strategia de livrare și de implementare;

— resursele alocate pentru versiune și pentru implementarea acesteia.

Ambele părți se informează reciproc cu privire la perioadele de planificare și de întreținere a versiunii. Dacă o versiune afectează atât UE, cât și CH, acestea coordonează etapa de planificare și definesc o perioadă comună pentru întreținere.

8.2. Conceperea și testarea pachetului de versiuni

Etapa de concepere și de testare a procesului de gestionare a versiunilor stabilește abordarea privind executarea versiunii sau a pachetului de versiuni și menținerea mediilor controlate înainte de modificarea producției, precum și testarea tuturor modificărilor din toate mediile lansate.

Dacă o versiune afectează atât UE, cât și CH, acestea coordonează planurile de livrare și testele. Acestea includ următoarele aspecte:

— cum și când vor fi livrate versiunile și componentele serviciilor;

— care sunt timpii de livrare obișnuiți; ce se întâmplă în cazul unei întârzieri;

— modul de monitorizare a progresului livrării și de obținere a confirmării;

— indicatori pentru monitorizarea și stabilirea gradului de reușită a efortului de implementare a versiunii;

— cazurile comune de testare a funcționalităților și a modificărilor relevante.

La finalul acestui subproces, toate componentele necesare ale versiunii sunt pregătite pentru faza de implementare concretă.

8.3. Pregătirea implementării

Subprocesul de pregătire asigură faptul că planurile de comunicare sunt corect definite, că notificările pot fi trimise tuturor părților interesate și utilizatorilor finali afectați și că versiunea este integrată în procesul de gestionare a modificărilor pentru a asigura faptul că toate modificările sunt efectuate într-un mod controlat și sunt aprobate de forurile competente.

Dacă o versiune afectează atât UE, cât și CH, acestea coordonează următoarele activități:

— înregistrarea cererii de modificare pentru programarea și pregătirea implementării în mediul de producție;

— crearea unui plan de implementare;

— abordarea revenirii la starea anterioară, astfel încât, în cazul unei probleme legate de implementare, să se poată reveni la starea anterioară;

— transmiterea de notificări tuturor părților relevante;

— solicitarea aprobării pentru implementarea versiunii de la nivelul de transmitere relevant.

8.4. Readucerea versiunii la starea anterioară

În cazul unei implementări nereușite sau în cazul în care, pe parcursul testării, s-a constatat că implementarea a fost nereușită sau nu a îndeplinit criteriile de acceptare/calitate convenite, echipele de gestionare a versiunii ale ambelor părți vor trebui să readucă versiunea la starea anterioară. Toate părțile interesate relevante vor trebui informate, inclusiv utilizatorii finali afectați/vizați. În așteptarea aprobării, procesul poate reporni în oricare dintre etapele anterioare.

8.5. Evaluarea și finalizarea versiunii

În evaluarea implementării unei versiuni ar trebui incluse următoarele activități:

— înregistrarea feedbackurilor privind gradul de satisfacție a clienților, a utilizatorilor și legat de prestarea serviciilor în ceea ce privește implementarea versiunii (colectarea feedbackurilor și luarea în considerare a acestora pentru îmbunătățirea continuă a serviciului);

— analizarea tuturor criteriilor de calitate care nu au fost îndeplinite;

— verificarea că toate acțiunile, corecțiile și modificările necesare au fost duse la bun sfârșit;

— asigurarea faptului că, la finalul implementării, nu există probleme legate de capabilități, resurse, capacitate sau performanță;

— verificarea că orice problemă, eroare și soluție alternativă cunoscută este documentată și acceptată de către client, utilizatorii finali, echipa de asistență operațională și de către alte părți afectate;

— monitorizarea incidentelor și a problemelor cauzate de implementare (asigurarea din timp a asistenței necesare echipelor operaționale în cazul în care versiunea a generat o creștere a volumului de lucru);

— actualizarea documentației de asistență (și anume, a documentelor cu informații tehnice);

— încredințarea în mod oficial a implementării versiunii echipelor operaționale din cadrul serviciilor;

— documentarea lecțiilor învățate;

— preluarea documentului de sinteză privind versiunea de la echipele de punere în aplicare;

— închiderea oficială a implementării versiunii după verificarea înregistrării cererii de modificare.

9. GESTIONAREA INCIDENTELOR DE SECURITATE

Gestionarea incidentelor de securitate este un proces de gestionare a incidentelor de securitate pentru a permite comunicarea incidentelor părților interesate potențial afectate, evaluarea și ierarhizarea incidentelor și răspunsul la incidente în vederea soluționării oricărei încălcări reale, suspectate sau potențiale a confidențialității, a disponibilității sau a integrității activelor informaționale sensibile.

9.1. Clasificarea incidentelor de securitate a informațiilor

Toate incidentele care afectează legătura dintre registrul Uniunii și registrul elvețian sunt analizate pentru a stabili o posibilă încălcare a confidențialității, a integrității sau a disponibilității oricărei informații sensibile înregistrate în Evidența informațiilor sensibile (SIL).

În acest caz, incidentul este caracterizat ca incident de securitate a informațiilor, este înregistrat imediat în instrumentul de gestionare a serviciilor IT (ITSM) și gestionat ca atare.

9.2. Gestionarea incidentelor de securitate a informațiilor

Incidentele de securitate se află în responsabilitatea celui de al treilea nivel de transmitere, iar de rezolvarea acestora se va ocupa o echipă specială de gestionare a incidentelor (IMT).

IMT este responsabilă cu:

— efectuarea unei analize inițiale, clasificarea și evaluarea gradului de gravitate a incidentului;

— coordonarea acțiunilor între toate părțile interesate, inclusiv documentarea completă a analizei incidentului, a deciziilor luate pentru a rezolva incidentul și a eventualelor puncte slabe identificate;

— în funcție de gravitatea incidentului de securitate, transmiterea incidentului în timp util către nivelul corespunzător spre informare și/sau pentru luarea unei decizii.

În cadrul procesului de management al securității informațiilor, toate informațiile referitoare la incidente sunt clasificate la cel mai înalt nivel de sensibilitate a informațiilor, dar în orice caz nu la un nivel mai mic decât nivelul SENSITIVE: *ETS*.

În cazul unei investigări în curs și/sau al unui punct slab care ar putea fi exploatat și până la remedierea acestuia, informațiile sunt clasificate drept SPECIAL HANDLING: *ETS Critical*.

9.3. Identificarea incidentelor de securitate

În funcție de tipul de eveniment de securitate, responsabilul cu securitatea informațiilor stabilește organizațiile competente care trebuie implicate și care vor face parte din echipa de gestionare a incidentelor.

9.4. Analiza incidentelor de securitate

IMT asigură legătura cu toate organizațiile implicate și, după caz, cu membrii relevanți ai echipelor acestora în vederea analizării incidentului. În cadrul analizei, se identifică amploarea pierderii confidențialității, integrității sau disponibilității unui activ și se evaluează consecințele pentru toate organizațiile afectate. În continuare, sunt definite măsurile inițiale și subsecvente pentru rezolvarea incidentului și gestionarea impactului acestuia, inclusiv a impactului acestor măsuri asupra resurselor.

9.5. Evaluarea gravității incidentelor de securitate, transmiterea și raportarea acestora

IMT evaluează gravitatea fiecărui incident de securitate nou după încadrarea acestuia ca incident de securitate și ia imediat măsurile necesare în funcție de gravitatea acestuia.

9.6. Raportarea răspunsurilor la incidentele de securitate

IMT include în raportul de răspuns la incidentele de securitate a informațiilor rezultatele privind izolarea incidentului și restabilirea sistemului. Raportul este transmis până la nivelul al treilea de transmitere prin intermediul unui e-mail securizat sau prin intermediul altor mijloace de comunicare securizate, acceptate de ambele părți.

Partea responsabilă analizează rezultatele privind izolarea incidentului și restabilirea sistemului și:

— reconectează registrul în cazul deconectării prealabile;

— transmite echipelor registrelor informări cu privire la incident;

— închide incidentul.

În raportul privind incidentele de securitate a informațiilor, IMT ar trebui să includă – într-o manieră securizată – detalii relevante pentru a asigura înregistrarea coerentă și comunicarea și pentru a permite luarea unor măsuri prompte și adecvate pentru izolarea incidentului. După finalizarea acestuia, IMT transmite în timp util raportul final privind incidentul de securitate a informațiilor.

9.7. Monitorizarea, consolidarea capacităților și îmbunătățirea continuă

IMT va furniza rapoarte pentru toate incidentele de securitate până la nivelul al treilea de transmitere. Rapoartele vor fi utilizate la acest nivel de transmitere pentru a stabili următoarele:

— punctele slabe în ceea ce privește controalele de securitate și/sau operațiunile care trebuie consolidate;

— eventuala necesitate de ameliorare a acestei proceduri în vederea îmbunătățirii eficacității răspunsului la incidente;

— oportunitățile de formare și de consolidare a capacităților pentru a îmbunătăți mai mult reziliența sistemelor registrelor în ceea ce privește securitatea informațiilor, pentru a reduce riscul unor incidente viitoare și pentru a reduce la minimum impactul acestora.

10. MANAGEMENTUL SECURITĂȚII INFORMAȚIILOR

Managementul securității informațiilor vizează asigurarea confidențialității, a integrității și a disponibilității informațiilor și datelor clasificate, precum și a serviciilor IT ale unei organizații. Pe lângă componentele tehnice, inclusiv conceperea și testarea acestora (a se vedea LTS), sunt necesare următoarele procedee comune de funcționare în vederea îndeplinirii cerințelor de securitate pentru legătura permanentă între registre.

10.1. Identificarea informațiilor sensibile

Nivelul de sensibilitate al unei informații este evaluat prin stabilirea nivelului impactului asupra activității (de exemplu, pierderi financiare, afectarea imaginii, încălcări ale legii etc.) pe care l-ar putea avea o încălcare a securității respectivelor informații.

Activele informaționale sensibile sunt identificate pe baza impactului lor asupra legăturii.

Nivelul de sensibilitate al acestor informații este evaluat în funcție de scala de sensibilitate aplicabilă pentru această legătură și este prezentat în detaliu în secțiunea „Gestionarea incidentelor de securitate a informațiilor” din prezentul document.

10.2. Nivelurile de sensibilitate ale activelor informaționale

După identificarea sa, activul informațional este clasificat aplicând următoarele reguli:

— identificarea cel puțin a unui nivel RIDICAT de confidențialitate, integritate sau disponibilitate clasifică activul drept SPECIAL HANDLING: *ETS Critical*;

— identificarea cel puțin a unui nivel MEDIU de confidențialitate, integritate sau disponibilitate clasifică activul drept SENSITIVE: *ETS*;

— identificarea cel puțin a unui nivel REDUS de confidențialitate, integritate sau disponibilitate clasifică activul drept Marcajul EU: SENSITIVE: *ETS Joint Procurement;* Marcajul CH: LIMITED: *ETS*.

10.3. Desemnarea proprietarului activelor informaționale

Toate activele informaționale ar trebui să aibă un proprietar desemnat. Activele informaționale ale ETS, care aparțin legăturii dintre EUTL și SSTL sau se referă la aceasta ar trebui incluse într-o listă comună de inventariere a activelor, menținută de ambele părți. Activele informaționale ale ETS din afara legăturii dintre EUTL și SSTL ar trebui incluse într-o listă de inventariere a activelor, menținută de partea corespunzătoare.

Dreptul de proprietate asupra fiecărui activ informațional care aparține legăturii dintre EUTL și SSTL sau se referă la aceasta va fi convenit de către părți. Proprietarul unui activ informațional este responsabil pentru evaluarea nivelului de sensibilitate al acestuia.

Proprietarul ar trebui să aibă un nivel de responsabilitate corespunzător valorii activului (activelor) atribuit(e). Responsabilitatea proprietarului în ceea ce privește activul (activele), precum și obligația acestuia de a menține nivelul de confidențialitate, integritate și disponibilitate necesare ar trebui să fie convenite și oficializate.

10.4. Înregistrarea informațiilor sensibile

Toate informațiile sensibile sunt înregistrate în Evidența informațiilor sensibile (SIL).

Dacă este cazul, agregarea unor informații sensibile care ar putea avea un impact mai mare decât impactul unei singure informații trebuie luată în considerare și înregistrată în SIL (de exemplu, un set de informații stocate în baza de date a sistemului).

SIL nu este statică. Amenințările, vulnerabilitățile, probabilitatea sau consecințele incidentelor de securitate legate de active se pot schimba fără nicio indicație și pot fi introduse active noi în operarea sistemele registrelor.

Prin urmare, SIL trebuie revizuită periodic și toate informațiile noi considerate ca fiind sensibile trebuie înregistrate imediat în SIL.

SIL conține cel puțin următoarele informații pentru fiecare înregistrare:

— descrierea informațiilor;

— proprietarul informațiilor;

— nivelul de sensibilitate;

— o mențiune care să indice dacă informațiile includ date cu caracter personal;

— informații suplimentare, dacă este cazul.

10.5. Gestionarea informațiilor sensibile

Atunci când sunt prelucrate în afara legăturii dintre registrul Uniunii și registrul elvețian, informațiile sensibile sunt gestionate în conformitate cu Instrucțiunile de gestionare.

Informațiile sensibile prelucrate prin intermediul legăturii dintre registrul Uniunii și registrul elvețian sunt gestionate de către părți în conformitate cu cerințele în materie de securitate.

10.6. Gestionarea accesului

Obiectivul procesului de management al accesului este de a acorda utilizatorilor autorizați dreptul de a utiliza un serviciu, împiedicând în același timp accesul utilizatorilor neautorizați. Managementul accesului este uneori denumit și „managementul drepturilor” sau „managementul identității”.

Pentru legătura permanentă între registre și funcționarea acesteia, ambele părți au nevoie de acces la următoarele componente:

— Wiki: un mediu de colaborare pentru schimbul de informații comune, cum ar fi planificarea versiunilor;

— instrumentul de gestionare a serviciilor IT (ITSM) pentru gestionarea incidentelor și a problemelor (a se vedea capitolul 3 „Abordare și standarde”);

— sistemul de schimb de mesaje: fiecare parte pune la dispoziție un sistem securizat de transfer de mesaje pentru transmiterea mesajelor care conțin date privind tranzacțiile.

Administratorul registrului elvețian și administratorul central al Uniunii se asigură că accesurile sunt actualizate și funcționează ca puncte de contact pentru părțile lor în cadrul activităților de management al accesului. Cererile de acces sunt gestionate conform procedurilor de soluționare a cererilor.

10.7. Gestionarea certificatelor/cheilor

Fiecare parte răspunde de gestionarea propriilor certificate/chei (generare, înregistrare, stocare, instalare, utilizare, reînnoire, revocare, realizarea de copii de rezervă și recuperarea certificatelor/cheilor). Conform standardelor tehnice de creare a legăturii (LTS), se utilizează numai certificate digitale emise de o autoritate de certificare (CA) acceptată de ambele părți. Gestionarea și stocarea certificatelor/cheilor trebuie să respecte dispozițiile din Instrucțiunile de gestionare.

Orice revocare și/sau reînnoire a certificatelor și a cheilor este coordonată de ambele părți. Aceasta se realizează conform procedurilor de soluționare a cererilor.

Administratorul registrului elvețian și administratorul central al Uniunii vor face schimb de certificate/chei prin mijloace de comunicare securizate în conformitate cu dispozițiile din Instrucțiunile de gestionare.

Orice verificare a certificatelor/cheilor prin orice mijloc între părți se va realiza în afara benzii.

ANEXA III

STANDARDE TEHNICE DE CREARE A LEGĂTURII (LTS) ÎN TEMEIUL ARTICOLULUI 3 ALINEATUL (7) DIN ACORDUL DINTRE UNIUNEA EUROPEANĂ ȘI CONFEDERAȚIA ELVEȚIANĂ PENTRU CREAREA UNEI LEGĂTURI ÎNTRE RESPECTIVELE LOR SCHEME DE COMERCIALIZARE A CERTIFICATELOR DE EMISII DE GAZE CU EFECT DE SERĂ

Standarde pentru legătura permanentă între registre

Cuprins

1. GLOSAR . . . 23
2. INTRODUCERE . . . 25
2.1. Domeniul de aplicare . . . 25
2.2. Destinatari . . . 25
3. DISPOZIȚII GENERALE . . . 25
3.1. Arhitectura legăturii de comunicare . . . 25
3.1.1. Schimbul de mesaje . . . 26
3.1.2. Mesaj XML – Descriere de nivel înalt . . . 26
3.1.3. Ferestre de ingerare (Ingestion Windows) . . . 26
3.1.4. Fluxurile de mesaje privind tranzacțiile . . . 27
3.2. Securitatea transferurilor de date . . . 29
3.2.1. Firewall și interconectarea între rețele . . . 29
3.2.2. Rețea virtuală privată (VPN) . . . 29
3.2.3. Implementarea IPSec . . . 29
3.2.4. Protocol de transfer securizat pentru schimburile de mesaje . . . 30
3.2.5. Criptare și semnătură bazate pe XML . . . 30
3.2.6. Chei criptografice . . . 30
3.3. Lista funcțiilor în cadrul legăturii . . . 30
3.3.1. Tranzacțiile comerciale . . . 30
3.3.2. Protocolul reconcilierilor . . . 31
3.3.3. Mesaj test . . . 31
3.4. Cerințe privind înregistrarea datelor . . . 31
3.5. Cerințele operaționale . . . 32
4. DISPOZIȚII PRIVIND DISPONIBILITATEA . . . 32
4.1. Proiectarea disponibilității comunicațiilor . . . 32
4.2. Planul de inițializare, comunicare, reactivare și testare . . . 33
4.2.1. Testele interne pentru infrastructura TIC . . . 33
4.2.2. Testele de comunicare . . . 33
4.2.3. Teste pentru întregul sistem (de la un capăt la celălalt capăt) . . . 33
4.2.4. Testele de securitate . . . 33
4.3. Mediile de acceptare/de testare . . . 34
5. DISPOZIȚII PRIVIND CONFIDENȚIALITATEA ȘI INTEGRITATEA . . . 34
5.1. Infrastructura de testare a securității . . . 34
5.2. Dispoziții privind suspendarea și reactivarea legăturii . . . 35

5.3. Dispoziții privind încălcarea securității 35
5.4. Orientări privind testarea securității 35
5.4.1. Software 35
5.4.2. Infrastructură 36
5.5. Dispoziții privind evaluarea riscurilor 36

1. GLOSAR

Tabelul 1-1 Acronime și definiții comerciale

Acronim/termen	Definiție
Certificat	Dreptul de a emite o tonă de dioxid de carbon echivalent pe parcursul unei perioade specificate, care va fi valabil exclusiv în scopul respectării cerințelor ETS ale fiecărei entități.
CH	Confederația Elvețiană.
CHU	Tipul de certificat pentru instalația staționară, denumit și CHU2 (cu referire la perioada de angajament 2 din Protocolul de la Kyoto), emis de Confederația Elvețiană.
CHUA	Certificat elvețian pentru aviație.
COP	Procedee comune de funcționare. Procedee elaborate în comun pentru operaționalizarea legăturii dintre EU ETS și ETS-ul Elveției.
ETR	Registru de comercializare a certificatelor de emisii.
ETS	Schema de comercializare a certificatelor de emisii.
UE	Uniunea Europeană.
EUA	Certificat general al UE.
EUAA	Certificat pentru aviație al UE.
EUCR	Registrul consolidat al Uniunii Europene.
EUTL	Registrul de tranzacții al Uniunii Europene.
Registrul	Un sistem de contabilizare a certificatelor emise în cadrul ETS, care ține evidența drepturilor de proprietate asupra certificatelor deținute în conturile electronice.
SSTL	Registrul suplimentar de tranzacții al Elveției.
Operațiune	Un proces în cadrul unui registru care include transferul unui certificat dintr-un cont în alt cont.
Sistem al unui registru de tranzacții	Registrul de tranzacții include o evidență a fiecărei tranzacții propuse trimise de la un registru la celălalt.

Tabelul 1-2 Acronime și definiții tehnice

Acronim	Definiție
Criptografie asimetrică	Utilizează chei publice și private pentru criptarea și decriptarea datelor.
Autoritate de certificare (CA)	Entitate care emite certificate digitale
Cheie criptografică	O informație care determină rezultatul funcțional al unui algoritm criptografic.
Decriptare	Proces opus criptării.
Semnătură digitală	O tehnică matematică utilizată pentru validarea autenticității și integrității unui mesaj, software sau document digital.
Criptare	Procesul de conversie a informațiilor sau a datelor într-un cod, în special pentru a împiedica accesul neautorizat.
Ingerare de fișiere	Procesul de citire a unui fișier.
Firewall	Aparat sau software de securitate în rețea care monitorizează și controlează traficul de rețea de intrare și de ieșire pe baza unor reguli prestabilite.
Monitorizarea ritmicității (heartbeat)	Semnal periodic generat și monitorizat de hardware sau software pentru a indica funcționarea normală sau pentru a sincroniza alte componente ale unui sistem informatic.
IPSec	IP SECurity. Suită de protocoale de rețea care autentifică și criptează pachetele de date pentru a asigura o comunicare criptată securizată între două computere printr-o rețea de protocoale internet.
Test de rezistență la intruziuni	Practică de testare a unui sistem informatic, a unei rețele sau a unei aplicații web pentru a descoperi vulnerabilități de securitate pe care un atacator le-ar putea exploata.
Proces de reconciliere	Proces de asigurare a faptului că două seturi de înregistrări concordă.
VPN	Rețea virtuală privată.
XML	Limbaj de marcare extensibil. Permite proiectanților să își creeze propriile etichete personalizate, care să permită definirea, transmiterea, validarea și interpretarea datelor între aplicații și între organizații.

2. INTRODUCERE

Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 23 noiembrie 2017 (denumit în continuare „acordul”) prevede recunoașterea reciprocă a certificatelor de emisii care pot fi utilizate pentru asigurarea conformității în cadrul sistemului de comercializare a certificatelor de emisii (denumit în continuare „EU ETS”) sau în cadrul sistemului Elveției de comercializare a certificatelor de emisii (denumit în continuare ETS-ul Elveției). În vederea activării legăturii dintre EU ETS și ETS-ul Elveției, se va crea o legătură directă între Registrul de tranzacții al Uniunii Europene (EUTL) din cadrul registrului Uniunii și Registrul suplimentar de tranzacții al Elveției (SSTL) din cadrul registrului elvețian, ceea ce va permite transferul dintr-un registru în altul al certificatelor de emisii emise în cadrul oricăruia dintre ETS-uri [articolul 3 alineatul (2) din acord]. Pentru a operaționaliza legătura dintre EU ETS și ETS-ul Elveției, în 2020 a fost pusă în aplicare o soluție provizorie. Începând din 2023, legătura dintre cele două sisteme de comercializare a certificatelor de emisii se va transforma treptat într-o legătură permanentă între registre, a cărei implementare este preconizată a avea loc cel târziu în 2024, care va permite funcționarea piețelor legate în ceea ce privește beneficiile oferite de lichiditatea pieței și de executarea tranzacțiilor între cele două sisteme conectate într-un mod echivalent cu o piață formată din două sisteme și care va permite participanților la piață să acționeze ca și cum ar fi pe o singură piață, sub rezerva unor dispoziții de reglementare individuale ale părților (anexa II la acord).

În conformitate cu articolul 3 alineatul (7) din acord, administratorul registrului elvețian și administratorul central al Uniunii stabilesc standardele tehnice de creare a legăturii (LTS) pe baza principiilor prevăzute în anexa II la acord, în care sunt descrise în detaliu cerințele pentru stabilirea unei legături robuste și securizate între SSTL și EUTL. Standardele tehnice de creare a legăturii elaborate de administratori produc efecte după ce sunt adoptate printr-o decizie a comitetului mixt.

LTS a fost adoptată de comitetul mixt prin Decizia nr. 2/2020. Procedeele comune de funcționare actualizate, astfel cum sunt specificate în prezentul document, vor fi adoptate prin Decizia nr. 1/2024 a comitetului mixt. În conformitate cu prezenta decizie și cu solicitările Comitetului mixt, administratorul registrului elvețian și administratorul central al Uniunii au elaborat și vor actualiza orientări tehnice suplimentare pentru activarea legăturii și pentru a garanta că acestea sunt adaptate permanent la progresul tehnic și la noile cerințe privind siguranța și securitatea legăturii și funcționarea efectivă și eficientă a acesteia.

2.1. Domeniul de aplicare

Prezentul document reprezintă înțelegerea comună între părțile la acord cu privire la stabilirea fundamentelor tehnice ale legăturii dintre registrele EU ETS și ETS-ul Elveției. Deși documentul pune bazele specificațiilor tehnice în ceea ce privește cerințele privind arhitectura, serviciile și securitatea, vor fi necesare unele orientări suplimentare detaliate pentru activarea legăturii.

Pentru funcționarea sa corespunzătoare, legătura va necesita procese și procedee pentru operaționalizarea în continuare a acesteia. În conformitate cu articolul 3 alineatul (6) din acord, aceste aspecte sunt prezentate în detaliu într-un document separat privind procedeele comune de funcționare, care urmează să fie adoptat separat prin decizia comitetului mixt.

2.2. Destinatari

Prezentul document se adresează administratorului registrului elvețian și administratorului central al Uniunii.

3. DISPOZIȚII GENERALE

3.1. Arhitectura legăturii de comunicare

Scopul prezentei secțiuni este de a oferi o descriere a arhitecturii generale a activării legăturii dintre EU ETS și ETS-ul Elveției și a diferitelor componente implicate în aceasta.

Având în vedere faptul că securitatea reprezintă un element-cheie pentru definirea arhitecturii legăturii dintre registre, au fost luate toate măsurile pentru crearea unei arhitecturi robuste. Legătura permanentă între registre utilizează un mecanism de schimb de fișiere, ca implementare a unei conexiuni securizate Air Gap.

Soluția tehnică utilizează:

— un protocol de transfer securizat pentru schimburile de mesaje;

— mesaje XML;

— semnătură digitală și criptare bazate pe XML;

— VPN.

3.1.1. Schimbul de mesaje

Comunicarea dintre registrul Uniunii și registrul elvețian se bazează pe un mecanism de schimb de mesaje prin intermediul unor canale securizate. Fiecare parte se bazează pe propriul sistem de colectare a mesajelor primite.

Ambele părți țin o evidență a mesajelor primite, împreună cu detaliile procesărilor.

Erorile sau situațiile neașteptate trebuie raportate, sub formă de alerte, și ar trebui să aibă loc contactul uman între echipele de asistență.

Erorile și evenimentele neașteptate sunt gestionate conform procedeelor de funcționare prevăzute în secțiunea privind procesul de gestionare a incidentelor din procedeele comune de funcționare.

3.1.2. Mesaj XML – Descriere de nivel înalt

Un mesaj XML conține unul dintre următoarele elemente:

— una sau mai multe cereri de tranzacții și/sau unul sau mai multe răspunsuri la tranzacții;

— o operațiune/un răspuns legat de reconciliere;

— un mesaj test.

Fiecare mesaj conține un antet care include:

— sistemul ETS de origine;

— numărul de secvență.

3.1.3. Ferestre de ingerare (Ingestion Windows)

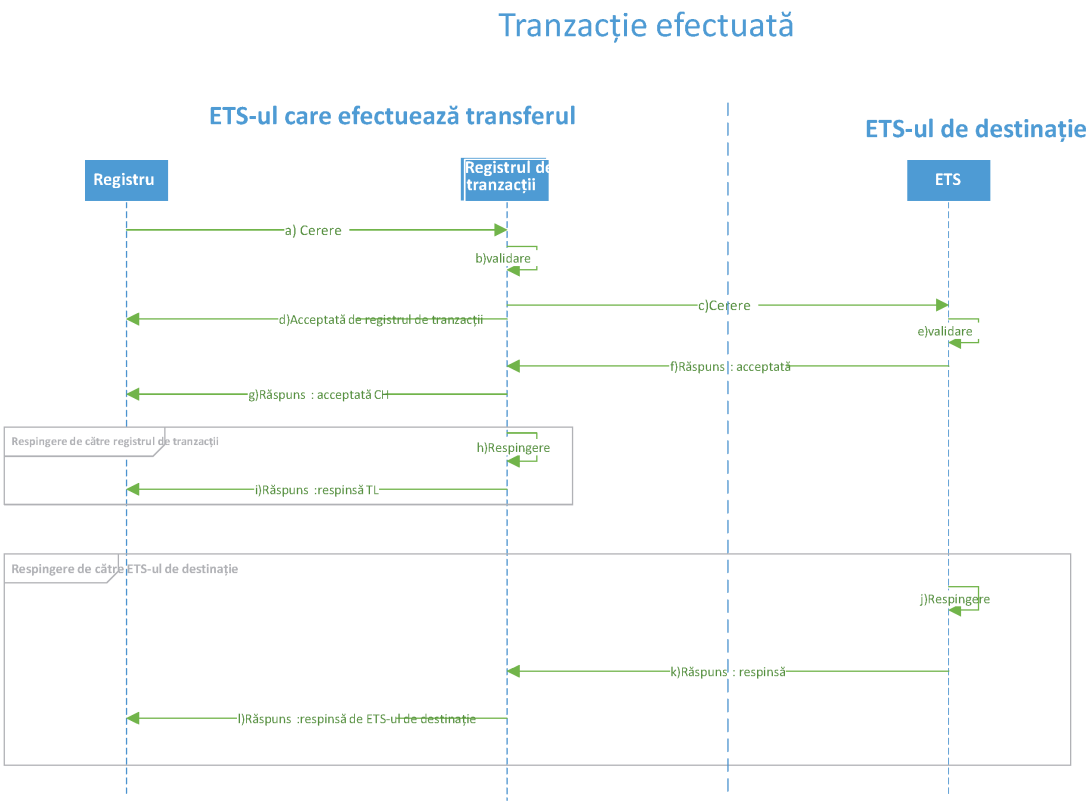
Legătura permanentă între registre se bazează pe ferestre de ingerare predefinite care sunt urmate de un set de evenimente cu nume. Cererile de tranzacții primite prin intermediul legăturii vor fi ingerate numai la intervale predefinite. Ferestrele de ingerare includ o validare tehnică pentru tranzacțiile efectuate și primite. În plus, reconcilierile pot fi derulate zilnic și declanșate manual.

Modificările de frecvență și/sau ale momentelor de desfășurare ale oricăruia dintre aceste evenimente vor fi gestionate conform procedeelor de funcționare prevăzute în secțiunea privind procesul de soluționare a cererilor din procedeele comune de funcționare.

3.1.4. Fluxurile de mesaje privind tranzacțiile

Tranzacțiile efectuate

Reflectă punctul de vedere al ETS-ului care efectuează transferul. Fluxul specific este prezentat în următoarea diagramă de secvență:



Fluxul principal prezintă următoarele etape (la fel ca în desenul de mai sus):

(a) În cadrul ETS-ului care efectuează transferul, cererea de tranzacție este trimisă de la registru către registrul de tranzacții, după încheierea tuturor întârzierilor comerciale (întârziere de 24 de ore, după caz).

(b) Registrul de tranzacții validează cererea de tranzacție.

(c) Cererea de tranzacție este trimisă către ETS-ul de destinație.

(d) Răspunsul de acceptare este trimis către registrul din cadrul ETS-ului de origine.

(e) ETS-ul de destinație validează cererea de tranzacție.

(f) ETS-ul de destinație retrimite răspunsul de acceptare către registrul de tranzacții din cadrul ETS-ului de origine.

(g) Registrul de tranzacții trimite răspunsul de acceptare către registru.

Flux alternativ „Respingerea registrului de tranzacții” [astfel cum este indicat în desenul de mai sus, începând de la litera (a) din fluxul principal]:

(a) În cadrul sistemului de origine, cererea de tranzacție este trimisă de la registru către registrul de tranzacții, după încheierea tuturor întârzierilor comerciale (întârziere de 24 de ore, după caz).

(b) Registrul de tranzacții nu validează cererea

(c) Mesajul de respingere este trimis către registrul de origine.

Debit alternativ „Respingere ETS” [astfel cum este prezentat în desenul de mai sus, începând de la litera (d) în fluxul principal]:

(a) În cadrul ETS-ului de origine, cererea de tranzacție este trimisă de la registru către registrul de tranzacții, după încheierea tuturor întârzierilor comerciale (întârziere de 24 de ore, după caz).

(b) Registrul de tranzacții validează tranzacția.

(c) Cererea de tranzacție este trimisă către ETS-ul de destinație.

(d) Mesajul de acceptare este trimis către registrul din cadrul ETS-ului de origine.

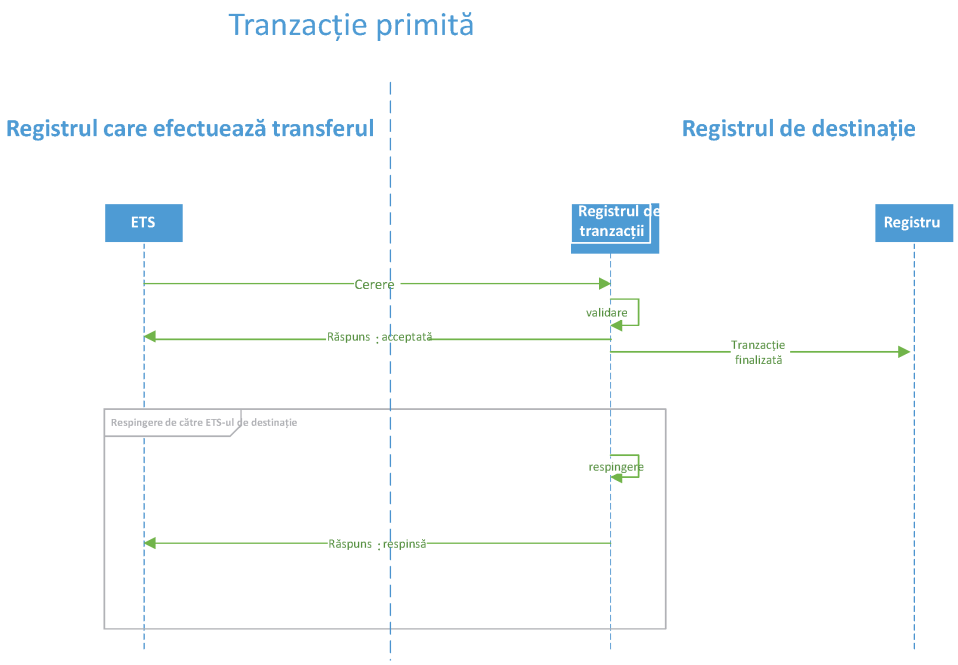
(e) Registrul de tranzacții din cadrul ETS-ului de destinație nu validează tranzacția.

(f) ETS-ul de destinație trimite răspunsul de refuz către registrul de tranzacții din cadrul ETS-ului care a efectuat transferul.

(g) Registrul de tranzacții trimite refuzul către registru.

Tranzacțiile primite

Aceasta reflectă punctul de vedere al ETS-ului de destinație. Fluxul specific este prezentat în următoarea diagramă de secvență:



În diagramă se indică următoarele:

1. Atunci când registrul de tranzacții din cadrul ETS-ului de destinație validează cererea, acesta trimite mesajul de acceptare către ETS-ul care efectuează transferul și mesajul „tranzacție finalizată” către registrul din cadrul ETS-ului de destinație.

2. Atunci când o cerere primită este refuzată în registrul de tranzacții de destinație și este refuzată, cererea de tranzacție nu este trimisă către registrul din cadrul ETS-ului de destinație.

Protocol

Ciclul mesajelor privind tranzacțiile implică doar două mesaje:

— ETS-ul care efectuează transferulà Propunerea de tranzacție pentru ETS-ul de destinație;

— ETS-ul de destinație à Răspunsul la tranzacție pentru ETS-ul care efectuează transferul: Fie „Acceptată”, fie „Respinsă” (inclusiv motivul respingerii).

  — Acceptat: Tranzacția este finalizată.

  — Respinsă: Tranzacția este încheiată.

Stadiul tranzacției

— În momentul trimiterii cererii, stadiul tranzacției va fi setat la „propusă” în cadrul ETS-ului care efectuează transferul.

— În momentul primirii cererii și pe parcursul procesării acesteia, stadiul tranzacției va fi setat la „propusă” în cadrul ETS-ului de destinație.

— După procesarea cererii, stadiul tranzacției va fi setat la „finalizată”/„încheiată” în cadrul ETS-ului de destinație. ETS-ul de destinație va trimite apoi mesajul de acceptare/respingere corespunzător.

— După primirea și procesarea mesajului de acceptare/respingere, stadiul tranzacției va fi setat la „finalizată”/„încheiată” în cadrul ETS-ului care efectuează transferul.

— În cazul în care nu se primește niciun răspuns, stadiul tranzacției va rămâne „propusă” în cadrul ETS-ului care efectuează transferul.

— Stadiul tranzacției în cadrul ETS-ului de destinație va fi setat ca „încheiată” dacă orice tranzacție propusă rămâne în stadiul de „propusă” mai mult de 30 de minute.

Incidentele legate de tranzacții vor fi gestionate cu respectarea procedeelor de funcționare prevăzute în cadrul procesului de gestionare a incidentelor din procedeele comune de funcționare.

3.2. Securitatea transferurilor de date

Datele aflate în tranzit vor face obiectul a patru niveluri de securitate:

1. Controlul accesului la rețea: firewall și nivelul de interconectare între rețele.

2. Criptarea la nivelul de transport: VPN.

3. Criptarea la nivelul sesiunilor: protocol de transfer securizat pentru schimburile de mesaje.

4. Criptarea la nivelul aplicațiilor: semnătură și criptare a conținutului bazate pe XML.

3.2.1. Firewall și interconectarea între rețele

Legătura este stabilită prin intermediul unei rețele protejate de un firewall pe bază de hardware. Firewall-ul este configurat cu reguli potrivit cărora doar clienții „înregistrați” să se poată conecta la serverul VPN.

3.2.2. Rețea virtuală privată (VPN)

Toate comunicările dintre părți sunt protejate cu ajutorul unei tehnologii cu rețea virtuală privată (VPN). Tehnologiile VPN oferă posibilitatea „transportului” dintr-un punct în altul printr-o rețea precum internetul, protejând toate comunicațiile. Înainte de crearea tunelului VPN, un certificat digital este transmis către punctul final al unui potențial client, permițând clientului să furnizeze dovada identității pe parcursul negocierii legăturii. Fiecare parte este responsabilă pentru instalarea certificatului în propriul punct final VPN. Utilizând certificate digitale, fiecare server VPN final va accesa o autoritate centrală pentru a negocia acreditările de autentificare. Pe parcursul procesului de creare a tunelului, se negociază criptarea, asigurând protejarea tuturor comunicațiilor efectuate prin intermediul tunelului.

Punctele finale VPN ale clienților sunt configurate pentru a menține în permanență tunelul VPN, pentru a permite în orice moment o comunicare fiabilă, bidirecțională și în timp real între părți.

În general, Uniunea Europeană utilizează serviciile transeuropene securizate de telematică între administrații (STESTA) ca rețea privată bazată pe IP. Prin urmare, această rețea este adecvată și pentru legătura permanentă între registre.

3.2.3. Implementarea IPSec

Utilizarea protocolului IPSec pentru formarea infrastructurii VPN site-to-site va asigura autentificarea site-to-site, integritatea datelor și criptarea acestora. Configurațiile VPN care includ protocoale IPSec asigură o autentificare corectă între două puncte finale în cazul unei conexiuni VPN. Părțile vor identifica și autentifica clientul de la distanță prin conexiunea IPSec utilizând un certificat digital emis de o autoritate de certificare recunoscută de cealaltă parte.

Protocolul IPSec asigură, de asemenea, integritatea datelor pentru toate comunicațiile efectuate prin intermediul tunelului VPN. Pachetele de date sunt trunchiate și semnate utilizând informațiile de autentificare stabilite prin VPN. Confidențialitatea datelor este asigurată și prin activarea criptării IPSec.

3.2.4. Protocol de transfer securizat pentru schimburile de mesaje

Legătura permanentă între registre se bazează pe mai multe niveluri de criptare pentru schimbul securizat de date între părți. Ambele sisteme și mediile lor diferite sunt interconectate la nivelul rețelei prin intermediul unor tuneluri VPN. La nivel de aplicație, fișierele sunt transferate cu ajutorul unui protocol de transfer securizat pentru schimburile de mesaje la nivel de sesiune.

3.2.5. Criptare și semnătură bazate pe XML

În fișierele XML, semnarea și criptarea se realizează la două niveluri. Fiecare cerere de tranzacție, răspuns la o tranzacție și mesaj de reconciliere se semnează digital, în mod individual.

Într-o a doua etapă, fiecare subelement al elementului „mesaj" este criptat individual.

În plus, ca o a treia etapă și pentru a asigura integritatea și non-repudierea întregului mesaj, mesajul elementului rădăcină este semnat digital. Acesta conduce la un nivel ridicat de protecție pentru datele încorporate în format XML. Implementarea tehnică respectă standardele consorțiului World Wide Web.

Pentru a decripta și a verifica mesajul, procesul este efectuat în ordine inversă.

3.2.6. Chei criptografice

Criptografia cu chei publice va fi utilizată pentru criptare și semnare.

Pentru cazul specific al IPSec, se va utiliza un certificat digital emis de o autoritate de certificare (CA) acceptată de ambele părți. Respectiva autoritate de certificare verifică identitatea deținătorului certificatului și emite certificate care sunt utilizate pentru a identifica pozitiv o organizație și a configura canale de comunicații de date securizate între părți.

Cheile criptografice sunt utilizate pentru semnarea și criptarea canalelor de comunicare și a fișierelor de date. Certificatele publice sunt schimbate digital de către părți prin intermediul unor canale securizate și sunt verificate pe un canal de comunicare diferit de cel principal. Această procedură este o parte integrantă a procesului de management al securității informațiilor prevăzut în procedeele comune de funcționare.

3.3. Lista funcțiilor în cadrul legăturii

Legătura specifică sistemul de transmisie pentru o serie de funcții care implementează procesele comerciale prevăzute în acord. Legătura include, de asemenea, specificația pentru procesul de reconciliere și pentru mesajele test care vor permite implementarea unei monitorizări a ritmicității.

3.3.1. Tranzacțiile comerciale

Din perspectivă comercială, legătura include patru (4) tipuri de cereri de tranzacții:

— Transfer extern:

  — După activarea legăturii între ETS-uri, certificatele UE și CH sunt fungibile și, prin urmare, complet transferabile, între părți.

  — Un transfer efectuat prin intermediul legăturii va implica un cont de transfer pe un ETS și un cont de achiziție pe celălalt ETS.

  — transferul poate include orice cantitate din cele patru (4) tipuri de certificate:

    — Certificate generale elvețiene (CHU)

    — Certificate pentru aviație elvețiene (CHUA)

    — Certificate generale ale UE (EUA)

    — Certificate pentru aviație al UE (EUAA)

— Alocare internațională:

  Operatorii de aeronave administrați de un ETS cu obligații în celălalt ETS și îndreptățiți să primească certificate gratuite de la cel de-al doilea ETS, vor primi certificate pentru aviație gratuite de la cel de-al doilea ETS prin intermediul tranzacției de certificate internaționale.

— Revocarea unei alocări internaționale:

Această tranzacție se va realiza în cazul în care certificatele gratuite alocate unui operator de aeronave deținut de celălalt ETS trebuie revocate în totalitate.

— Returnarea unei alocări în exces:

Similar cu revocarea, dar în cazul în care alocarea nu trebuie să fie revocată în totalitate și numai certificatele supraalocate trebuie returnate ETS-ului care le-a alocat.

3.3.2. Protocolul reconcilierilor

Reconcilierile vor avea loc numai după închiderea ferestrei pentru ingerarea, validarea și procesarea mesajelor.

Reconcilierile sunt o parte integrantă a măsurilor privind securitatea și coerența legăturii. Ambele părți vor conveni asupra momentului exact al reconcilierii înainte de elaborarea oricărui calendar. O reconciliere zilnică programată se poate realiza doar cu acordul ambelor părți. Cel puțin o reconciliere programată va fi executată în orice caz după efectuarea operațiunii de ingerare.

În orice caz, oricare dintre părți poate să inițieze în orice moment reconcilieri manuale.

Modificările momentelor de desfășurare și ale frecvenței reconcilierii programate vor fi gestionate conform procedeelor de funcționare prevăzute în secțiunea privind procesul de soluționare a cererilor din procedeele comune de funcționare.

3.3.3. Mesaj test

Un mesaj test este prevăzut pentru a testa comunicarea de la un capăt la celălalt capăt. Mesajul va conține date care vor identifica mesajul drept test și va primi un răspuns după primirea sa la celălalt capăt.

3.4. Cerințe privind înregistrarea datelor

Pentru a răspunde nevoii ambelor părți de a păstra informații corecte și coerente și de a furniza instrumente care să fie utilizate în cadrul procesului de reconciliere pentru remedierea neconcordanțelor, sunt păstrate patru (4) tipuri de evidențe de date de către ambele părți:

— registrele de tranzacții;

— registrele de reconcilieri;

— arhiva de mesaje;

— registrele de evidență a auditurilor interne.

Toate datele din registrele respective sunt păstrate pentru o perioadă de cel puțin trei (3) luni în scopul efectuării operațiunilor de depanare, iar păstrarea lor ulterioară va depinde de legislația privind efectuarea auditurilor, aplicabilă la fiecare capăt. Fișierele-jurnal mai vechi de trei (3) luni pot fi arhivate într-o locație securizată într-un sistem IT independent atât timp cât acestea pot fi preluate sau accesate într-o perioadă rezonabilă.

Registrele de tranzacții

Subsistemele EUTL și SSTL sunt implementări ale registrelor de tranzacții.

Mai exact, registrele de tranzacții vor ține o evidență a fiecărei tranzacții propuse trimise celuilalt ETS. Fiecare evidență include toate câmpurile conținutului tranzacției și rezultatul ulterior al tranzacției (răspunsul ETS-ului de destinație). Registrele de tranzacții vor ține și o evidență a tranzacțiilor efectuate, precum și răspunsul trimis ETS-ului de origine.

Registrele de reconcilieri

Registrul de reconcilieri include o evidență a fiecărui mesaj de reconciliere transmis între cele două părți, inclusiv ID-ul reconcilierii, marcajul temporal și rezultatul reconcilierii: Stadiul reconcilierii „Reușită” sau „Discrepanțe”. În cadrul legăturii permanente între registre, mesajele de reconciliere fac parte integrantă din mesajele schimbate și, prin urmare, sunt stocate astfel cum se descrie în secțiunea „Arhiva de mesaje”.

Ambele părți înregistrează fiecare cerere și răspunsul aferent în Registrul de reconcilieri. Cu toate că informațiile din Registrul de reconcilieri nu sunt partajate în mod direct ca parte a reconcilierii în sine, poate fi necesar accesul la respectivele informații pentru a remedia neconcordanțele.

Arhiva de mesaje

Ambele părți au obligația de a arhiva o copie a datelor partajate (fișierele XML), trimise și primite, indiferent dacă respectivele date sau mesajele XML au fost corecte în formatul lor sau nu.

Scopul principal al arhivării este de a avea dovada mesajelor trimise celeilalte părți și primite de la cealaltă parte, pe care să o prezinte în cursul unui audit. În acest scop, împreună cu fișierele, trebuie să fie arhivate și certificatele aferente.

Fișierele respective vor oferi, de asemenea, informații suplimentare pentru operațiunile de depanare.

Registrele de evidență a auditurilor interne

Aceste registre sunt definite și utilizate individual de către fiecare parte.

3.5. Cerințele operaționale

Schimbul de date între cele două sisteme nu este complet autonom în cadrul legăturii permanente între registre, ceea ce înseamnă că este nevoie de operatori și de proceduri pentru activarea legăturii. Mai multe roluri și instrumente sunt detaliate în acest scop în cadrul acestui proces.

4. DISPOZIȚII PRIVIND DISPONIBILITATEA

4.1. Proiectarea disponibilității comunicațiilor

Arhitectura legăturii permanente între registre este în esență o infrastructură și un software TIC care permite comunicarea între ETS-ul Elveției și EU ETS. Prin urmare, asigurarea unor niveluri ridicate de disponibilitate, integritate și confidențialitate a acestui flux de date devine un aspect esențial de luat în considerare pentru proiectarea legăturii permanente între registre. Fiind un proiect în care infrastructura TIC, software-ul personalizat și procesele joacă un rol fundamental, toate cele trei elemente trebuie luate în considerare pentru proiectarea unui sistem rezilient.

Reziliența infrastructurii TIC

În capitolul privind dispozițiile generale din prezentul document sunt descrise în detaliu elementele constitutive ale arhitecturii. În ceea ce privește infrastructura TIC, legătura permanentă între registre instituie o rețea VPN rezilientă care creează tuneluri de comunicare securizate prin intermediul cărora se pot realiza schimburi de mesaje securizate. Alte elemente de infrastructură sunt configurate cu un grad ridicat de disponibilitate și/sau se bazează pe mecanisme de rezervă.

Reziliența software-ului personalizat

Modulele software personalizate dezvoltate îmbunătățesc reziliența prin reluarea comunicării cu celălalt capăt pentru o anumită perioadă, în cazul în care aceasta nu este disponibilă din anumite motive.

Reziliența serviciilor

În legătura permanentă între registre, schimburile de date dintre părți au loc la intervale predefinite. Unele dintre etapele necesare pentru schimburile de date programate în prealabil necesită intervenția manuală a operatorilor sistemului și/sau a administratorilor registrelor. Luând în considerare acest aspect și pentru a spori gradul de disponibilitate și de reușită a schimburilor:

— Procedeele de funcționare prevăd intervale orare pentru efectuarea fiecărei etape.

— Modulele software pentru legătura permanentă între registre implementează o comunicare asincronă.

— Procesul de reconciliere automată va detecta dacă au existat probleme în ingerarea fișierelor de date la fiecare dintre capete.

— Procesele de monitorizare (infrastructura TIC și modulele software personalizate) sunt luate în considerare și declanșează procedeele de gestionare a incidentelor (astfel cum sunt definite în documentul referitor la procedeele comune de funcționare). Procedeele care vizează reducerea timpului pentru restabilirea funcționării normale în urma unor incidente sunt esențiale pentru asigurarea unor niveluri ridicate de disponibilitate.

4.2. Planul de inițializare, comunicare, reactivare și testare

Toate elementele diferite implicate în arhitectura legăturii permanente între registre fac obiectul unei serii de teste individuale și colective în vederea confirmării faptului că platforma este pregătită la nivelul infrastructurii TIC și a sistemului de informații. Aceste teste de funcționare reprezintă o condiție obligatorie de fiecare dată când platforma tranzitează legătura permanentă între registre de la stadiul de „suspendată” la stadiul de „funcțională”.

Activarea stadiului funcțional al legăturii necesită apoi executarea cu succes a unui plan de testare predefinit. Acesta confirmă faptul că fiecare registru a efectuat mai întâi un set de teste interne, urmat de validarea conectivității între utilizatorii finali înainte de a începe tranzacțiile de producție între cele două părți.

În planul de testare ar trebui să se menționeze strategia generală de testare și detalii privind infrastructura de testare. Planul de testare ar trebui să includă, în special, pentru fiecare element al fiecărui bloc de testare:

— criteriile și instrumentele de testare;

— rolurile atribuite pentru efectuarea testului;

— rezultatele scontate (pozitive și negative);

— calendarul testelor;

— înregistrarea cerințelor privind rezultatele testelor;

— documentația referitoare la operațiunile de depanare;

— dispoziții privind escaladările.

Ca proces, testele de activare a stadiului funcțional pot fi împărțite în patru (4) blocuri sau faze conceptuale:

4.2.1. Testele interne pentru infrastructura TIC

Testele respective trebuie efectuate și/sau verificate individual de către administratorii registrelor la fiecare capăt.

Fiecare element al infrastructurii TIC de la fiecare capăt este testat individual. Acestea includ fiecare componentă a infrastructurii. Aceste teste pot fi executate automat sau manual, însă trebuie să verifice funcționalitatea fiecărui element al infrastructurii.

4.2.2. Testele de comunicare

Testele respective sunt declanșate individual de către fiecare parte și pentru finalizarea lor este necesară cooperarea celuilalt capăt.

Atunci când fiecare element în parte este funcțional, trebuie testate canalele de comunicare între cele două registre. În acest scop, fiecare parte verifică dacă accesul la internet funcționează, dacă tunelurile VPN sunt stabilite și dacă există conectivitate IP site-to-site. Accesibilitatea elementelor de infrastructură locale și la distanță și conectivitatea IP ar trebui apoi confirmate la celălalt capăt.

4.2.3. Teste pentru întregul sistem (de la un capăt la celălalt capăt)

Aceste teste trebuie executate la fiecare capăt, iar rezultatele sunt partajate cu cealaltă parte.

După ce au fost testate canalele de comunicare și fiecare componentă a ambelor registre, fiecare capăt va pregăti o serie de simulări de tranzacții și de reconcilieri, reprezentative pentru toate funcțiile care urmează să fie implementate în cadrul legăturii.

4.2.4. Testele de securitate

Aceste teste trebuie efectuate și/sau declanșate de administratorii registrelor la fiecare capăt și conform specificațiilor prevăzute în secțiunile 5.4, „Orientări privind testarea securității”, și 5.5, „Dispoziții privind evaluarea riscurilor”.

Numai după ce fiecare dintre cele patru faze/blocuri s-a încheiat cu rezultatele scontate, registrul permanent poate fi considerat funcțional.

Resurse de testare

Fiecare parte se bazează pe resurse de testare specifice (software și hardware specifice infrastructurii TIC) și dezvoltă funcții de testare în sistemele lor corespunzătoare pentru a susține validarea manuală și continuă a platformei. Procedurile de testare manuale individuale sau cooperative pot fi executate în orice moment de către administratorii registrelor. Activarea stadiului de funcționare este un proces manual în sine.

Se prevede, de asemenea, ca platforma să efectueze verificări automate la intervale regulate. Aceste verificări vizează creșterea disponibilității platformei prin detectarea din timp a potențialelor probleme legate de infrastructură sau de software. Acest plan de monitorizare a platformei este alcătuit din două elemente:

— Monitorizarea infrastructurilor TIC: la ambele capete, infrastructura va fi monitorizată de furnizorii de servicii de infrastructură TIC. Testele automate vor acoperi diferitele elemente de infrastructură și disponibilitatea canalelor de comunicare.

— Monitorizarea aplicațiilor: modulele software pentru crearea registrului permanent vor implementa monitorizarea comunicării în cadrul sistemului la nivel de aplicație (manual și/sau la intervale regulate), care va testa disponibilitatea de la un capăt la altul a legăturii prin simularea unora dintre tranzacțiile efectuate în cadrul legăturii.

4.3. Mediile de acceptare/de testare

Arhitectura registrului Uniunii și a registrului Elveției constă în următoarele trei medii:

— Producție (PROD): Acest mediu deține datele reale și procesează tranzacții reale.

— Acceptare (ACC): Acest mediu conține date reprezentative nereale sau anonimizate. Este mediul în care operatorii de sistem ale ambelor părți validează noile versiuni.

— Test (TEST): Acest mediu conține date reprezentative nereale sau anonimizate. Acest mediu este limitat la administratorii registrelor și menit să fie utilizat pentru a efectua teste de integrare de către ambele părți.

Cu excepția VPN, cele trei medii sunt complet independente unele de altele; cu alte cuvinte, hardware-ul, software-ul, bazele de date, mediile virtuale, adresele IP și porturile sunt configurate și funcționează independent unele de altele.

În ceea ce privește configurația VPN, comunicarea dintre cele trei medii trebuie să fie complet independentă, ceea ce este asigurat prin utilizarea STESTA.

5. DISPOZIȚII PRIVIND CONFIDENȚIALITATEA ȘI INTEGRITATEA

Mecanismele și procedurile de securitate prevăd o metodă pentru două persoane (principiul „celor patru ochi”) pentru operațiunile desfășurate în cadrul legăturii dintre registrul Uniunii și registrul elvețian. Metoda pentru două persoane se aplică ori de câte ori este necesar. Cu toate acestea, nu se poate aplica tuturor etapelor parcurse de administratorii registrelor.

Cerințele de securitate sunt luate în considerare și abordate în planul de gestionare a securității, care include, de asemenea, procese legate de gestionarea incidentelor de securitate ca urmare a unei eventuale încălcări a securității. Partea operațională a acestor procese este descrisă în procedeele comune de funcționare.

5.1. Infrastructura de testare a securității

Fiecare parte se angajează să creeze o infrastructură de testare a securității (prin utilizarea software-ului și hardware-ului comune utilizate pentru detectarea vulnerabilităților în fazele de dezvoltare și de funcționare):

— separat de mediul de producție;

— în cazul în care securitatea este analizată de o echipă independentă de echipa de dezvoltare și operare a sistemului.

Fiecare parte se angajează să efectueze atât analize statice, cât și analize dinamice.

În cazul unei analize dinamice (cum ar fi testul de rezistență la intruziuni), ambele părți se angajează să restricționeze evaluările în mod obișnuit la mediile de testare și de acceptare (astfel cum sunt definite în secțiunea 4.3, „Medii de acceptare/de testare”). Excepțiile de la această politică fac obiectul aprobării de către ambele părți.

Înainte de implementarea în mediul de producție, se testează securitatea fiecărui modul software al legăturii (astfel cum este definit în secțiunea 3.4, „Arhitectura legăturii de comunicare”).

Infrastructura de testare trebuie să fie separată de cea de producție, atât la nivel de rețea, cât și la nivel de infrastructură. Infrastructura de testare este cea în care se efectuează testele de securitate necesare pentru a verifica respectarea cerințelor de securitate.

5.2. Dispoziții privind suspendarea și reactivarea legăturii

Atunci când există suspiciunea că securitatea registrului elvețian, a SSTL, a registrului Uniunii sau a EUTL a fost compromisă, fiecare parte o informează imediat pe cealaltă și suspendă legătura dintre SSTL și EUTL;

Procedurile privind schimbul de informații, pentru o decizie de suspendare și pentru o decizie de reactivare fac parte din procesul de soluționare a cererilor prevăzut în procedeele comune de funcționare.

Suspendări

Suspendarea legăturii între registre în conformitate cu anexa II la acord se poate produce în următoarele situații:

— Din motive administrative (de exemplu întreținere), care sunt planificate;

— Din motive de securitate (sau defecțiuni ale infrastructurii IT), care sunt neplanificate.

În caz de urgență, oricare dintre părți va informa cealaltă parte și va suspenda unilateral legătura între registre.

Dacă se ia decizia de a suspenda legătura între registre, atunci fiecare parte se va asigura că legătura este întreruptă la nivel de rețea (prin blocarea părților sau a tuturor conexiunilor de intrare și de ieșire).

Decizia de suspendare a legăturii între registre, indiferent dacă este planificată sau neplanificată, se va lua în conformitate cu procedura de gestionare a modificărilor sau de gestionare a incidentelor de securitate prevăzută în procedeele comune de funcționare.

Reactivarea comunicării

O decizie de reactivare a legăturii între registre va fi luată în modul prezentat în detaliu în procedeele comune de funcționare și, în orice caz, înainte de finalizarea cu succes a procedurilor de testare a securității, astfel cum sunt prezentate în detaliu în secțiunile 5.4, „Orientări privind testările de securitate”, și 4.2, „Planul de inițializare, comunicare, reactivare și testare”.

5.3. Dispoziții privind încălcarea securității

O încălcare a securității este considerată un incident de securitate care afectează confidențialitatea și integritatea oricăror informații sensibile și/sau disponibilitatea sistemului care le gestionează.

Informațiile sensibile sunt menționate în Evidența informațiilor sensibile și pot fi gestionate în cadrul sistemului sau în cadrul oricărei componente conexe a sistemului.

Informațiile direct legate de încălcarea securității vor fi considerate sensibile, marcate cu mențiunea „SPECIAL HANDLING: *ETS critical*” și gestionat în conformitate cu instrucțiunile de gestionare, cu excepția cazului în care se specifică altfel.

Fiecare încălcare a securității va fi gestionată în conformitate cu secțiunea „Gestionarea incidentelor de securitate” din procedeele comune de funcționare.

5.4. Orientări privind testarea securității

5.4.1. Software

Testarea securității, inclusiv testul de rezistență la intruziuni, dacă este cazul, se efectuează cel puțin pe toate noile versiuni importante ale software-ului, în conformitate cu cerințele de securitate prevăzute în standardele tehnice de creare a legăturii, pentru a evalua securitatea legăturii și riscurile aferente.

Dacă în ultimele 12 luni nu s-a produs nicio versiune importantă, se efectuează testul de securitate în sistemul curent, luând în considerare evoluția amenințărilor cibernetice din cursul ultimelor 12 luni.

Testarea securității legăturii între registre se efectuează în mediul de acceptare și, dacă este necesar, în mediul de producție și cu coordonarea și acordul reciproc ale ambelor părți.

Testarea aplicațiilor web va respecta standardele internaționale deschise, cum ar fi cele elaborare de fundația Open Web Application Security Project (OWASP).

5.4.2. Infrastructură

Infrastructura care susține sistemul de producție este scanată în mod regulat împotriva vulnerabilităților (cel puțin o dată pe lună), iar vulnerabilitățile detectate sunt remediate pe baza aceluiași principiu definit în secțiunea precedentă, utilizând o bază de date actualizată a vulnerabilităților.

5.5. Dispoziții privind evaluarea riscurilor

Dacă testul de rezistență la intruziuni este aplicabil, acesta trebuie inclus în testarea securității.

Fiecare parte poate contracta o societate specializată pentru efectuarea testelor de securitate, cu condiția ca respectiva societate:

— să aibă competențele și experiența necesare pentru efectuarea unor astfel de teste de securitate;

— să nu raporteze direct dezvoltatorului și/sau contractantului său, să nu fie implicată în dezvoltarea software-ului legăturii și nici să nu fie subcontractant al dezvoltatorului;

— să fi semnat un acord de confidențialitate pentru păstrarea confidențialității rezultatelor și pentru gestionarea acestora la nivelul „SPECIAL HANDLING: *ETS Critical*” în conformitate cu instrucțiunile de gestionare.