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]

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]) („acordul"), în special articolul 3 alineatul (7) și articolul 13 alineatul (2),

întrucât:

(1) Decizia nr. 2/2019 a comitetului mixt din 5 decembrie 2019 ([2]) a modificat anexele I și II la acord, îndeplinind astfel condițiile prevăzute în acord pentru crearea legăturii.

(2) După adoptarea Deciziei nr. 2/2019 a comitetului mixt și în temeiul articolului 21 alineatul (3) din acord, părțile au făcut schimb de instrumente de ratificare sau aprobare, deoarece consideră că au fost îndeplinite toate condițiile pentru crearea legăturii, astfel cum sunt prevăzute în acord.

(3) În conformitate cu articolul 21 alineatul (4) din acord, acordul a intrat în vigoare la 1 ianuarie 2020.

(4) Anexa I la acord ar trebui modificată în conformitate cu articolul 13 alineatul (2) din acord pentru a asigura o tranziție ușoară în ceea ce privește administrarea operatorilor de aeronave atribuiți Elveției pentru prima dată, luând în considerare progresele înregistrate în stabilirea legăturii între registre.

(5) Pentru a îngloba evoluțiile recente și pentru a asigura un nivel crescut de flexibilitate în ceea ce privește stabilirea legăturii dintre registre prevăzută în acord, anexa II la acord ar trebui modificată în conformitate cu articolul 13 alineatul (2) din acord pentru a include un set mai mare, dar echivalent de tehnologii în vederea realizării legăturii între registre.

(6) În temeiul articolului 3 alineatul (7) din acord, administratorul registrului elvețian și administratorul central al Uniunii ar trebui să elaboreze standarde tehnice de creare a legăturii (LTS) pe baza principiilor stabilite în anexa II la acord. În standardele tehnice de creare a legăturii ar trebui descrise în detaliu cerințele pentru stabilirea unei legături robuste și securizate între Registrul suplimentar de tranzacții al Elveției (SSTL) și Registrul de tranzacții al Uniunii Europene (EUTL). Standardele tehnice de creare a legăturii ar trebui să producă efecte după ce vor fi adoptate prin decizia comitetului mixt.

(7) În conformitate cu articolul 13 alineatul (1) din acord, comitetul mixt ar trebui să convină asupra unor orientări tehnice pentru a asigura punerea în aplicare corespunzătoare a acordului, inclusiv asupra stabilirii unei legături robuste și securizate între SSTL și EUTL. Orientările tehnice pot fi elaborate de un grup de lucru instituit în temeiul articolului 12 alineatul (5) din acord. Grupul de lucru ar trebui să-i aibă în componența sa cel puțin pe administratorul registrului elvețian și pe administratorul central al Uniunii și ar trebui să sprijine comitetul mixt în exercitarea funcțiilor sale în conformitate cu articolul 13 din acord.

(8) Având în vedere caracterul tehnic al orientărilor și necesitatea adaptării acestora la evoluțiile actuale, orientările tehnice elaborate de administratorul registrului elvețian și de administratorul central al Uniunii ar trebui să fie transmise comitetului mixt pentru informare sau, după caz, pentru aprobare,

([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 (JO L 314, 29.9.2020, p. 68).

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În partea B punctul 17 din anexa I la acord, al doilea paragraf se înlocuiește cu următorul text:

„Operatorii de aeronave atribuiți Elveției pentru prima dată după intrarea în vigoare a prezentului acord sunt administrați de Elveția după data de 30 aprilie a anului atribuirii și după ce legătura provizorie dintre registre devine funcțională."

Articolul 2

Al patrulea paragraf din anexa II la acord se înlocuiește cu următorul text:

„În standardele tehnice de creare a legăturii se stabilește că toate comunicările dintre SSTL și EUTL constau în schimburi securizate de mesaje prin servicii web, pe baza următoarelor tehnologii (*) sau a unor tehnologii echivalente:

— servicii web care utilizează protocolul Simple Object Access Protocol (SOAP);

— rețea privată virtuală (VPN) bazată pe hardware;

— limbaj de marcare extensibil (XML);

— semnătură digitală; și

— protocoale de sincronizare a ceasului în rețea.

_____

(*) Aceste tehnologii sunt utilizate în prezent pentru stabilirea unei legături între registrul Uniunii și Registrul internațional al tranzacțiilor, precum și între registrul elvețian și Registrul internațional al tranzacțiilor."

Articolul 3

Se adoptă standardele tehnice de creare a legăturii (LTS), astfel cum sunt anexate la prezenta decizie.

Articolul 4

Se instituie, prin prezenta decizie, un grup de lucru în temeiul articolului 12 alineatul (5) din acord. Acesta sprijină comitetul mixt pentru asigurarea punerii în aplicare corespunzătoare a acordului, inclusiv la elaborarea orientărilor tehnice pentru punerea în aplicare a standardelor tehnice de creare a legăturii.

Grupul de lucru îi are în componența sa cel puțin pe administratorul registrului elvețian și pe administratorul central al Uniunii.

Articolul 5

Prezenta decizie intră în vigoare la data adoptării sale.

Adoptată la Bruxelles, 5 noiembrie 2020.

Pentru comitetul mixt	Președintele	Secretarul pentru Elveția
Secretarul pentru Uniunea Europeană	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

ANEXĂ

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 O SOLUȚIE PROVIZORIE

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 în cadrul EU ETS sau al ETS-ului Elveției.
CH	Confederația Elvețiană
CHU	Certificate generale elvețiene (termenul „CHU2” este utilizat ca abreviere pentru certificatele CHU valabile pentru cea de a doua perioadă de angajament)
CHUA	Certificat elvețian pentru aviație
COP	Procedeele comune de funcționare elaborate în comun de părțile la acord pentru activarea legăturii dintre EU ETS și ETS-ul Elveției.
ETR	Registru de comercializare a certificatelor de emisii
ETS	Sistemul 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
Registru	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
Tranzacție	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.

Acronim	Definiție
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 activarea legăturii dintre EU ETS și ETS-ul Elveției, este instituită, înainte de mai 2020 sau cât mai curând posibil după această dată, o soluție provizorie. Părțile cooperează pentru a înlocui în cel mai scurt timp posibil soluția provizorie cu o legătură permanentă între registre (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.

Standardele tehnice de creare a legăturii, astfel cum sunt specificate în prezentul document, urmează să fie adoptate prin Decizia nr. 2/2020 a comitetului mixt. În conformitate cu prezenta decizie, comitetul mixt solicită administratorului registrului elvețian și administratorului central al Uniunii să elaboreze orientări tehnice suplimentare pentru activarea legăturii și să se asigure 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 o funcționare 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 (COP), 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 acestei 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 între registre, au fost luate toate măsurile pentru crearea unei arhitecturi robuste. Cu toate că legătura permanentă prevăzută între registre se va baza pe servicii web, soluția provizorie va utiliza, în schimb, un mecanism de schimb de fișiere.

Soluția tehnică utilizează:

— un protocol de transfer securizat pentru schimburile de mesaje;

— mesaje XML;

— semnătură digitală și criptare bazate pe XML;

— aparat VPN sau o rețea echivalentă de transport de date securizată.

3.1.1. Schimbul de mesaje

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

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

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

Erorile și evenimentele neașteptate vor fi 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 de test.

Fiecare mesaj conține un antet care include:

— sistemul ETS de origine;

— numărul de secvență.

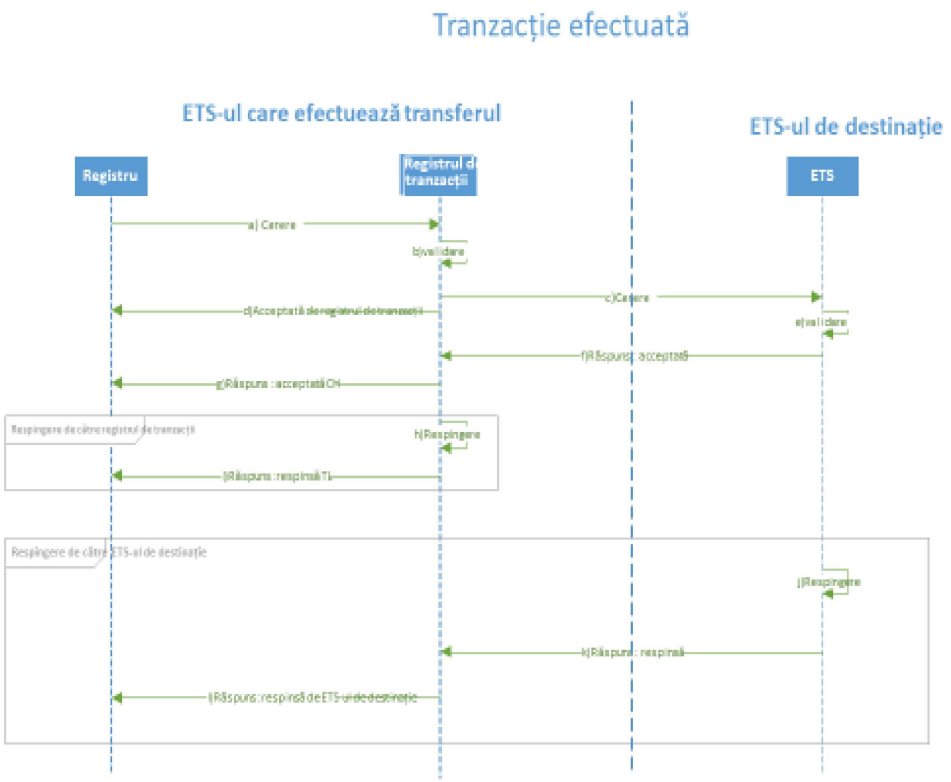
3.1.3. Ferestre de ingerare (Ingestion Windows)

Soluția provizorie 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. Diagrama de secvență de mai sus prezintă toate fluxurile specifice ale tranzacțiilor efectuate.

Fluxul principal „Tranzacție normală” (cu etapele indicate în imaginea 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.

Fluxul alternativ „Respingere de către registrul de tranzacții” [cu etapele indicate în imaginea de mai sus, începând, de asemenea, cu etapa de la litera (a)]:

(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).

Urmată de:

(b) Registrul de tranzacții nu validează cererea.

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

Fluxul alternativ „Respingere de către ETS” [cu etapele indicate în imaginea de mai sus, începând cu etapa descrisă la litera (a)]:

(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.

Urmată de:

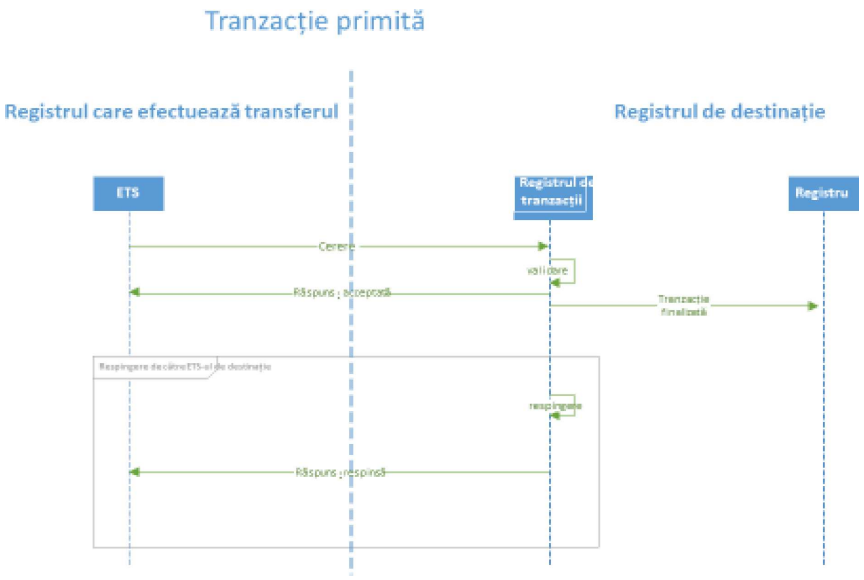
(e) Registrul de tranzacții din cadrul ETS-ului de destinație nu validează tranzacția.

(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

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 transferul Propunerea de tranzacție pentru ETS-ul de destinație;

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

  — Acceptată: 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 va fi setat la „încheiată” în cadrul ETS-ului de destinație pentru orice tranzacție rămasă 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 sau o rețea echivalentă de transport de date securizată;

(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 de transport de date securizate. În cazul unei rețele virtuale private (VPN), infrastructura ar trebui să se bazeze pe hardware sau pe aparate virtuale. 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.

Orice altă soluție echivalentă trebuie să respecte principiile menționate mai sus.

3.2.3. Implementarea IPSec

În cazul utilizării unei soluții VPN, 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

Soluția provizorie 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 sau al unor rețele echivalente de transport securizat de date. 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 de test care vor permite implementarea monitorizării 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 după efectuarea fiecărei operațiuni 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 de test

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

3.4. *Standarde pentru serviciile web*

Serviciile web nu vor fi utilizate în cadrul soluției provizorii. Se poate remarca însă faptul că forma și formatul mesajelor XML vor rămâne în mare măsură neschimbate. Odată cu introducerea în viitor a legăturii permanente între registre, serviciile web ar trebui să permită schimbul de mesaje XML în timp real.

3.5. *Definiția specifică serviciilor web*

Această secțiune nu se aplică pentru soluția provizorie. Astfel cum s-a menționat în secțiunea anterioară, serviciile web vor fi utilizate doar în cadrul viitoarei legături permanente între registre.

3.6. *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 aceste registre 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 pot fi preluate sau accesate într-o perioadă rezonabilă.

Registrele de tranzacții

Subsistemele EUTL și SSTL conțin 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 soluției provizorii, mesajele de reconciliere constituie o parte integrantă a mesajelor transmise.

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 dovezi ale 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 arhivate și certificatele aferente.

Aceste fișiere 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.

3.7. *Cerințele operaționale*

Schimbul de date între cele două sisteme nu este complet autonom în cadrul soluției provizorii, ceea ce înseamnă că este nevoie de operatori și de proceduri pentru activarea legăturii.

4. **Dispoziții privind disponibilitatea**

4.1. *Proiectarea disponibilității comunicațiilor*

Arhitectura soluției provizorii este în esență o infrastructură și un software TIC care permite comunicarea între ETS-ul Elveției și EU ETS. Asigurarea unor niveluri ridicate de disponibilitate, integritate și confidențialitate a acestui flux de date devine astfel un aspect esențial de luat în considerare pentru proiectarea soluției provizorii și a 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 provizorie instituie o rețea VPN rezilientă (sau o rețea echivalentă) 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 cadrul soluției provizorii, schimburile de date între părți se realizează la intervale de timp predefinite pe tot parcursul anului. 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 semnificative pentru efectuarea fiecărei etape;

— modulele software pentru soluția provizorie 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 soluției provizorii 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 soluția provizorie 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

Aceste teste trebuie efectuate și/sau verificate individual de către ambele părți 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

Aceste teste sunt declanșate individual de oricare dintre părți, iar 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 (sau rețeaua de transport securizată echivalentă) 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 ambele părți 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, legătura provizorie poate fi considerată funcțională.

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 legăturii provizorii 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 din 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 este menit să fie utilizat pentru a efectua teste de integrare de către ambele părți.

Cu excepția VPN (sau a unei rețele echivalente), 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 prezentarea VPN, acesta este configurată în două medii diferite, unul pentru PROD și altul independent pentru ACC și TEST.

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 3.1, „Arhitectura legăturii de comunicare").

Infrastructura de testare trebuie separată de cea de producție, atât la nivel de rețea, cât și la nivel de infrastructură. Testele de securitate necesare pentru a verifica respectarea cerințelor de securitate se efectuează în cadrul infrastructurii de testare.

5.2. *Dispoziții privind suspendarea și reactivarea legăturii*

În cazul în care există suspiciunea că securitatea registrului elvețian, a SSTL, a registrului Uniunii sau a EUTL a fost compromisă, oricare dintre părți o informează imediat pe cealaltă și suspendă legătura dintre SSTL și EUTL.

Procedurile privind schimbul de informații, privind decizia de suspendare și privind decizia 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, întreținerea), 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 a suspenda legătura între registre, indiferent dacă este planificată sau neplanificată, se va lua conform procedurii de gestionare a modificărilor sau de gestionare a incidentelor de securitate prevăzută în procedeele comune de funcționare.

Reactivarea comunicării

Decizia de a reactiva legătura 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 legate direct de încălcarea securității vor fi considerate sensibile, marcate ca „ETS CRITICAL” (informații ETS deosebit de sensibile) și gestionate conform instrucțiunilor de gestionare, cu excepția cazului în care se specifică altfel.

Fiecare încălcare a securității va fi gestionată conform secțiunii „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 testarea securității 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. Testarea se efectuează pe baza metodei descrise în secțiunea 5.4.1, 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 „ETS CRITICAL”, în conformitate cu instrucțiunile de gestionare.