РЕШЕНИЕ № 2/2020 НА СЪВМЕСТНИЯ КОМИТЕТ, СЪЗДАДЕН СЪГЛАСНО СПОРАЗУМЕНИЕТО МЕЖДУ ЕВРОПЕЙСКИЯ СЪЮЗ И КОНФЕДЕРАЦИЯ ШВЕЙЦАРИЯ ЗА СВЪРЗВАНЕ НА ТЕХНИТЕ СИСТЕМИ ЗА ТЪРГОВИЯ С ЕМИСИИ НА ПАРНИКОВИ ГАЗОВЕ

от 5 ноември 2020 година

за изменение на приложения I и II към споразумението и приемане на Технически стандарти за свързването (LTS) [2021/1034]

СЪВМЕСТНИЯТ КОМИТЕТ,

като взе предвид Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове ([1]) (наричано по-нататък „споразумението“), и по-специално член 3, параграф 7 и член 13, параграф 2 от него,

като има предвид, че:

1) С Решение № 2/2019 на Съвместния комитет от 5 декември 2019 г. ([2]) бяха изменени приложения I и II към споразумението и по този начин бяха удовлетворени условията за свързване, посочени в споразумението.

2) След приемането на Решение № 2/2019 на Съвместния комитет и в съответствие с член 21, параграф 3 от споразумението страните размениха своите инструменти за ратифициране или одобрение, тъй като считат, че всички условия за свързване, предвидени в споразумението, са изпълнени.

3) В съответствие с член 21, параграф 4 от споразумението то влезе в сила на 1 януари 2020 г.

4) Приложение I към споразумението следва да бъде изменено в съответствие с член 13, параграф 2 от споразумението, за да се осигури плавният преход в администрирането на оператори на въздухоплавателни средства, което е разпределено на Швейцария за първи път, като се вземе предвид постигнатият напредък по създаването на връзката между регистрите.

5) С цел да се вземат предвид последните тенденции и да се гарантира по-голяма степен на гъвкавост за създаването на изискваната от споразумението връзка между регистрите, приложение II към споразумението следва да бъде изменено в съответствие с член 13, параграф 2 от него, за да се осигури по-широк, но еквивалентен набор от технологии за изграждане на въпросната връзка между регистрите.

6) Съгласно член 3, параграф 7 от споразумението администраторът на Швейцарския регистър и централният администратор за Съюза следва да изготвят Технически стандарти за свързването (LTS), базиращи се на принципите, определени в приложение II към споразумението. В LTS следва да бъдат описани подробните изисквания за установяването на надеждна и защитена връзка между Швейцарския допълнителен дневник за трансакциите (SSTL) и Дневника на ЕС за трансакциите (EUTL). LTS следва да пораждат действие след приемането им с решение на Съвместния комитет.

7) В съответствие с член 13, параграф 1 от споразумението Съвместният комитет следва да постигне съгласие по технически насоки, за да осигури правилното изпълнение на споразумението, включително установяването на надеждна и защитена връзка между SSTL и EUTL. Техническите насоки може да бъдат разработени от работна група, учредена съгласно член 12, параграф 5 от споразумението. Работната група следва да включва най-малко администратора на Швейцарския регистър и централния администратор на Съюза и следва да подпомага Съвместния комитет във функциите му съгласно член 13 от споразумението.

8) С оглед на техническия характер на насоките и необходимостта от адаптирането им към текущите новости, техническите насоки, разработени от администратора на Швейцарския регистър и централния администратор за Съюза, следва да се предоставят на Съвместния комитет за информация или, когато е целесъобразно, за одобрение,

([1]) ОВ L 322, 7.12.2017 г., стр. 3.

([2]) Решение № 2/2019 на Съвместния комитет, създаден съгласно Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове от 5 декември 2019 година за изменение на приложения I и II към Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове (ОВ L 314, 29.9.2020 г., стр. 68).

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Вторият параграф от точка 17 в част Б от приложение I към споразумението се заменя със следния текст:

„Операторите на въздухоплавателни средства, които са разпределени за пръв път на Швейцария след влизането в сила на настоящото споразумение, се администрират от Швейцария с начална дата след 30 април от годината на разпределяне и след като временната връзка между регистрите започне да функционира.“.

Член 2

Четвъртата алинея от приложение II към споразумението се заменя със следния текст:

„В LTS трябва да е посочено, че комуникациите между SSTL и EUTL се състоят от защитен обмен на съобщения за уебуслуги на базата на посочените по-долу технологии (*) или еквивалентни на тях:

— уебуслуги с използване на Simple Object Access Protocol (SOAP, протокол за обмен на структурирана информация в компютърни мрежи);

— базирана на хардуер виртуална частна мрежа (VPN);

— XML (Разширяем маркиращ език);

— електронен подпис; както и

— времеви мрежови протоколи.

(*) Тези технологии се използват понастоящем за установяване на връзка между Регистъра на Съюза и Дневника за международни трансакции, както и между Швейцарския регистър и Дневника за международни трансакции.“

Член 3

Приемат се Техническите стандарти за свързването (LTS), приложени към настоящото решение.

Член 4

С настоящото се учредява работна група съгласно член 12, параграф 5 от споразумението. Тя подпомага Съвместния комитет, за да осигурява правилното изпълнение на споразумението, включително при разработването на технически насоки за изпълнение на Техническите стандарти за свързването.

Работната група включва най-малко администратора на Швейцарския регистър и централния администратор на Съюза.

Член 5

Настоящото решение влиза в сила в деня на неговото приемане.

Съставено в Брюксел на 5 ноември 2020 година.

За Съвместния комитет	Председател	Секретар за Швейцария
Секретар за Европейския съюз	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

ПРИЛОЖЕНИЕ

Технически стандарти за свързването (lts) съгласно член 3, параграф 7 от Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове

СТАНДАРТИ ЗА ВРЕМЕННО РЕШЕНИЕ

1. **Речник на термините**

Таблица 1-1

Съкращения и определения, свързани с работния процес

Съкращение/Термин	Определение
Квота	Квота за отделяне на един тон еквивалент на въглероден диоксид в рамките на определен период, която е валидна единствено за целите на изпълнение на изискванията съгласно СТЕ на ЕС или на СТЕ на Швейцария.
CH	Конфедерация Швейцария
CHU	Обичайни квоти на Швейцария (терминът „CHU2“ се използва като съкращение за обичайните квоти на Швейцария за втория период на задължения)
CHUA	Квоти за авиационни емисии на Швейцария
ОРП	Общи работни процедури, разработени съвместно от страните по споразумението, за привеждането в действие на връзката между СТЕ на ЕС и СТЕ на Швейцария.
ETR	Регистър за търговия с емисии
СТЕ	Система за търговия с емисии
ЕС	Европейски съюз
EUA	Обичайни квоти на ЕС
EUAA	Квоти за авиационни емисии на ЕС
EUCR	Консолидиран регистър на Европейския съюз
EUTL	Дневник на ЕС за трансакциите
Регистър	Система за отчитане на квотите, издадени в рамките на СТЕ, с която собствеността на квотите се проследява по електронен път.
SSTL	Швейцарски допълнителен дневник за трансакциите
Трансакция	Процес в регистър, който включва прехвърлянето на квоти от една партида към друга.
Система за дневник за трансакциите	Дневникът за трансакциите съдържа запис на всяка предложена трансакция, изпратена от единия регистър към другия.

Таблица 1-2

Съкращения и определения в техническата област

Съкращение	Определение
Асиметрична криптография	Използва частни и публични ключове за криптиране и декриптиране на данни.
Сертифициращ орган (СО)	Субект, който издава електронни сертификати.

Съкращение	Определение
Криптографски ключ	Информация, която определя функционалните изходящи данни от криптографския алгоритъм.
Декриптиране	Обратният процес на криптиране.
Цифров подпис	Математическа техника, използвана за потвърждаване на автентичността и интегритета на съобщение, софтуер или цифров документ.
Криптиране	Процесът на преобразуване на информация или данни в код, особено с цел предотвратяване на неупълномощен достъп.
Постъпване на файл	Процесът на четене на даден файл.
Защитна стена	Устройство или софтуер за мрежова сигурност, които проследяват и контролират входящия и изходящия мрежов трафик въз основа на предварително определени правила.
Мониторинг на синхронизацията (heartbeat)	Периодичен сигнал, генериран и наблюдаван от хардуер или софтуер с цел указване на нормална експлоатация или синхронизиране на други части на компютърна система.
IPSec	Интернет протокол за сигурност (IP SECurity). Пакет от мрежови протоколи, чрез който се удостоверяват и криптират пакетите от данни, за да се осигури защитена криптирана комуникация между два компютъра в базирана на такива протоколи мрежа.
Изпитване за пробив	Практика на изпитване на компютърна система, мрежа или уеб приложение за откриване на слаби места в сигурността, които атакуващ би могъл да използва.
Процес на съгласуване	Процес на гарантиране, че между два набора от записи има съответствие.
VPN	Виртуална частна мрежа.
XML	Разширяем маркиращ език. Той позволява на разработчиците да създават свои собствени персонализирани етикети, даващи възможност за определяне, предаване, валидиране и тълкуване на данни между приложенията и между организациите.

2. **Въведение**

В Споразумението между Европейския съюз и Конфедерация Швейцария за свързване на техните системи за търговия с емисии на парникови газове от 23 ноември 2017 г. (наричано по-долу „споразумението“) се предвижда взаимно признаване на квотите за емисии, които могат да бъдат използвани за спазване на изискванията по Системата за търговия с емисии на Европейския съюз („СТЕ на ЕС“) със Системата за търговия с емисии на Швейцария („СТЕ на Швейцария“). За да може да функционира връзката между СТЕ на ЕС и СТЕ на Швейцария, ще се създаде директна връзка между Дневника на ЕС за трансакциите (EUTL) към Регистъра на Съюза и Швейцарския допълнителен дневник на трансакциите (SSTL) към Швейцарския регистър, която ще позволи прехвърлянето от регистър до регистър на квоти за емисии, издадени в рамките на всяка от двете СТЕ (член 3, параграф 2 от споразумението). С цел привеждане в действие на свързването на СТЕ на ЕС и СТЕ на Швейцария през май 2020 г. или възможно най-скоро след това се въвежда временно решение. Страните си сътрудничат, за да заменят възможно най-скоро временното решение с постоянна връзка между регистрите (приложение II към споразумението).

Съгласно член 3, параграф 7 от споразумението администраторът на Швейцарския регистър и централният администратор на Съюза изготвят Технически стандарти за свързването (LTS), базиращи се на определените в приложение II принципи, в които стандарти трябва да бъдат описани подробни изисквания за установяването на надеждна и защитена връзка между SSTL и EUTL. Изготвените от администраторите LTS пораждат действие след приемането им с решение на Съвместния комитет.

Посочените в настоящия документ LTS следва да бъдат приети от Съвместния комитет с Решение № 2/2020 на Съвместния комитет. В съответствие с настоящото решение Съвместният комитет отправя искане до администратора на Швейцарския регистър и централния администратор за Съюза да разработят допълнителни технически насоки за привеждане в действие на връзката и да гарантират, че те постоянно се адаптират към техническия прогрес и новите изисквания, свързани с безопасността и сигурността на връзката и нейното ефективно и ефикасно функциониране.

2.1. *Обхват*

В настоящия документ е изложена общата договореност между страните по споразумението във връзка с установяването на техническите основи за връзката между регистъра на СТЕ на ЕС и регистъра на СТЕ на Швейцария. Въпреки че в него са очертани основните параметри за техническите спецификации по отношение на изискванията към архитектурата, услугите и сигурността, за привеждането в действие на връзката ще са необходими допълнителни подробни насоки.

За нейното правилно функциониране ще бъдат необходими съответни процеси и процедури за по-нататъшното ѝ привеждане в действие. Съгласно член 3, параграф 6 от споразумението тези въпроси са описани подробно в самостоятелен документ за Общи работни процедури (ОРП), който трябва да бъде приет отделно с решение на Съвместния комитет.

2.2. *Адресати*

Адресати на настоящия документ са администраторът на Швейцарския регистър и централният администратор на Съюза.

3. **Общи разпоредби**

3.1. *Архитектура на комуникационната връзка*

Целта на настоящия раздел е да предостави описание на цялостната архитектура на привеждането в действие на връзката между СТЕ на ЕС и СТЕ на Швейцария и различните компоненти, които я изграждат.

Тъй като сигурността е ключов елемент за определянето на архитектурата на връзката между регистрите, са предприети всички мерки за изграждане на надеждна архитектура. Въпреки че предвидената постоянна връзка между регистрите ще се основава на уеб услуги, вместо това за временното решение ще се използва механизъм за обмен на файлове.

В техническите решения се използват:

— протокол за прехвърляне за защитен обмен на съобщения;

— XML съобщения;

— XML базиран цифров подпис и криптиране;

— VPN устройство или еквивалентна мрежа за защитен пренос на данни.

3.1.1. Обмен на съобщения

Комуникацията между Регистъра на ЕС и Швейцарския регистър ще се основава на механизъм за обмен на съобщения чрез защитени канали. Всеки край ще разчита на собствено хранилище на получени съобщения.

Двете страни ще водят регистър на получените съобщения, заедно с подробностите за обработката.

Ако възникнат грешки или неочаквано състояние, те трябва да се докладват като предупреждения, както и да се осъществи човешки контакт между екипите за поддръжка.

Грешките и неочакваните събития ще бъдат разглеждани при спазване на работните процедури, установени в процеса на управление на инциденти от ОРП.

3.1.2. XML съобщение — описание на високо равнище

XML съобщението съдържа един от следните елементи:

— една или няколко заявки за трансакции и/или един или няколко отговора на заявки за трансакции;

— една операция/отговор, свързан(а) със съгласуването;

— едно тестово съобщение.

Всяко съобщение съдържа заглавна част със следните елементи:

— СТЕ на произход;

— пореден номер.

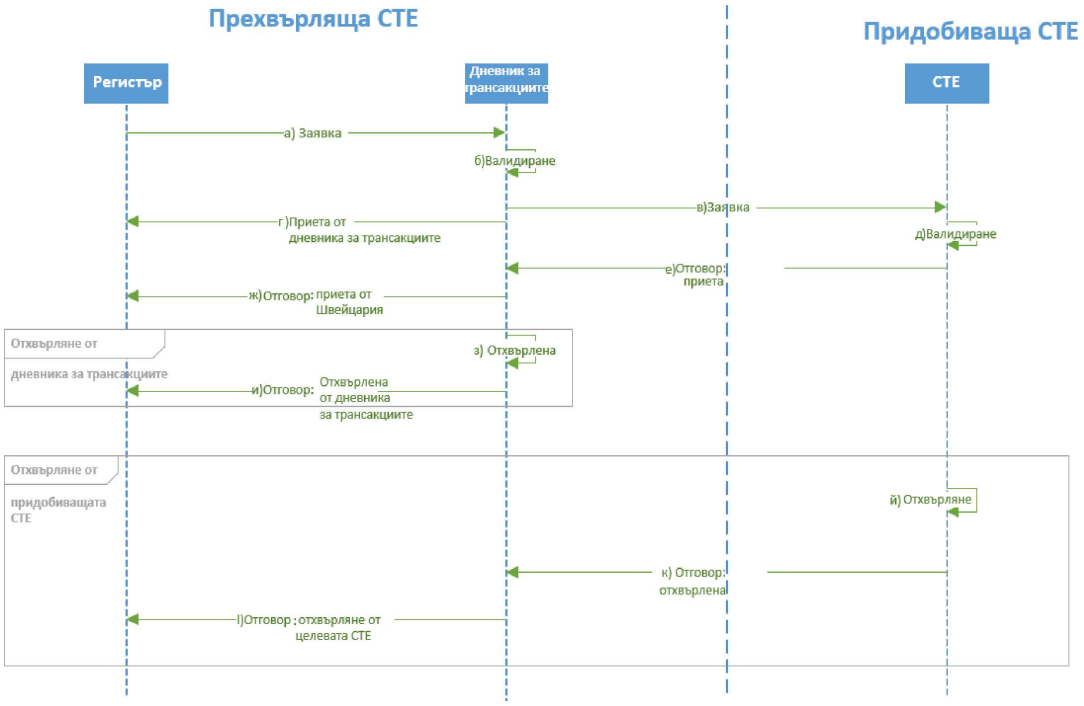
3.1.3. Периоди за постъпване

Временното решение се основава на предварително определени периоди за постъпване, които са последвани от поредица от определени събития. Заявките за трансакции, получени чрез връзката, ще постъпват само на предварително определени интервали от време. Времевите промеждутъци, в които постъпват заявките, включват техническо валидиране на изходящите и входящите трансакции. В допълнение, съгласуването може да се извършва ежедневно и може да се задейства ръчно.

Промените в честотата и/или времето на провеждане на тези събития ще се разглеждат при спазване на работните процедури, установени в процеса на изпълнение на заявката от ОРП.

3.1.4. Потоци от съобщения за трансакции

Изходящи трансакции



Това отразява гледната точка на прехвърлящата СТЕ. На диаграмата на последователността по-горе са изобразени всички потоци от изходящи трансакции.

Основен поток „Нормална трансакция“ (включващ стъпките, посочени на чертежа по-горе):

а) в рамките на прехвърлящата СТЕ заявката за трансакция се изпраща от регистъра към дневника за трансакциите, след като изтекат всички обичайни работни срокове на изчакване (24 часа изчакване, където е приложимо).

б) дневникът за трансакциите валидира заявката за трансакция;

в) заявката за трансакция се изпраща до целевата СТЕ;

г) отговорът за приемане се изпраща до регистъра на СТЕ на произход;

д) целевата СТЕ валидира заявката за трансакция;

е) целевата СТЕ изпраща обратно отговора за приемане до дневника за трансакциите на СТЕ на произход;

ж) дневникът за трансакциите изпраща отговора за приемане до регистъра.

Алтернативен поток „Отхвърляне от дневника за трансакциите“ (включващ стъпките, посочени на схемата по-горе, като се започва по същия начин от буква а):

а) в рамките на СТЕ на произход заявката за трансакция се изпраща от регистъра до дневника за трансакциите, след като изтекат всички обичайни работни срокове на изчакване (24 часа изчакване, където е приложимо);

след това:

б) дневникът за трансакциите не валидира заявката;

в) съобщението за отхвърляне се изпраща до регистъра на произход.

Алтернативен поток „Отхвърляне от СТЕ“ (включващ стъпките, посочени на схемата по-горе, като се започва по същия начин от буква а):

а) в рамките на СТЕ на произход заявката за трансакция се изпраща от регистъра до дневника за трансакциите, след като изтекат всички обичайни работни срокове на изчакване (24 часа изчакване, където е приложимо);

б) дневникът за трансакциите валидира трансакцията;

в) заявката за трансакция се изпраща до целевата СТЕ;

г) съобщението за приемане се изпраща до регистъра на СТЕ на произход.

след това:

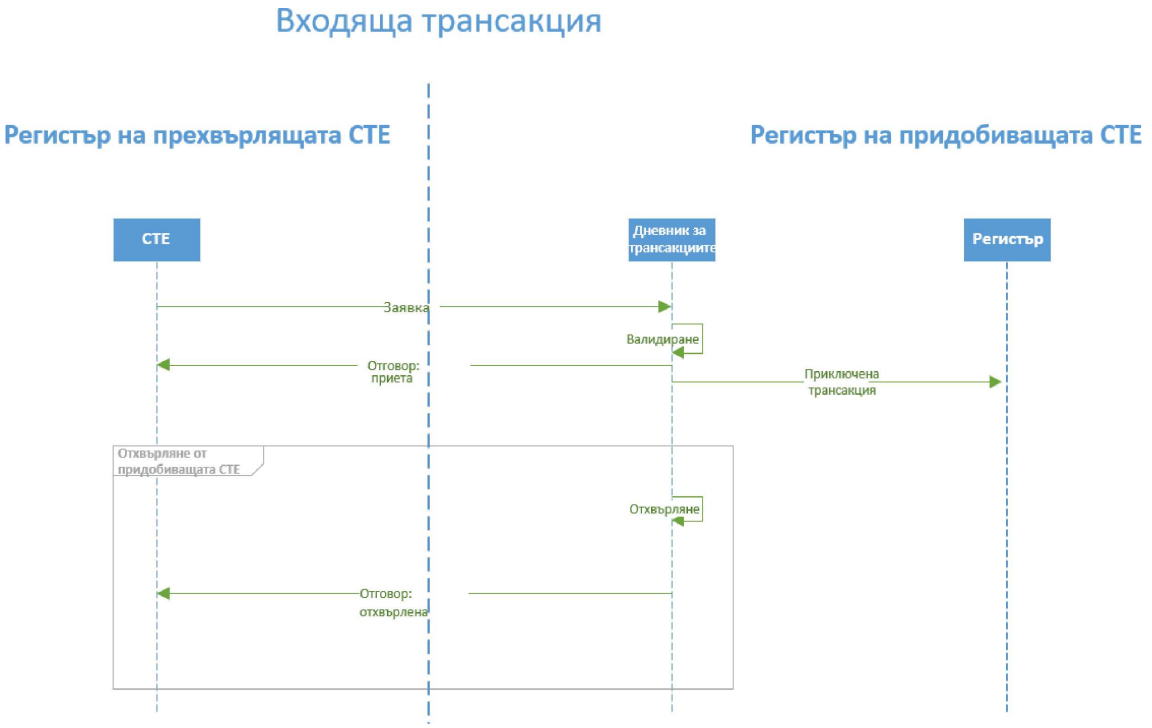
д) дневникът за трансакциите на придобиващата СТЕ не валидира трансакцията;

е) придобиващата СТЕ изпраща отговора за отказ до дневника за трансакциите на прехвърлящата СТЕ;

ж) дневникът за трансакциите изпраща отказа до регистъра.

Входящи трансакции

Това отразява гледната точка на придобиващата СТЕ. Конкретният поток е изобразен в диаграмата на последователността по-долу.



На диаграмата е показано, че:

1. Когато дневникът за трансакциите на придобиващата СТЕ валидира заявката, той изпраща съобщението за приемане до прехвърлящата СТЕ, както и съобщение за „изпълнена трансакция“ до регистъра на придобиващата СТЕ;

2. Когато дневникът за трансакциите на придобиващата СТЕ откаже входящата заявка, заявката за трансакция не се изпраща до регистъра на придобиващата СТЕ.

Протокол

Цикълът на съобщенията за трансакция включва само две съобщения:

— прехвърлящата СТЕ предложение за трансакция за придобиващата СТЕ;

— придобиващата СТЕ отговор на заявка за трансакция на прехвърлящата СТЕ: приета или отхвърлена (включително причината за отхвърлянето):

  — приета: трансакцията е изпълнена;

  — отхвърлена: трансакцията е прекратена.

Състояние на трансакцията:

— когато заявката бъде изпратена, състоянието на трансакцията в прехвърлящата СТЕ ще се определи като „предложена“;

— когато заявката бъде получена и в хода на разглеждането ѝ, състоянието на трансакцията в придобиващата СТЕ ще се определи като „предложена“;

— когато предложението бъде обработено, състоянието на трансакцията в придобиващата СТЕ ще се определи като „изпълнена“/„прекратена“. След това придобиващата СТЕ ще изпрати съответното съобщение за приемане/отхвърляне;

— когато приемането/отхвърлянето бъде получено и обработено, състоянието на трансакцията в прехвърлящата СТЕ ще се определи като „изпълнена“/„прекратена“;

— в случай че не бъде получен отговор, състоянието на трансакцията в прехвърлящата СТЕ ще продължи да бъде „предложена“;

— трансакцията в придобиващата СТЕ ще се определи като „прекратена“, ако предложената трансакция се задържи в състояние „предложена“ повече от 30 минути.

Инцидентите, свързани с трансакции, ще бъдат разглеждани при спазване на работните процедури, установени в процеса на управление на инциденти от ОРП.

3.2. *Сигурност на преноса на данни*

Прехвърляните данни ще подлежат на четири равнища на сигурност:

1) контрол на достъпа до мрежите: защитна стена и равнище на взаимосвързаност на мрежите;

2) криптиране на прехвърлянето на данни: VPN или еквивалентна мрежа за защитен пренос на данни;

3) криптиране на сесии: протокол за прехвърляне за защитен обмен на съобщения;

4) криптиране на приложения: криптиране и подпис на съдържание в XML формат.

3.2.1. Защитна стена и взаимосвързаност на мрежите

Връзката се установява посредством мрежа, защитена от базирана на хардуер защитна стена. Защитната стена се конфигурира с такива правила, според които само „регистрираните“ клиенти могат да правят връзки с VPN сървъра.

3.2.2. Виртуална частна мрежа (VPN)

Всички съобщения между страните са защитени чрез технология за защитен пренос на данни. В случая на виртуална частна мрежа (VPN) инфраструктурата следва да е базирана на хардуерни или виртуални устройства. Технологиите за VPN предоставят възможност чрез мрежа, като интернет, да се изгради „път“ („тунел“) от една точка до друга, като по този начин се защитават всички съобщения. Преди създаването на VPN тунела на бъдеща крайна точка на клиента се издава електронен сертификат, който позволява на клиента да представи доказателство за самоличност по време на договарянето на връзката. Всяка страна отговаря за инсталирането на сертификата на своята крайна точка в рамките на VPN. Като използва електронни сертификати, всеки краен VPN сървър ще има достъп до централен орган за договаряне на идентификационни данни. По време на процеса на създаване на тунел се договаря криптиране, което да гарантира, че всички съобщения през тунела са защитени.

Крайните точки на клиентите в рамките на VPN са конфигурирани така, че VPN тунелът да се поддържа постоянно, за да се даде възможност за непрекъсната надеждна двупосочна комуникация в реално време между страните.

Всяко друго еквивалентно решение е в съответствие с горепосочените принципи.

3.2.3. Прилагане на протокол IPsec

В случай на VPN решение използването на протокола IPSec за изграждане на инфраструктура „сайт-към-сайт VPN“ ще осигури удостоверяване на автентичността на равнище сайт-към-сайт, интегритет на данните и криптиране на данните. Конфигурациите на IPsec VPN гарантират правилното удостоверяване на автентичността между две крайни точки в рамките на VPN връзката. Страните ще идентифицират и удостоверяват автентичността на отдалечения клиент чрез IPSec връзка с помощта на електронни сертификати, предоставени от сертифициращ орган, който е признат от другата крайна точка.

IPsec осигурява също интегритета на данните за всички съобщения, преминаващи през VPN тунела. Пакетите данни се хешират и подписват, като се използва информацията за удостоверяване на автентичността, установена чрез VPN. Поверителността на данните отново се осигурява, като се дава възможност за IPSec криптиране.

3.2.4. Протокол за прехвърляне за защитен обмен на съобщения

Временното решение се основава на множество равнища на криптиране, за да може обменът на данни между страните да се осъществява по сигурен начин. Двете системи и техните различни среди са взаимосвързани на мрежово равнище посредством VPN тунели или еквивалентни мрежи за защитен пренос на данни. В приложенията файловете се прехвърлят чрез протокол за прехвърляне за защитен обмен на съобщения на равнище сесия.

3.2.5. XML криптиране и подпис

В рамките на XML файлове подписването и криптирането се извършват на две равнища. Всяка заявка за трансакция, отговор на заявка за трансакция и съобщение за съгласуване се подписват поотделно по електронен път.

Като втора стъпка, всеки поделемент на „съобщението“ се криптира поотделно.

Освен това, като трета стъпка и за да се гарантират интегритетът и невъзможността за отричане на цялото съобщение, основният елемент се подписва с цифров подпис. Това води до високо равнище на защита на вградените XML данни. При техническото изпълнение се спазват стандартите на Консорциума на световната мрежа.

За да се декриптира и провери съобщението, процесът се извършва в обратен ред.

3.2.6. Криптографски ключове

За криптирането и подписването ще се използва криптография с публични ключове.

В конкретния случай на IPSec се използва електронен сертификат, издаден от сертифициращ орган (СО), на който се доверяват и двете страни. Този СО проверява самоличността на притежателя на сертификата и издава сертификати, които се използват за положително идентифициране на организация и създаване на защитени канали за комуникация между страните.

За подписването и криптирането на каналите за комуникация и файловете с данни се използват криптографски ключове. Публичните сертификати се обменят от страните по електронен път, като се използват защитени канали и се проверяват по различен от обичайния канал за връзка начин (out-of-band). Тази процедура е неразделна част от процеса за управление на информационната сигурност от ОРП.

3.3. *Списък на функциите в рамките на връзката*

Връзката определя преносната система за поредица от функции, с помощта на които се изпълняват работните процеси, произтичащи от споразумението. Връзката включва също и спецификацията за процеса на съгласуване и за тестовите съобщения, които ще дадат възможност за прилагане на мониторинг на синхронизацията („heartbeat“).

3.3.1. Трансакции в работния процес

От гледна точка на работния процес във връзката са предвидени четири вида заявки за трансакции.

— Външно прехвърляне

  — след влизането в сила на свързването на СТЕ, квотите на ЕС и на Швейцария са заменяеми и по този начин могат да се прехвърлят изцяло между страните,

— прехвърляне на квоти, изпратено чрез връзката, ще включва прехвърляща партида в едната СТЕ и придобиваща партида в другата СТЕ,

— прехвърлянето може да включва всякакви количества от четирите (4) вида квоти:

— обичайни квоти на Швейцария (CHU);

— квоти за авиационни емисии на Швейцария (CHUA);

— обичайни квоти на ЕС (EUA);

— квоти за авиационни емисии на ЕС (EUAA).

— Международно предоставяне

Операторите на въздухоплавателни средства, администрирани от една СТЕ, със задължения по другата СТЕ и имащи право да получават безплатни квоти от тази втора СТЕ, ще получат безплатни квоти за авиационни емисии от втората СТЕ посредством трансакцията за международно предоставяне.

— Отменяне на международното предоставяне

Тази трансакция ще се извършва в случай че безплатните квоти, предоставени на оператор на въздухоплавателно средство, който е обект на другата СТЕ, трябва да бъдат изцяло отменени.

— Връщане на излишни предоставени квоти

Подобно на отмяната, но когато не е необходима пълна отмяна на предоставените квоти, а само излишните предоставени квоти трябва да бъдат върнати на предоставящата СТЕ.

3.3.2. Протокол за съгласуване

Съгласуването ще се извършва едва след като приключат периодите за постъпване, валидиране и обработване на съобщения.

Съгласуването е неразделна част от мерките за сигурност и съгласуваност на свързването. Двете страни ще се споразумеят относно точния момент на съгласуване, преди да изготвят график. Може да се извършва ежедневно планирано съгласуване, ако бъде договорено от двете страни. След всяко постъпване на съобщение ще се извършва най-малко едно планирано съгласуване.

Във всеки случай всяка от страните може по всяко време да започне ръчно съгласуване.

Промените във времетраенето и честотата на планираното съгласуване ще се разглеждат при спазване на работните процедури, установени в процеса на изпълнение на заявката от ОРП.

3.3.3. Тестово съобщение

Предвижда се тестово съобщение с цел изпитване на комуникацията от край до край. Съобщението ще съдържа данни, които ще го идентифицират като тестово и ще получите отговор, след като другата страна получи съобщението.

3.4. *Стандарти за уеб услуги*

Във временното решение няма да се използват уеб услуги. Важно е да се отбележи обаче, че формата и форматът на XML съобщенията ще останат до голяма степен непроменени. С въвеждането на постоянната връзка между регистрите в бъдеще, уеб услугите следва да предоставят възможност за обмен на XML съобщения в реално време.

3.5. *Специфично определение на понятието „уеб услуги“*

Настоящият раздел не се прилага за временното решение. Както е посочено в предходния раздел, уеб услуги ще се използват само в бъдещата постоянна връзка между регистрите.

3.6. *Изисквания за регистриране на данни*

За да се подкрепи потребността и на двете страни да поддържат точна и съгласувана информация и да се осигурят инструменти, които да се използват в процеса на съгласуване с цел отстраняване на несъответствията, и двете страни поддържат четири вида регистри на данни:

— дневници за трансакциите;

— дневници за съгласуване;

— архив на съобщенията;

— дневници за вътрешен одит.

Всички данни в тези регистри се поддържат най-малко три месеца с цел отстраняване на неизправности и тяхното по-нататъшно запазване зависи от приложимото законодателство в областта на одита на всяка страна. Регистрационните файлове, които са на повече от три месеца, могат да бъдат архивирани на сигурно място в независима IT система, при условие че те могат да бъдат намерени или може да бъде получен достъп до тях в разумен срок.

Дневници за трансакциите

Както подсистемите на EUTL, така и подсистемите на SSTL съдържат версии на дневниците за трансакциите.

По-конкретно, в дневниците за трансакциите ще се съхранява запис на всяка предложена трансакция, изпратена до другата СТЕ. Всеки запис съдържа всички полета на съдържанието на трансакцията и последващите резултати от трансакцията (отговора на приемащата СТЕ). В дневниците за трансакциите също така ще се съхранява запис на входящите трансакции, както и на отговора, изпратен до СТЕ на произход.

Дневници за съгласуване

Дневникът за съгласуване съдържа запис на всички съобщения за съгласуване, обменяни между двете страни, включително идентификационния код на съгласуването, удостоверението за време и резултата от съгласуването: статус на съгласуваност „одобрен“ или „несъответствия“. Във временното решение съобщенията за съгласуване са неразделна част от обменените съобщения.

И двете страни регистрират всяка заявка и нейния отговор в дневника за съгласуване. Въпреки че информацията в дневника за съгласуване не се споделя пряко като част от самото съгласуване, може да е необходим достъп до тази информация, за да се отстранят несъответствията.

Архив на съобщенията

От двете страни се изисква да архивират копие от обменяните (изпращани и получавани) данни (XML файловете), независимо дали форматът на тези съобщения или на XML съобщенията е бил правилен.

Основната цел на архива е да се използва при одит, за да има доказателство за това, което е било изпратено до другата страна и получено от нея. В този смисъл заедно с файловете трябва да бъдат архивирани и съответните сертификати.

Тези файлове също така ще предоставят допълнителна информация за отстраняване на неизправности.

Дневник за вътрешен одит

Тези дневници се определят и използват самостоятелно от всяка от страните.

3.7. *Изисквания за привеждане в действие*

При временното решение обменът на данни между двете системи не е напълно самостоятелен, което означава, че то изисква оператори и процедури, за да се приведе връзката в действие.

4. **Разпоредби относно достъпността**

4.1. *Цел на достъпа до комуникация*

Архитектурата за временното решение в основата си представлява инфраструктура за ИКТ и софтуер, чрез които се позволява комуникацията между СТЕ на Швейцария и СТЕ на ЕС. Поради това гарантирането на високи равнища на достъп, интегритет и поверителност на този поток от данни следователно се превръща в съществен аспект, който трябва да бъде взет предвид при проектирането на временното решение и на постоянната връзката между регистрите. Тъй като става въпрос за проект, в който ролята на инфраструктурата за ИКТ, специално разработения софтуер и процесите е неразделна, трябва да бъдат взети предвид и трите елемента, за да се разработи устойчива система.

Устойчивост на инфраструктурата за ИКТ

В главата от настоящия документ относно общите разпоредби се описват подробно градивните елементи на архитектурата. По отношение на инфраструктурата за ИКТ временното свързване установява устойчива VPN мрежа (или равностойна на нея), която създава сигурни тунели за комуникация, в които може да се извършва обмен на съобщения. Други елементи на инфраструктурата са конфигурирани с висока степен на достъпност и/или разчитат на резервни механизми.

Устойчивост на софтуера, изработен по поръчка

Модулите на разработения по поръчка софтуер повишават устойчивостта чрез повтаряне на комуникацията за определен период от време с другата страна, ако поради някаква причина тя не е достъпна.

Устойчивост на услугите

При временното решение обменът на данни между страните се извършва в предварително определени времеви интервали през цялата година. Някои от стъпките, които са необходими за предварително насрочения обмен на данни, изискват ръчна намеса от страна на операторите на системите и/или администраторите на регистрите. Като се отчита този аспект и за да се увеличат достъпността и успехът на обмена:

— в работните процедури са предвидени значителни времеви интервали за извършване на всяка стъпка;

— в софтуерните модули за временното решение се прилага асинхронна комуникация;

— по време на автоматичния процес на съгласуване ще се установява дали има проблеми с постъпването на файлове с данни в един от двата края;

— процесите на мониторинг (на инфраструктурата за ИКТ и модулите на софтуера, изработен по поръчка) се отчитат и дават началото на процедури за управление на инциденти (както са определени в документа за общите работни процедури). Тези процедури, които имат за цел да намалят времето за възстановяване на нормалното функциониране след инциденти, са от съществено значение, за да се гарантира висока степен на достъпност.

4.2. *План за инициализиране, комуникация, възобновяване и изпитване*

Всички различни елементи, включени в архитектурата на временното решение, преминат през серия от индивидуални и колективни изпитвания, за да се потвърди, че платформата е готова на равнище инфраструктура за ИКТ и информационна система. Тези изпитвания за привеждане в действие са задължителна предпоставка всеки път, когато платформата промени състоянието на временното решение от „временно прекъснато“ на „приведено в действие“.

След това активирането състоянието на привеждане в действие на връзката изисква успешното изпълнение на предварително определен план за изпитване. Това потвърждава, че преди да започне представянето на производствени трансакции между двете страни, всеки регистър първо е извършил набор от вътрешни изпитвания, последвани от валидиране на свързаността от край до край.

В плана за изпитване следва да се упоменат цялостната стратегия за изпитване и подробните данни относно инфраструктурата за изпитване. По-специално за всички елементи от всеки изпитвателен блок планът следва да включва:

— критериите и инструментите за изпитване;

— възложените функции за провеждане на изпитването;

— очакваните резултати (положителни и отрицателни);

— последователността на изпитванията;

— регистрирането на изискванията за резултатите от изпитванията;

— документацията за отстраняване на неизправности;

— разпоредбите относно пренасочването.

Като процес изпитванията за активиране на състоянието на привеждане в действие биха могли да бъдат разделени на четири концептуални градивни елемента или етапи:

4.2.1. Вътрешни изпитвания на инфраструктурата за ИКТ

Тези изпитвания са предназначени да бъдат извършени и/или проверени поотделно от двете страни във всеки край.

Всеки елемент на инфраструктурата за ИКТ във всеки край се изпитва поотделно. Това включва всеки един компонент на инфраструктурата. Тези изпитвания могат да се извършват автоматично или ръчно, но се проверява дали всеки елемент от инфраструктурата е приведен в действие.

4.2.2. Изпитвания на комуникацията

Всяка от страните започва индивидуално тези изпитвания, но приключването им изисква сътрудничество от другия край.

След като отделните елементи са приведени в действие, трябва да бъдат изпитани каналите за комуникация между двата регистъра. За тази цел всяка страна проверява дали достъпът до интернет функционира, дали са създадени VPN тунелите (или еквивалентна защитена преносна мрежа), както и дали има свързване към интернет по протокол IP от сайт към сайт.- След това трябва да се потвърди достижимостта на местните и отдалечени елементи на инфраструктурата и свързването към интернет по протокол IP с другия край.

4.2.3. Изпитвания на цялата система (от край до край)

Тези изпитвания са предназначени за изпълнение във всеки край, а резултатите се споделят с другата страна.

След като бъдат изпитани каналите за комуникация и всички отделни компоненти на двата регистъра, всеки край изготвя серия от симулирани трансакции и съгласуване, представителни за всички функции, които трябва да бъдат изпълнени в рамките на връзката.

4.2.4. Изпитвания на сигурността

Тези изпитвания са предназначени да бъдат извършени и/или започнати от двете страни във всеки край, както е описано подробно в раздели 5.4 „Насоки за изпитване на сигурността“ и 5.5 „Разпоредби относно оценката на риска“.

Едва след като всеки от четирите етапа/градивни елемента приключи с предвидим резултат, временната връзка може да се счита за приведена в действие.

Ресурси за изпитване

Всяка от страните разчита на специфични ресурси за изпитване (специфичен софтуер и хардуер за ИКТ) и разработва функции за изпитване в съответните си системи, за да подкрепи ръчното и постоянно валидиране на платформата. Администраторите на регистри може да изпълняват по всяко време процедурите за ръчно индивидуално или съвместно изпитване. Активирането на състоянието на привеждане в действие само по себе си е ръчен процес.

Също така е предвидено в платформата да се извършват редовни автоматични проверки. Тези проверки са насочени към увеличаване на достъпността на платформата чрез откриване на потенциални проблеми, свързани с инфраструктурата или софтуера. Този план за наблюдение на платформата се състои от два елемента:

— наблюдение на инфраструктурата за ИКТ: и в двата края инфраструктурата ще бъде наблюдавана от доставчиците на услуги в областта на инфраструктурата за ИКТ. Автоматичните изпитвания ще обхващат различните елементи на инфраструктурата и достъпността на каналите за комуникация.

— наблюдение на приложенията: с помощта на софтуерните модули на временното свързване ще се прилага наблюдение на системата за комуникация на равнище приложение (ръчно и/или на редовни интервали от време), което ще изпитва достъпността от край до край чрез симулиране на някои от трансакциите в рамките на връзката.

4.3. *Приемателна/изпитвателна среда*

Архитектурата на Регистъра на Съюза и на Швейцарския регистър се състои от следните три среди:

— производствена (PROD): в тази среда се съдържат действителни данни и се обработват реални трансакции;

— приемателна (ACC): в тази среда се съдържат недействителни или анонимизирани представителни данни. Това е среда, в която операторите на системи от двете страни валидират нови версии;

— изпитвателна (TEST): в тази среда се съдържат недействителни или анонимизирани представителни данни. Тази среда е ограничена до администраторите на регистри и е предназначена да се използва за извършване на интеграционно изпитване от двете страни.

С изключение на VPN (или еквивалентна мрежа), трите среди са напълно независими една от друга, т.е. хардуер, софтуер, бази данни, виртуални среди, IP адреси и портове са създадени и функционират независимо едно от друго.

Що се отнася до структурата на VPN, тя е създадена в рамките на две различни среди — една за PROD, друга, независима за ACC и TEST.

5. **Разпоредби за поверителност и интегритет**

Механизмите и процедурите за сигурност предвиждат принцип на двойната проверка („принцип на четирите очи“) за операциите, които възникват във връзката между Регистъра на Съюза и Швейцарския регистър. Принципът на двойната проверка се прилага, когато е необходимо. Той обаче може да не се прилага за всички стъпки, които предприемат администраторите на регистри.

Изискванията за сигурност се вземат под внимание и се разглеждат в плана за управление на сигурността, който включва също така процеси за разглеждане на инциденти, свързани със сигурността, след евентуално нарушение на сигурността. Оперативната част на тези процеси е описана в ОРП.

5.1. *Инфраструктура за изпитване на сигурността*

Всяка страна се ангажира да създаде инфраструктура за изпитване на сигурността (с помощта на общ набор от софтуер и хардуер, използван при откриването на слаби места по време на етапа на разработване и функциониране):

— отделена от производствената среда;

— когато сигурността се анализира от екип, който е независим от разработването и функционирането на системата.

Всяка страна се ангажира да извършва статичен и динамичен анализ.

В случая на динамичен анализ (като изпитване за пробив) двете страни се ангажират обикновено да ограничават оценките до изпитвателната среда и приемателната средата (както е определено в раздел 4.3 „приемателна среда“ / „изпитвателна среда“). Изключенията от тази политика подлежат на одобрение от двете страни.

Преди да бъде внедрен в производствената среда, всеки софтуерен модул на връзката (както е определен в раздел 3.1 „Архитектура на комуникационната връзка“) трябва да бъде изпитан за сигурност.

Инфраструктурата за изпитване трябва да бъде разделена от инфраструктурата за производство както на равнище мрежа, така и на равнище инфраструктура. Изпитванията на сигурността, необходими за проверка на съответствието с изискванията за сигурност, се провеждат в рамките на инфраструктурата за изпитване.

5.2. *Разпоредби относно временното прекъсване на връзката и възобновяването*

Ако е налице подозрение за компрометиране на сигурността на Швейцарския регистър, на SSTL, на регистъра на Съюза или на EUTL, всяка от страните е длъжна незабавно да уведоми другата страна и да прекъсне временно връзката между SSTL и EUTL.

Процедурите за обмен на информация, за решението за временно прекъсване и за решението за възобновяване са част от процеса на изпълнение на заявката от ОРП.

Временно прекъсване

Временното прекъсване на връзката между регистрите в съответствие с приложение II към споразумението може да се извърши поради:

— административни съображения (например поддръжка), които са планирани;

— съображения, свързани със сигурността (или сривове в ИТ инфраструктурата), които не са били планирани.

В случай на извънредна ситуация всяка от страните уведомява другата страна за това и едностранно временно прекъсва връзката между регистрите.

Ако бъде взето решение за временно прекъсване на връзката между регистрите, то следователно всяка от страните гарантира, че връзката бива прекъсната на равнище мрежа (като блокира части от или всички входящи и изходящи връзки).

Решението за временно прекъсване на връзката между регистрите, независимо дали е планирано, ще бъде взето в съответствие с процедурата за управление на промени или процедурата за управление на инциденти, свързани със сигурността, от ОРП.

Възобновяване на комуникацията

Решението за възобновяване на връзката между регистрите ще бъде взето, както е описано подробно в ОРП и във всеки случай не преди успешното приключване на процедурите за изпитване на сигурността, както е описано подробно в раздели 5.4 „Насоки за изпитване на сигурността“ и 4.2 „План за инициализиране, комуникация, възобновяване и изпитване“.

5.3. *Разпоредби относно нарушение на сигурността*

Нарушението на сигурността се счита за инцидент, свързан със сигурността, който оказва въздействие върху поверителността и интегритета на чувствителна информация и/или работата на системата, в която се тя се обработва.

Чувствителната информация е определена в списъка с чувствителна информация и може да се обработва в системата или в друга свързана с нея част.

Информацията, пряко свързана с нарушението на сигурността, ще се счита за чувствителна, ще бъде маркирана като „ETS CRITICAL“ и ще бъде третирана в съответствие с указанията за боравене с чувствителна информация, освен ако не е посочено друго.

Всяко нарушение на сигурността се разглежда в съответствие с главата относно управлението на инциденти, свързани със сигурността, от ОРП.

5.4. *Насоки за изпитване на сигурността*

5.4.1. Софтуер

Изпитването на сигурността, включително изпитването за пробив, ако е приложимо, се извършва най-малко във всички нови основни версии на софтуера в съответствие с изискванията за сигурност, определени в Техническите стандарти за свързването (LTS), за да се оценят сигурността на свързването и свързаните рискове.

Ако през последните 12 месеца не е създадена основна версия, се провежда изпитване на сигурността на настоящата система, като се отчита нарастването на заплахите за киберсигурността от последните 12 месеца.

Изпитването на сигурността на връзката между регистрите се извършва в приемателната среда и, ако се изисква, в производствената среда, както и при съгласуване с двете страни и тяхното взаимно съгласие.

При изпитването на уеб приложения ще се спазват международните отворени стандарти, например разработените от Отворения проект за сигурност на уеб приложения (Open Web Application Security Project — OWASP).

5.4.2. Инфраструктура

Инфраструктурата, подпомагаща производствената система, редовно се проверява за слаби места (най-малко веднъж месечно) и установените слабости се отстраняват. Проверката протича по метода, изложен в раздел 5.4.1, като се използва актуална база данни за слабите места.

5.5. *Разпоредби относно оценката на риска*

Ако се прилага изпитване за пробив, то трябва да бъде включено в изпитването на сигурността.

Всяка страна може да сключи договор със специализирано дружество за извършване на изпитване на сигурността, при условие че това дружество:

— притежава уменията и опита за такова изпитване на сигурността;

— не се отчита пряко на разработчика на проекта и/или на неговия изпълнител и не участва в разработването на софтуера на връзката, нито е подизпълнител на разработчика;

— е подписало Споразумение за неразкриване на информация, за да пази резултатите поверителни и да ги обработва на равнище „ETS CRITICAL“ в съответствие с указанията за боравене с чувствителна информация.