2025/908

23.5.2025 г.

РЕШЕНИЕ № 1/2024 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 4 декември 2024 година

за изменение на приложение II към споразумението и на общите работни процедури и техническите стандарти за свързването [2025/908]

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 9 и член 13, параграф 2 от него,

като има предвид, че:

(1) В Решение № 2/2019 на Съвместния комитет ([2]) беше предвидено временно решение за осъществяване на връзка между СТЕ на ЕС и СТЕ на Швейцария.

(2) На третото си заседание Съвместният комитет постигна съгласие относно необходимостта от анализ на разходната ефективност на постоянната връзка между Регистъра на Съюза и Швейцарския регистър.

(3) На своето пето заседание Съвместният комитет постигна съгласие по доклада, представен от работната група, създадена с решения 1/2020 ([3]) и 2/2020 ([4]) на Съвместния комитет. В този доклад работната група анализира и препоръча подход за осъществяване на постоянната връзка между Регистъра на Съюза и на Швейцарския регистър.

(4) За да се отразят техническите изисквания за постоянната връзка между Регистъра на Съюза и Швейцарския регистър, както и за да се рационализират разпоредбите на приложение II към споразумението с оглед на технологичното развитие, приложение II към споразумението следва да бъде изменено.

(5) За да се осигури съгласуваност на общите работни процедури и техническите стандарти за свързването с приложение II към споразумението, посочените документи също следва да бъдат изменени,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

1. Приложение II към споразумението се заменя с текста, съдържащ се в приложение I към настоящото решение.

2. Общите работни процедури, посочени в член 3, параграф 6 от споразумението, се съдържат в приложение II към настоящото решение. Те заменят Общите работни процедури, съдържащи се в приложението към Решение № 1/2020.

([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 г. 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 [2020/1359] (ОВ L 314, 29.9.2020 г., стр. 68).

([3]) Решение № 1/2020 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 г. относно приемането на Общи работни процедури (ОРП) [2021/1033] (ОВ L 226, 25.6.2021 г., стр. 2).

([4]) 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 г. за изменение на приложения I и II към споразумението и приемане на Технически стандарти за свързването (LTS) (2021/1034) (ОВ L 226, 25.6.2021 г., стр. 16).

3. Техническите стандарти за свързването, посочени в член 3, параграф 7 от споразумението, се съдържат в приложение III към настоящото решение. Те заменят Техническите стандарти за свързването, съдържащи се в приложението към Решение № 2/2020.

Член 2

Настоящото решение влиза в сила в деня на неговото приемане.

Съставено в Брюксел на 4 декември 2024 година.

За Съвместния комитет

Секретар за Европейския съюз	*Председател*	*Секретар за Швейцария*
Ruben VERMEEREN	Beatriz YORDI	Thomas MEIER

ПРИЛОЖЕНИЕ I

„ПРИЛОЖЕНИЕ II

ТЕХНИЧЕСКИ СТАНДАРТИ ЗА СВЪРЗВАНЕТО

С цел осъществяване на свързването на СТЕ на ЕС и СТЕ на Швейцария през 2020 г. беше въведено временно решение. Считано от 2023 г., връзката между регистрите на двете системи за търговия с емисии постепенно ще се превърне в постоянна връзка между регистрите, която се очаква да бъде въведена не по-късно от 2024 г. и която позволява функционирането на свързаните пазари от гледна точка на ползите от пазарната ликвидност и осъществяването на трансакции между двете свързани системи така, както биха се осъществявали на един пазар, съставен от две системи, който позволява на участниците на пазара да действат така, сякаш се намират на един пазар, при спазване само на отделни регулаторни разпоредби на страните.

В Техническите стандарти за свързването (LTS) се посочват:

— архитектурата на комуникационната връзка;

— комуникациите между SSTL и EUTL;

— сигурността на преноса на данни;

— списъкът на функциите (трансакции, съгласуване и др.);

— определение на транспортния слой;

— изискванията за записване на данните;

— работните разпоредби (помощен център, подпомагане);

— планът за задействане на комуникационната връзка и процедурата за изпитване;

— процедурата за изпитване на сигурността.

В LTS е посочено, че администраторите трябва да предприемат всички разумно възможни мерки за гарантиране, че SSTL, EUTL и връзката са в работно състояние 24 часа в денонощието и 7 дни в седмицата и че прекъсванията на функционирането на SSTL, на EUTL и на връзката се свеждат до минимум.

В LTS са определени допълнителни изисквания за сигурност на Швейцарския регистър, SSTL, Регистъра на Съюза и EUTL и те се документират в „план за управление по отношение на сигурността“. По-специално в LTS се посочва, че:

— ако съществува съмнение, че сигурността на Швейцарския регистър, SSTL, Регистъра на Съюза или EUTL е компрометирана, двете страни незабавно се информират взаимно и преустановяват връзката между SSTL и EUTL;

— при нарушение на сигурността страните се задължават незабавно да си обменят информацията. Доколкото има подробна техническа информация, в срок от 24 часа след като инцидентът бъде определен като нарушение на сигурността, администраторът на Швейцарския регистър и централният администратор на Съюза си обменят доклад, описващ инцидента (дата, причина, последици, предприети мерки).

Процедурата за изпитване на сигурността, която е установена в LTS, се изпълнява преди установяване на комуникационната връзка между SSTL и EUTL, както и когато е необходима нова версия или вариант на SSTL или EUTL.

В допълнение към работната среда в LTS са предвидени две изпитвателни среди: изпитвателна среда за разработване и изпитвателна среда за приемане.

Страните предоставят доказателства посредством администратора на Швейцарския регистъри централния администратор на Съюза, че през предходните 12 месеца е направена независима оценка на сигурността на техните системи в съответствие с изискванията за сигурност, определени в LTS. Изпитването на сигурността, и по-специално изпитването за проникване, се извършва върху всички значими нови варианти на софтуера в съответствие с изискванията за сигурност, определени в LTS. Изпитването за проникване не се извършва от разработчика на софтуера или от подизпълнител на разработчика на софтуера.“

ПРИЛОЖЕНИЕ II

ОБЩИ РАБОТНИ ПРОЦЕДУРИ (ОРП) СЪГЛАСНО ЧЛЕН 3, ПАРАГРАФ 6 ОТ СПОРАЗУМЕНИЕТО МЕЖДУ ЕВРОПЕЙСКИЯ СЪЮЗ И КОНФЕДЕРАЦИЯ ШВЕЙЦАРИЯ ЗА СВЪРЗВАНЕ НА ТЕХНИТЕ СИСТЕМИ ЗА ТЪРГОВИЯ С ЕМИСИИ НА ПАРНИКОВИ ГАЗОВЕ

Процедури за постоянна връзка между регистрите

Съдържание

1. СПИСЪК НА ТЕРМИНИТЕ И СЪКРАЩЕНИЯТА 7
2. ВЪВЕДЕНИЕ 7
2.1. Приложно поле 8
2.2. Адресати 8
3. ПОДХОД И СТАНДАРТИ 8
4. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ 9
4.1. Засичане и записване на инциденти 9
4.2. Класифициране и дейности по първоначална поддръжка 9
4.3. Проучване и диагностика 10
4.4. Разрешаване на инциденти и възстановяване на услугата 10
4.5. Приключване на инциденти 10
5. УПРАВЛЕНИЕ НА ПРОБЛЕМИ 11
5.1. Установяване и записване на проблеми 11
5.2. Подреждане на проблемите по приоритет 11
5.3. Проучване и диагностика на проблеми 11
5.4. Разрешаване на проблеми 11
5.5. Приключване на проблеми 11
6. ИЗПЪЛНЕНИЕ НА ЗАЯВКИ 11
6.1. Подаване на заявки 11
6.2. Регистриране и анализ на заявки 12
6.3. Одобряване на заявки 12
6.4. Изпълнение на заявки 12
6.5. Пренасочване на заявки 12
6.6. Преглед на изпълнението на заявки 12
6.7. Приключване на заявки 12
7. УПРАВЛЕНИЕ НА ПРОМЕНИ 12
7.1. Заявки за промяна 13
7.2. Оценяване и планиране на промени 13
7.3. Одобряване на промени 13
7.4. Изпълнение на промени 13
8. УПРАВЛЕНИЕ НА ВЕРСИИ 13
8.1. Планиране на версии 14
8.2. Изготвяне и изпитване на пакети от версии 14
8.3. Подготвяне за внедряване 14
8.4. Връщане на версия в предишно стабилно състояние 15

8.5. Преглед и приключване на версии 15
9. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СИГУРНОСТТА 15
9.1. Категоризация на инциденти, свързани с информационната сигурност 15
9.2. Разглеждане на инциденти, свързани с информационната сигурност 15
9.3. Установяване на инциденти, свързани със сигурността 16
9.4. Анализ на инциденти, свързани със сигурността 16
9.5. Оценка на сериозността, пренасочване и докладване на свързани със сигурността инциденти 16
9.6. Докладване на реакции във връзка със сигурността 16
9.7. Наблюдение, изграждане на капацитет и непрекъснато подобрение 16
10. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ 17
10.1. Разпознаване на чувствителната информация 17
10.2. Степени на чувствителност на информационните активи 17
10.3. Определяне на собственик на информационните активи 17
10.4. Регистриране на чувствителна информация 17
10.5. Работа с чувствителна информация 18
10.6. Управление на достъпа 18
10.7. Управление на сертификати/ключове 18

1. **СПИСЪК НА ТЕРМИНИТЕ И СЪКРАЩЕНИЯТА**

Таблица 1-1

Съкращения и определения

Съкращение/Термин	Определение
Сертифициращ орган (СО)	Субект, който издава електронни сертификати
CH	Конфедерация Швейцария
СТЕ	Система за търговия с емисии
ЕС	Европейски съюз
ЕУИ	Екип за управление на инциденти
Информационен актив	Информация, която е ценна за дружество или организация
ИТ	Информационни технологии
ITIL	Библиотека за инфраструктурата на информационните технологии
ITSM	Управление на услугите в областта на информационните технологии
LTS	Технически стандарти за свързването
Регистър	Система за отчитане на квотите, издадени в рамките на СТЕ, с която собствеността на квотите се проследява по електронен път
RFC	Заявка за промяна
СЧИ	Списък с чувствителна информация
SR	Заявка за услуга
Уики	Уебсайт, който позволява на потребителите да обменят информация и знания чрез добавяне или адаптиране на съдържание директно чрез уеб браузър.

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 взаимното 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 се осъществи връзката между СТЕ на ЕС и СТЕ на Швейцария, се създава 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 осъществяване на свързването на СТЕ на ЕС и СТЕ на Швейцария през 2020 г. беше въведено временно решение. Считано от 2023 г., връзката между регистрите на двете системи за търговия с емисии постепенно ще се превърне в постоянна връзка между регистрите, която се очаква да бъде въведена не по-късно от 2024 г. и която позволява функционирането на свързаните пазари от гледна на ползите от пазарната ликвидност и осъществяването на трансакции между двете свързани системи така, както биха се осъществявали на един пазар, съставен от две системи, който позволява на участниците на пазара да действат така, сякаш се намират на един пазар, при спазване само на отделните регулаторни разпоредби на страните (приложение II към споразумението).

В съответствие с член 3, параграф 6 от споразумението администраторът на Швейцарския регистър и централният администратор за Съюза определят общи работни процедури във връзка с технически или други въпроси, необходими за функционирането на връзката, с отчитане на приоритетите на вътрешното законодателство. Изготвените от администраторите ОРП пораждат действие след приемането им с решение на Съвместния комитет.

ОРП бяха приети от Съвместния комитет с Решение № 1/2020. Посочените в настоящия документ ОРП ще бъдат приети с Решение № 1/2024 на Съвместния комитет. В съответствие с настоящото решение и искания от Съвместния комитет, администраторът на Швейцарския регистър и централният администратор за Съюза разработиха и ще актуализират допълнителни технически насоки за осъществяване на връзката с цел да гарантират, че насоките постоянно се адаптират към техническия прогрес и новите изисквания, свързани с безопасността и сигурността на връзката и нейното ефективно функциониране.

2.1. **Приложно поле**

В настоящия документ е изложена общата договореност между страните по споразумението във връзка с установяването на процедурните основи за връзката между регистъра на СТЕ на ЕС и регистъра на СТЕ на Швейцария. Макар в него да са очертани общите процедурни изисквания по отношение на операциите, за осъществяване на връзката ще бъдат необходими някои допълнителни технически насоки.

За нейното правилно функциониране ще бъдат необходими технически спецификации за връзката за по-нататъшното ѝ осъществяване. Съгласно член 3, параграф 7 от споразумението тези въпроси са описани подробно в документа за Технически стандарти за свързването (LTS), който трябва да бъде приет отделно с решение на Съвместния комитет.

Целта на ОРП е да се гарантира, че услугите в областта на информационните технологии, свързани с функционирането на връзката между регистъра на СТЕ на ЕС и регистъра на СТЕ на Швейцария, се предоставят ефективно и ефикасно, особено за целите на изпълнението на заявки за услуги, отстраняването на неизправности на услугите, разрешаването на проблеми, както и за изпълнението на рутинни оперативни задачи в съответствие с международните стандарти за управление на услугите в областта на ИТ.

За постоянната връзка между регистрите ще бъдат необходими само следните ОРП, които са част от настоящия документ:

— Управление на инциденти;

— Управление на проблеми;

— Изпълнение на заявки;

— Управление на промени;

— Управление на версии;

— Управление на инциденти, свързани със сигурността;

— Управление на информационната сигурност.

2.2. **Адресати**

Целевата аудитория на настоящите ОРП са екипите за поддръжка на Регистъра на ЕС и Швейцарския регистър.

3. **ПОДХОД И СТАНДАРТИ**

Следният принцип се прилага за всички ОРП:

— ЕС и СН се договарят да определят ОРП въз основа на ITIL (Библиотека за инфраструктурата на информационните технологии, версия 4). Практиките от този стандарт се използват повторно и се адаптират към конкретните нужди, свързани с постоянната връзка между регистрите;

— Комуникацията и координацията между двете страни, необходими за обработването на ОРП, се осъществяват чрез бюрата за обслужване на регистрите на СН и ЕС. Задачите винаги се възлагат на една от страните;

— Ако има несъгласие относно работата с ОРП, то ще бъде анализирано и разрешено между двете бюра за обслужване. Ако не може да се постигне съгласие, намирането на съвместно решение се пренасочва на следващото равнище.

Равнища на пренасочване	ЕС	СН
Равнище 1	Бюро за обслужване на ЕС	Бюро за обслужване на СН
Равнище 2	Ръководител операции за ЕС	Ръководител по прилагането за регистъра СН
Равнище 3	Съвместен комитет (който може да делегира тази отговорност предвид член 12, параграф 5 от споразумението)	
Равнище 4	Съвместният комитет, ако равнище 3 е делегирано	

— Всяка от страните може да определя процедурите за функционирането на системата на своя регистър, като взема предвид изискванията и интерфейсите, свързани с настоящите ОРП;

— За поддръжката на ОРП, по-специално управление на инциденти, управление на проблеми и изпълнение на заявки, както и за комуникацията между двете страни, се използва инструмент за управление на услугите в областта на ИТ(ITSM);

— Освен това се разрешава обмен на информация по електронна поща;

— Двете страни гарантират, че изискванията за информационна сигурност се изпълняват в съответствие с указанията за работа с чувствителна информация.

4. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Целта на процеса на управление на инциденти е след инцидент да настъпи възможно най-бързо връщане на ИТ услугите към нормално ниво на обслужване и при минимално прекъсване на стопанската дейност.

Управлението на инциденти следва да включва също така воденето на регистър на инцидентите за целите на докладването и то следва да се интегрира с други процеси, за да води към непрекъснато подобрение.

В по-общ план управлението на инциденти включва следните дейности:

— Засичане и записване на инциденти;

— Класифициране и дейности по първоначална поддръжка;

— Проучване и диагностика;

— Разрешаване на инциденти и възстановяване на услугата;

— Приключване на инциденти.

През целия жизнен цикъл на инцидента от процеса на управление на инциденти зависи постоянното разглеждане на въпросите, свързани със собствеността, наблюдението, проследяването и комуникацията.

4.1. Засичане и записване на инциденти

Един инцидент може да бъде засечен от група за поддръжка, от инструменти за автоматизирано наблюдение или от техническия персонал, който извършва рутинен надзор.

След като бъде засечен, инцидентът трябва да бъде записан и да му се зададе уникален идентификатор, който дава възможност за правилно проследяване и наблюдение на инцидента. Уникалният идентификатор на инцидента е идентификаторът, зададен в общата система за записване от бюрото за обслужване на съответната страна (ЕС или СН), което е отчело инцидента, и трябва да се използва при всяка комуникация, свързана с този инцидент.

По отношение на всички инциденти звеното за контакт следва да бъде бюрото за обслужване на съответната страна, която е регистрирала записа.

4.2. Класифициране и дейности по първоначална поддръжка

Класифицирането на инциденти има за цел да се разбере и определи коя система и/или услуга е засегната от даден инцидент и доколко. За да бъде ефективно класифицирането, инцидентът следва да бъде насочен към правилния екип още от първия път, за да се ускори разрешаването му.

В етапа на класифициране инцидентът следва да се категоризира и приоритизира според неговото въздействие и спешност, за да бъде третиран съгласно сроковете за съответното ниво на приоритет.

Ако инцидентът има потенциално въздействие върху поверителността или интегритета на чувствителни данни и/или въздействие върху работата на системата, той се обявява и като инцидент, свързан със сигурността, и след това се управлява в съответствие с процеса, определен в глава „Управление на инциденти, свързани със сигурността“, от настоящия документ.

Ако е възможно, бюрото за обслужване, което е регистрирало записа, извършва първоначална диагностика. За целта бюрото за обслужване ще прецени дали инцидентът представлява известна грешка. Ако това е така, тогава начинът на разрешаване или временното решение вече са известни и документирани.

Ако бюрото за обслужване успее да разреши инцидента, тогава то всъщност ще приключи инцидента още на този етап, тъй като основната цел на управлението на инциденти би била изпълнена (т.е. бързото възстановяване на услугата за крайния ползвател). Ако това не е така, бюрото за обслужване ще пренасочи инцидента към правилната група по разрешаване, за да бъде допълнително проучен и диагностициран.

4.3. **Проучване и диагностика**

Проучване и диагностика на инциденти се прилагат, когато бюрото за обслужване не може да разреши даден инцидент като част от първоначалната диагностика и поради това го пренасочва към подходящото равнище. Пренасочването на инцидента е самостойна част от процеса на проучване и диагностика.

Обща практика на етапа на проучване и диагностика е опитът инцидентът да се пресъздаде при контролирани условия. Важно е при проучването и диагностиката на инциденти да се разбере правилният ред на събитията, довели до инцидента.

Пренасочване означава да се признае, че даден инцидент не може да бъде разрешен на настоящото равнище на поддръжка и трябва да бъде прехвърлен на група за поддръжка на по-високо равнище или на другата страна. Пренасочването може да следва две направления: хоризонтално (функционално) или вертикално (йерархично).

Бюрото за обслужване, което е записало и завело инцидента, е отговорно за неговото пренасочване към правилния екип и за проследяването на цялостния статус и възлагане на инцидента.

Страната, на която е възложен инцидентът, отговаря за това поисканите действия да се извършват своевременно и нейното бюро за обслужване да получи обратна информация.

4.4. **Разрешаване на инциденти и възстановяване на услугата**

Разрешаването на инциденти и възстановяването на услугата се извършва, след като бъде добита пълна представа за инцидента. Намирането на разрешение на даден инцидент означава, че е установен начин за отстраняване на проблема. Прилагането на разрешението представлява етапа на възстановяване на услугата.

След като проблемът с услугата бъде разрешен от подходящия екип, инцидентът се насочва обратно към съответното бюро за обслужване, което е регистрирало инцидента, и то потвърждава заедно с инициатора на инцидента, че грешката е отстранена и инцидентът може да бъде приключен. Констатациите от обработката на инцидента трябва да се записват с цел бъдеща употреба.

Възстановяването на услугата може да се извършва от ИТ персонал по поддръжка или чрез предоставяне на набор от инструкции на крайния ползвател, които той да следва.

4.5. **Приключване на инциденти**

Приключването е последната стъпка в процеса на управление на инциденти и се извършва малко след разрешаването на инцидента.

В контролните списъци на дейностите, които трябва да бъдат извършвани по време на етапа на приключване, е подчертано следното:

— проверка на първоначалната категоризация на инцидента;

— правилно отразяване на цялата информация, свързана с инцидента;

— правилно документиране на инцидента и актуализиране на базата от знания;

— подходящо информиране на всички заинтересовани страни, които са засегнати пряко или косвено от инцидента.

Инцидентът е официално приключен, след като бюрото за обслужване изпълни етапа на приключване на инцидента и го съобщи на другата страна.

След като инцидентът бъде приключен, той не се въвежда отново. Ако той се появи отново в рамките на кратък период от време, първоначалният инцидент не се въвежда отново, а вместо това трябва да се регистрира нов инцидент.

Ако инцидентът се проследява както от бюрото за обслужване на ЕС, така и от бюрото за обслужване на СН, окончателното приключване е отговорност на бюрото за обслужване, което е регистрирало записа.

5. УПРАВЛЕНИЕ НА ПРОБЛЕМИ

Тази процедура следва да се прилага всеки път, когато се открие проблем и съответно започва процесът на управление на проблеми. Управлението на проблеми е насочено към повишаване на качеството и намаляване на броя на възникналите инциденти. Даден проблем може да бъде причината за един или повече инциденти. Когато се докладва инцидент, целта на управлението на инциденти е услугата да се възстанови възможно най-бързо, евентуално с помощта на временни решения. Когато възникне проблем, целта е да се проучи основната причина за него, за да се установи промяна, която да гарантира, че проблемът и свързаните с него инциденти няма да се повторят.

5.1. Установяване и записване на проблеми

В зависимост от това коя страна е извършила записа, бюрото за обслужване на ЕС или бюрото за обслужване на СН ще бъде звеното за контакт по въпроси, свързани с проблема.

Уникалният идентификатор на даден проблем е идентификаторът, който му е зададен от инструмента за управление на услугите в областта на ИТ (ITSM). Той трябва да се използва при всяка комуникация, свързана с този проблем.

Даден проблем може да бъде въведен заради инцидент или по собствена инициатива за разрешаване на въпроси, открити в системата в произволен момент.

5.2. Подреждане на проблемите по приоритет

Проблемите могат да бъдат категоризирани според тяхната сериозност и приоритет по същия начин като инцидентите с цел да се улесни проследяването им, като се вземе предвид въздействието на свързаните с тях инциденти и честотата им на възникване.

5.3. Проучване и диагностика на проблеми

Всяка от страните може да съобщи за проблем и бюрото за обслужване на инициращата страна ще бъде отговорно за регистрирането на проблема, възлагането му на съответния екип и проследяването на цялостния му статус.

Групата за разрешаване, към която е пренасочен проблемът, е отговорна за своевременното разглеждане на проблема и за комуникацията с бюрото за обслужване.

При поискване всяка от двете страни е отговорна да гарантира изпълнението на възложените действия и да предостави обратна информация на своето бюро за обслужване.

5.4. Разрешаване на проблеми

Групата по разрешаване, на която е възложен проблемът, отговаря за разрешаването му и за предоставянето на съответната информация на бюрото за обслужване на своята страна.

Констатациите от обработката на проблема трябва да се записват за бъдеща употреба.

5.5. Приключване на проблеми

Даден проблем е официално приключен, след като бъде разрешен чрез внасяне на промяна. Етапът на приключване на проблема ще се изпълнява от бюрото за обслужване, което е регистрирало проблема и е уведомило бюрото за обслужване на другата страна.

6. ИЗПЪЛНЕНИЕ НА ЗАЯВКИ

Процесът на изпълнение на заявка представлява управление от край до край на заявка за нова или съществуваща услуга от момента, в който тя е регистрирана и е одобрена, до момента на приключване. Заявките за услуги обикновено представляват кратки, предварително определени, възпроизводими, чести, предварително одобрени и процедурни искания.

По-долу са изложени основните стъпки, които трябва да бъдат следвани.

6.1. Подаване на заявки

Информацията, свързана със заявка за услуга, се подава до бюрото за обслужване на ЕС или бюрото за обслужване на СН по електронна поща, по телефона или чрез инструмента за управление на услугите в областта на ИТ (ITSM) или всеки друг договорен канал за комуникация.

6.2. **Регистриране и анализ на заявки**

За всички заявки за услуги звеното за контакт следва да бъде бюрото за обслужване на ЕС или бюрото за обслужване на СН, в зависимост от това коя страна е подала заявката за услуга. Това бюро за обслужване ще отговаря за регистрирането и анализирането на заявката за услуга с надлежното внимание.

6.3. **Одобряване на заявки**

Представителят на бюрото за обслужване на страната, която е подала заявката за услуга, проверява дали са необходими някакви одобрения от другата страна, и ако това е така, пристъпва към получаването им. Ако заявката за услуга не бъде одобрена, бюрото за обслужване актуализира и приключва записа.

6.4. **Изпълнение на заявки**

Тази стъпка е предназначена за ефективно и ефикасно обработване на заявките за услуги. Трябва да се прави разлика между следните случаи:

— изпълнението на заявката за услуга засяга само една от страните. В този случай съответната страна издава указанията за работа и координира изпълнението им.

— Изпълнението на заявката за услуга засяга както ЕС, така и СН. В този случай бюрата за обслужване издават указанията за работа в областта, за която носят отговорност. Процесът на изпълнение на заявката за услуга се координира между двете бюра за обслужване. Цялостната отговорност се носи от бюрото за обслужване, което е получило и внесло заявката за услуга.

Когато заявката за услуга бъде изпълнена, трябва да ѝ се зададе статус „изпълнена“.

6.5. **Пренасочване на заявки**

Бюрото за обслужване може, ако е необходимо, да пренасочи неизпълнената заявка за услуга към съответния екип (трета страна).

Пренасочването се извършва към съответните трети страни, т.е. бюрото за обслужване на ЕС ще трябва да изпрати заявката първо на бюрото за обслужване на СН, за да я пренасочи към трета страна от СН, и обратно.

Третата страна, към която е пренасочена заявката за услуга, е отговорна за своевременното ѝ обработване и за комуникацията с бюрото за обслужване, което я е пренасочило.

Бюрото за обслужване, което е регистрирало заявката за услуга, е отговорно за проследяването на цялостния ѝ статус и за възлагането ѝ.

6.6. **Преглед на изпълнението на заявки**

Отговорното бюро за обслужване представя записа на заявката за услуга на орган по краен контрол на качеството, преди тя да бъде приключена. Целта е да се гарантира, че заявката за услуга действително е обработена и че цялата необходима информация за описване на жизнения цикъл на заявката е предоставена достатъчно подробно. В допълнение към това, констатациите от обработката на заявката трябва да се записват за бъдеща употреба.

6.7. **Приключване на заявки**

Ако страните, на които е възложена заявката за услуга, са съгласни, че тя е изпълнена и вносителят счита случая за разрешен, следващият статус, който трябва да ѝ се определи, е „приключена“.

Заявката за услуга е официално приключена, след като бюрото за обслужване, което я е регистрирало, е изпълнило етапа на приключване на заявката и е уведомило бюрото за обслужване на другата страна.

7. **УПРАВЛЕНИЕ НА ПРОМЕНИ**

Целта е да се гарантира, че при управлението на ИТ инфраструктурата се използват стандартизирани методи и процедури за ефикасно и бързо разглеждане на всички промени, за да се сведе до минимум броят на всички свързани инциденти и тяхното отражение върху услугата. Промените в ИТ инфраструктурата могат да възникнат в отговор на проблеми или наложени външни изисквания, например законодателни промени, или да бъдат предприети активно с цел подобряване на ефикасността и ефективността или с цел разкриване на възможности или реагиране на бизнес инициативи.

Процесът на управление на промените включва различни стъпки, които отчитат всички подробности относно заявката за промяна с цел бъдещо проследяване. Тези процеси гарантират, че преди да се премине към внедряването ѝ, промяната е валидирана и изпитана. Успешното внедряване се осъществява чрез процеса на управление на версиите.

7.1. **Заявки за промяна**

Заявката за промяна (ЗП) се подава до екипа за управление на промените, за да бъде валидирана и одобрена. За всички заявки за промяна звеното за контакт следва да бъде бюрото за обслужване на ЕС или бюрото за обслужване на СН, в зависимост от това коя страна е подала заявката. Това бюро за обслужване ще отговаря за регистрирането и анализирането на заявката с надлежното внимание.

Заявките за промяна могат да произтичат:

— от инцидент, който води до промяна;

— от съществуващ проблем, който води до промяна;

— от краен ползвател, който подава заявка за нова промяна;

— от промяна в резултат на текуща поддръжка;

— от законодателна промяна.

7.2. **Оценяване и планиране на промени**

Този етап е свързан с дейностите по оценяване и планиране на промените. Той включва дейности по определяне на приоритет и планиране с цел свеждане до минимум на риска и въздействието.

Ако изпълнението на ЗП засяга както ЕС, така и СН, страната, която е регистрирала ЗП, проверява оценката и планирането на промяната с помощта на другата страна.

7.3. **Одобряване на промени**

Всяка регистрирана заявка за промяна трябва да бъде одобрена от съответното равнище на пренасочване.

7.4. **Изпълнение на промени**

Изпълнението на промяната се осъществява чрез процеса на управление на версиите. Екипите за управление на версии и на двете страни следват своите собствени процеси, които включват планиране и изпитване. След като приключи изпълнението, се извършва преглед на промяната. За да се гарантира, че всичко е преминало в съответствие с плана, съществуващият процес на управление на промените се преразглежда постоянно и се актуализира при необходимост.

8. **УПРАВЛЕНИЕ НА ВЕРСИИ**

Версията представлява една или повече промени в ИТ услуга, събрани в план за версия, които трябва да бъдат разрешени, подготвени, компилирани, изпитани и внедрени заедно. Версията може да представлява отстраняване на грешка, промяна на хардуер или други компоненти, промени на софтуер, надстройка на версии на приложения, промени в документацията и/или процесите. Съдържанието на всяка версия се управлява, изпитва и внедрява като едно цяло.

Управлението на версиите има за цел планиране, компилиране, изпитване и валидиране и осигуряване на способност за предоставяне на проектираните услуги, които ще удовлетворят изискванията на заинтересованите страни и ще реализират поставените цели. Критериите за приемане на всички промени в услугата ще бъдат определени и документирани по време на координирането на проекта и ще бъдат предоставени на екипите за управление на версии.

Версията обикновено се състои от редица решения на проблеми и подобрения на услугата. Тя съдържа необходимия нов или променен софтуер и всеки нов или променен хардуер, необходим за изпълнение на одобрените промени.

8.1. **Планиране на версии**

На първия етап от процеса се възлагат разрешените промени на пакетите от версии и се определят обхватът и съдържанието на версиите. Въз основа на тази информация чрез подпроцеса на планиране на версията се изготвя график за компилиране, изпитване и внедряване на версията.

При планирането следва да се определят:

— обхватът и съдържанието на версията;

— оценката на риска и рисковият профил на версията;

— клиентите/ползвателите, засегнати от версията;

— екипът, който отговаря за версията;

— стратегията за изпълнение и внедряване;

— ресурсите за версията и нейното внедряване.

Двете страни се уведомяват взаимно относно своите периоди на планиране и поддръжка. Ако дадена версия засяга както ЕС, така и СН, те координират планирането и определят общ период на поддръжка.

8.2. **Изготвяне и изпитване на пакети от версии**

На етапа на компилиране и изпитване от процеса на управление на версиите се установява подходът за изпълнение на версията или пакета от версии и за поддържане на контролираните среди преди промяната на производствената среда, както и за изпитване на всички промени във всички вече пуснати в експлоатация среди.

Ако версията засяга както ЕС, така и СН, те координират плановете за изпълнение и изпитванията. Това включва следните аспекти:

— как и кога ще се изпълняват елементи от версията и компоненти от услугата;

— какви са типичните необходими периоди за въвеждане; какво се случва, ако има забавяне;

— как да се проследи напредъкът по изпълнението и да се получи потвърждение;

— показателите за наблюдение и установяване на успеха на усилията за внедряване на версията;

— общите случаи на изпитване на съответните функции и промени.

В края на този подпроцес всички необходими компоненти на версията са готови за влизане в етапа на реална експлоатация.

8.3. **Подготвяне за внедряване**

Подготвителният подпроцес гарантира, че плановете за комуникация са определени правилно и уведомленията са готови за изпращане до всички засегнати заинтересовани страни и крайни ползватели и че версията е включена в процеса на управление на промените, за да се гарантира, че всички промени се извършват контролирано и се одобряват от съответните субекти.

Ако версията засяга както ЕС, така и СН, те координират следните дейности:

— записване на заявките за промяна с цел изготвяне на график и подготвяне на внедряването в работна среда;

— създаване на план за изпълнение;

— приемане на подход за връщане в предишно стабилно състояние, така че в случай на неуспешно внедряване да е възможно връщане към предишното състояние;

— изпращане на уведомления до всички необходими страни;

— изискване на одобрение за изпълнението на версията на съответното равнище на пренасочване.

8.4. **Връщане на версия в предишно стабилно състояние**

В случай че внедряването е било неуспешно или при изпитването се установи, че внедряването е било неуспешно или не отговаря на договорените критерии за приемане/качество, екипите за управление на версиите и на двете страни ще трябва да възстановят предишното състояние. Всички необходими заинтересовани страни трябва да бъдат уведомени, включително засегнатите/целевите крайни ползватели. До получаване на одобрение процесът може да бъде пуснат отново на всеки от предходните етапи.

8.5. **Преглед и приключване на версии**

При прегледа на внедряването на версията следва да бъдат включени дейностите, изброени по-долу:

— събиране на обратна информация от клиентите, ползвателите и звената, предоставящи услугата, относно удовлетвореността им от внедряването на версията (събиране и разглеждане на обратната информация с цел постоянно подобряване на услугата);

— преглед на всички критерии за качество, които не са изпълнени;

— проверка на това дали всички действия, необходими корекции и промени са завършени;

— гарантиране, че в края на внедряването няма проблеми, свързани със способностите, ресурсите, капацитета или изпълнението;

— гарантиране, че всички проблеми, известни грешки и временни решения са документирани и приети от клиента, крайните ползватели, звената за оперативна поддръжка и други засегнати страни;

— наблюдаване на инцидентите и проблемите, причинени от внедряването на версията (оказване на навременна подкрепа на оперативните екипи, в случай че версията води до увеличаване на обема на работа);

— актуализиране на документацията за поддръжката (т.е. технически информационни документи);

— официално предаване на версията за внедряване в експлоатационна среда;

— документиране на извлечените поуки;

— получаване на резюме за версията от екипите за изпълнение;

— официално приключване на версията след проверка на записа на заявката за промяна.

9. **УПРАВЛЕНИЕ НА ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СИГУРНОСТТА**

Управлението на инциденти, свързани със сигурността, е процес за разглеждане на свързани със сигурността инциденти, за да се даде възможност за съобщаване на инциденти на потенциално засегнати заинтересовани страни; оценяване и приоритизиране на инцидентите; и реагиране при инциденти с цел уреждане на действителни, предполагаеми или потенциални нарушения на поверителността, наличието или интегритета на чувствителни информационни активи.

9.1. **Категоризация на инциденти, свързани с информационната сигурност**

Всички инциденти, които оказват въздействие върху връзката между Регистъра на Съюза и Швейцарския регистър, се анализират, за да се установи евентуално нарушаване на поверителността, интегритета или наличността на чувствителна информация, записана в списъка с чувствителна информация (СЧИ).

Ако е налице такова нарушение, инцидентът се характеризира като инцидент, свързан със сигурността на информацията, незабавно се регистрира в инструмента за управление на услугите в областта на ИТ (ITSM) и се управлява като такъв.

9.2. **Разглеждане на инциденти, свързани с информационната сигурност**

Инцидентите, свързани със сигурността, са поставени под отговорността на 3-тото равнище на пренасочване и с разрешаването на инцидентите ще се занимава специализиран екип за управление на инциденти (ЕУИ).

ЕУИ отговаря:

— за извършването на първоначален анализ, категоризиране и оценяване на сериозността на инцидента;

— за координирането на действията между всички заинтересовани страни, включително цялата документация от анализа на инцидента, взетите решения за справяне с инцидента и всякакви евентуални установени слабости;

— в зависимост от сериозността на инцидента, свързан със сигурността — за своевременното пренасочване към съответното равнище с цел получаване на информация и/или вземане на решение.

По време на процеса на управление на информационната сигурност цялата информация относно инциденти се класифицира с най-високата степен на чувствителност на информацията, но при всички случаи не по-ниска от SENSITIVE: ETS („чувствителна информация за СТЕ“).

За целите на текущо разследване и/или слабост, която би могла да бъде проучена и до отстраняването ѝ, информацията се класифицира като SPECIAL HANDLING: *ETS Critical* („информация за СТЕ с критично значение“).

9.3. **Установяване на инциденти, свързани със сигурността**

Въз основа на вида на случая, свързан със сигурността, служителят по информационната сигурност определя съответните организации, които да се ангажират и да участват в ЕУИ.

9.4. **Анализ на инциденти, свързани със сигурността**

ЕУИ поддържа връзка с всички участващи организации и съответните членове на техните екипи, както е целесъобразно, за да направи преглед на инцидента. По време на анализа се установява до каква степен са изгубени поверителността, интегритетът или наличността на актива и се оценяват последиците за всички засегнати организации. След това се определят първоначалните и последващите действия за разрешаване на инцидента и за управление на неговото въздействие, включително въздействието на тези действия върху ресурсите.

9.5. **Оценка на сериозността, пренасочване и докладване на свързани със сигурността инциденти**

ЕУИ оценява сериозността на всеки нов свързан със сигурността инцидент след характеризирането му като такъв и започва незабавни необходими действия в зависимост от сериозността на инцидента.

9.6. **Докладване на реакции във връзка със сигурността**

ЕУИ включва резултатите от ограничаването на инцидента и възстановяването от него в доклада за реакция при инциденти, свързани с информационната сигурност. Докладът се представя на 3-ото равнище на пренасочване чрез защитена електронна поща или по друг договорен начин на комуникация.

Страната, която носи отговорност, прави преглед на резултатите от ограничаването и възстановяването и:

— отново свързва регистъра, в случай че връзката е била прекъсната;

— осигурява комуникация относно инцидентите с екипите за регистрация;

— приключва инцидента.

ЕУИ следва да включва — по сигурен начин — съответни подробни данни в доклада за инцидента, свързан с информационната сигурност, за да се гарантира последователно записване и комуникация и да се даде възможност за предприемане на бързи и подходящи действия за ограничаване на инцидента. След като приключи инцидента, свързан с информационната сигурност, ЕУИ представя своевременно окончателния доклад за него.

9.7. **Наблюдение, изграждане на капацитет и непрекъснато подобрение**

ЕУИ ще представя доклади за всички свързани със сигурността инциденти на 3-ото равнище на пренасочване. Докладите ще се използват от това равнище на пренасочване, за да се определи следното:

— слабостите при проверките за сигурност и/или операцията, която трябва да бъде подсилена;

— евентуалната необходимост от подобряване на тази процедура, за да се повиши ефективността ѝ по отношение на реакцията при инциденти;

— възможностите за обучение и изграждане на капацитет за по-нататъшно укрепване на устойчивостта на системите на регистъра по отношение на информационната сигурност, намаляване на риска от бъдещи инциденти и свеждане до минимум на тяхното въздействие.

10. **УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ**

Управлението на информационната сигурност има за цел да гарантира поверителността, интегритета и наличността на класифицираната информация, данни и ИТ услуги на дадена организация. В допълнение към техническите компоненти, включително тяхното проектиране и изпитване (вж. LTS), са необходими следните ОРП, за да бъдат изпълнени изискванията за сигурност за постоянната връзка между регистрите.

10.1. **Разпознаване на чувствителната информация**

Доколко е чувствителна дадена информация се преценява по отражението върху стопанската дейност (например финансови загуби, накърняване на репутацията, законови нарушения…), което би имало евентуалното нарушение на сигурността, свързано с тази информация.

Чувствителните информационни активи се обозначават като такива въз основа на отражението им върху свързването.

Степента на чувствителност на тази информация се оценява по скалата на чувствителност, приложима за въпросното свързване и описана подробно в раздел „Разглеждане на инциденти, свързани с информационната сигурност“ от настоящия документ.

10.2. **Степени на чувствителност на информационните активи**

Веднъж обозначен, информационният актив се класифицира по следните правила:

— при определянето на най-малко един висок (HIGH) клас на поверителност, на интегритет или на достъпност активът се класифицира като SPECIAL HANDLING: ETS Critical („информация за СТЕ с критично значение“);

— при определянето на най-малко един среден (MEDIUM) клас на поверителност, на интегритет или на достъпност активът се класифицира като SENSITIVE: ETS;

— при определянето само на нисък (LOW) клас на поверителност, на интегритет или на достъпност активът се класифицира като EU: SENSITIVE: ETS *Joint Procurement*; маркировка в CH: LIMITED: ETS.

10.3. **Определяне на собственик на информационните активи**

Всички информационни активи следва да имат определен собственик. Информационните активи на СТЕ, които принадлежат към връзката между EUTL и SSTL или са свързани с нея, следва да бъдат включени в съвместен инвентарен списък на активите, поддържан от двете страни. Информационните активи на СТЕ извън връзката между EUTL и SSTL следва да бъдат включени в инвентарен списък на активите, поддържан от съответната страна.

Страните се договарят за собствеността върху всеки информационен актив, принадлежащ към връзката между EUTL и SSTL или свързан с нея. Собственикът на даден информационен актив е отговорен за оценката на неговата чувствителност.

Собственикът следва да има опит, съответстващ на стойността на записани(те) му актив(и). Отговорността на собственика за актива(ите) и задължението му/ѝ за поддържане на изискваното ниво на поверителност, интегритет и наличност следва да бъдат договорени и формализирани.

10.4. **Регистриране на чувствителна информация**

Цялата чувствителна информация се регистрира в списъка с чувствителна информация (СЧИ).

Когато е целесъобразно, се взема предвид и се регистрира в СЧИ съвкупността от чувствителна информация, която би могла да доведе до по-голямо въздействие от въздействието на само едно сведение (например съвкупност от информация, съхранявана в базата данни на системата).

Списъкът с чувствителна информация не е статичен. Заплахи, слаби места, вероятност за настъпване на засягащи активи инциденти, свързани със сигурността, или последствия от такива инциденти могат да бъдат променяни, без това да се указва по какъвто и да е начин и в работата на регистрационните системи могат да бъдат въвеждани нови активи.

Поради това СЧИ се преразглежда редовно и всяка нова информация, определена като чувствителна, незабавно се регистрира в него.

Списъкът включва най-малко следните сведения за всяко вписване:

— описание на информацията

— собственик на информацията

— степен на чувствителност

— указание дали информацията включва лични данни

— допълнителна информация при необходимост

10.5. **Работа с чувствителна информация**

Когато чувствителна информация се обработва извън връзката между Регистъра на Съюза и Швейцарския регистър, тя се третира в съответствие с указанията за работа с чувствителна информация.

Чувствителната информация, обработвана чрез връзката между Регистъра на Съюза и Швейцарския регистър, се третира от страните в съответствие с изискванията за сигурност.

10.6. **Управление на достъпа**

Целта на управлението на достъпа е на упълномощените ползватели да се предостави правото да използват дадена услуга, като същевременно се предотврати достъпът на неупълномощени ползватели. Управлението на достъпа понякога се нарича също „управление на правата“ или „управление на идентичността“.

За постоянната връзка между регистрите и нейното функциониране двете страни се нуждаят от достъп до следните компоненти:

— Уики: среда за сътрудничество за обмен на обща информация, като например планирането на версии;

— инструмента за управление на услугите в областта на ИТ (ITSM) за управление на инциденти и проблеми (вж. Глава 3 „Подход и стандарти“);

— системата за обмен на съобщения: всяка от страните предоставя защитена система за обмен на съобщения за предаване на съобщенията, съдържащи данните за трансакции.

Администраторът на Швейцарския регистър и централният администратор за Съюза гарантират, че достъпът до тях е актуален и изпълняват ролята на звена за контакт за своите страни по отношение на дейностите по управление на достъпа. Заявките за достъп се обработват в съответствие с процедурите за изпълнение на заявки.

10.7. **Управление на сертификати/ключове**

Всяка от страните е отговорна за управлението на своите сертификати/ключове (генериране, регистриране, съхранение, инсталиране, използване, подновяване, отмяна, създаване на резервни копия и възстановяване на сертификати/ключове). Както е посочено в техническите стандарти за свързването (LTS), се използват само електронни сертификати, издадени от сертифициращия орган (CO), на които се доверяват и двете страни. Работата със сертификати/ключове и съхранението им трябва да се извършват в съответствие с разпоредбите, определени в указанията за работа с чувствителна информация.

Всяка отмяна и/или подновяване на сертификати и ключове се координира от двете страни. Това се извършва в съответствие с процедурите за изпълнение на заявки.

Администраторът на Швейцарския регистър и централният администратор за Съюза ще обменят сертификати/ключове чрез сигурни средства за комуникация в съответствие с разпоредбите, предвидени в указанията за работа с чувствителна информация.

Всяка проверка на сертификати/ключове между страните по какъвто и да е начин ще се извършва по различен от обичайния канал за връзка (out-of-band).

ПРИЛОЖЕНИЕ III

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

Стандарт за постоянна връзка между регистрите

Съдържание

1. СПИСЪК НА ТЕРМИНИТЕ И СЪКРАЩЕНИЯТА 21
2. ВЪВЕДЕНИЕ 22
2.1. Приложно поле 22
2.2. Адресати 23
3. ОБЩИ РАЗПОРЕДБИ 23
3.1. Архитектура на комуникационната връзка 23
3.1.1. Обмен на съобщения 23
3.1.2. XML съобщение — описание на високо равнище 23
3.1.3. Периоди за постъпване 24
3.1.4. Потоци от съобщения за трансакции 24
3.2. Сигурност на преноса на данни 26
3.2.1. Защитна стена и взаимосвързаност на мрежите 26
3.2.2. Виртуална частна мрежа (VPN) 26
3.2.3. Прилагане на протокол IPsec 27
3.2.4. Протокол за прехвърляне за защитен обмен на съобщения 27
3.2.5. XML криптиране и подпис 27
3.2.6. Криптографски ключове 27
3.3. Списък на функциите в рамките на връзката 27
3.3.1. Трансакции в работния процес 28
3.3.2. Протокол за съгласуване 28
3.3.3. Тестово съобщение 28
3.4. Изисквания за регистриране на данни 29
3.5. Изисквания за осъществяване на връзка 29
4. РАЗПОРЕДБИ ОТНОСНО ДОСТЪПНОСТТА 30
4.1. Проектиране на достъпа до комуникация 30
4.2. Инициализиране, комуникация, възобновяване и изпитване 30
4.2.1. Вътрешни изпитвания на инфраструктурата за ИКТ 31
4.2.2. Изпитвания на комуникацията 31
4.2.3. Изпитвания на цялата система (от край до край) 31
4.2.4. Изпитвания на сигурността 31
4.3. Приемателна/изпитвателна среда 32
5. РАЗПОРЕДБИ ЗА ПОВЕРИТЕЛНОСТ И ИНТЕГРИТЕТ 32
5.1 Инфраструктура за изпитване на сигурността 32
5.2 Разпоредби относно временното прекъсване на връзката и възобновяването 32
5.3 Разпоредби относно нарушения на сигурността 33

5.4 Насоки за изпитване на сигурността 33
5.4.1 Софтуер 33
5.4.2 Инфраструктура 34
5.5 Разпоредби относно оценката на риска 34

1. СПИСЪК НА ТЕРМИНИТЕ И СЪКРАЩЕНИЯТА

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 на СТЕ на някоя от страните
CH	Конфедерация Швейцария
CHU	Квота за стационарни инсталации, наричана също CHU2 (свързана с период на задължения 2 от Протокола от Киото), издадена от CH
CHUA	Квоти за авиационни емисии на Швейцария
ОРП	Общи работни процедури. Съвместно разработени процедури за осъществяване 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/Термин	Определение
Асиметрична криптография	Използва частни и публични ключове за криптиране и декриптиране на данни
Сертифициращ орган (СО)	Субект, който издава електронни сертификати
Криптографски ключ	Информация, която определя функционалните изходящи данни от криптографския алгоритъм
Декриптиране	Процес, обратен 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

Съкращение/Термин	Определение
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 взаимното 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 се осъществи връзката между СТЕ на ЕС и СТЕ на Швейцария, се създава 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 осъществяване на свързването на СТЕ на ЕС и СТЕ на Швейцария през 2020 г. беше въведено временно решение. Считано от 2023 г., връзката между регистрите на двете системи за търговия с емисии постепенно ще се превърне в постоянна връзка между регистрите, която се очаква да бъде въведена не по-късно от 2024 г. и която позволява функционирането на свързаните пазари от гледна на ползите от пазарната ликвидност и осъществяването на трансакции между двете свързани системи така, както биха се осъществявали на един пазар, съставен от две системи, който позволява на участниците на пазара да действат така, сякаш се намират на един пазар, при спазване само на отделните регулаторни разпоредби на страните (приложение II към споразумението).

Съгласно член 3, параграф 7 от споразумението администраторът на Швейцарския регистър и централният администратор за Съюза изготвят Технически стандарти за свързването (LTS), основани се на изложените 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.

LTS бяха приети от Съвместния комитет с Решение № 2/2020. Посочените в настоящия документ актуализирани LTS ще бъдат приети с Решение № 1/2024 на Съвместния комитет. В съответствие с настоящото решение и искания от Съвместния комитет, администраторът на Швейцарския регистър и централният администратор за Съюза разработиха и ще актуализират допълнителни технически насоки за осъществяване на връзката с цел да гарантират, че насоките постоянно се адаптират към техническия прогрес и новите изисквания, свързани с безопасността и сигурността на връзката и нейното ефективно функциониране.

2.1. **Приложно поле**

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 осъществяването на връзката ще са необходими допълнителни подробни насоки.

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

2.2. **Адресати**

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

3. **ОБЩИ РАЗПОРЕДБИ**

3.1. **Архитектура на комуникационната връзка**

Целта на настоящия раздел е да предостави описание на цялостната архитектура на осъществяването 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, са предприети всички мерки за изграждане на надеждна архитектура. Постоянната връзка между регистрите използва механизъм за обмен на файлове за осъществяването на сигурна връзка с изолирана среда.

В техническите решения се използват:

— протокол за прехвърляне за защитен обмен на съобщения;

— XML съобщения;

— XML базиран цифров подпис и криптиране;

— VPN.

3.1.1. *Обмен на съобщения*

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

Двете страни водят регистър на получените съобщения, заедно с подробни данни 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 се разглеждат 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*

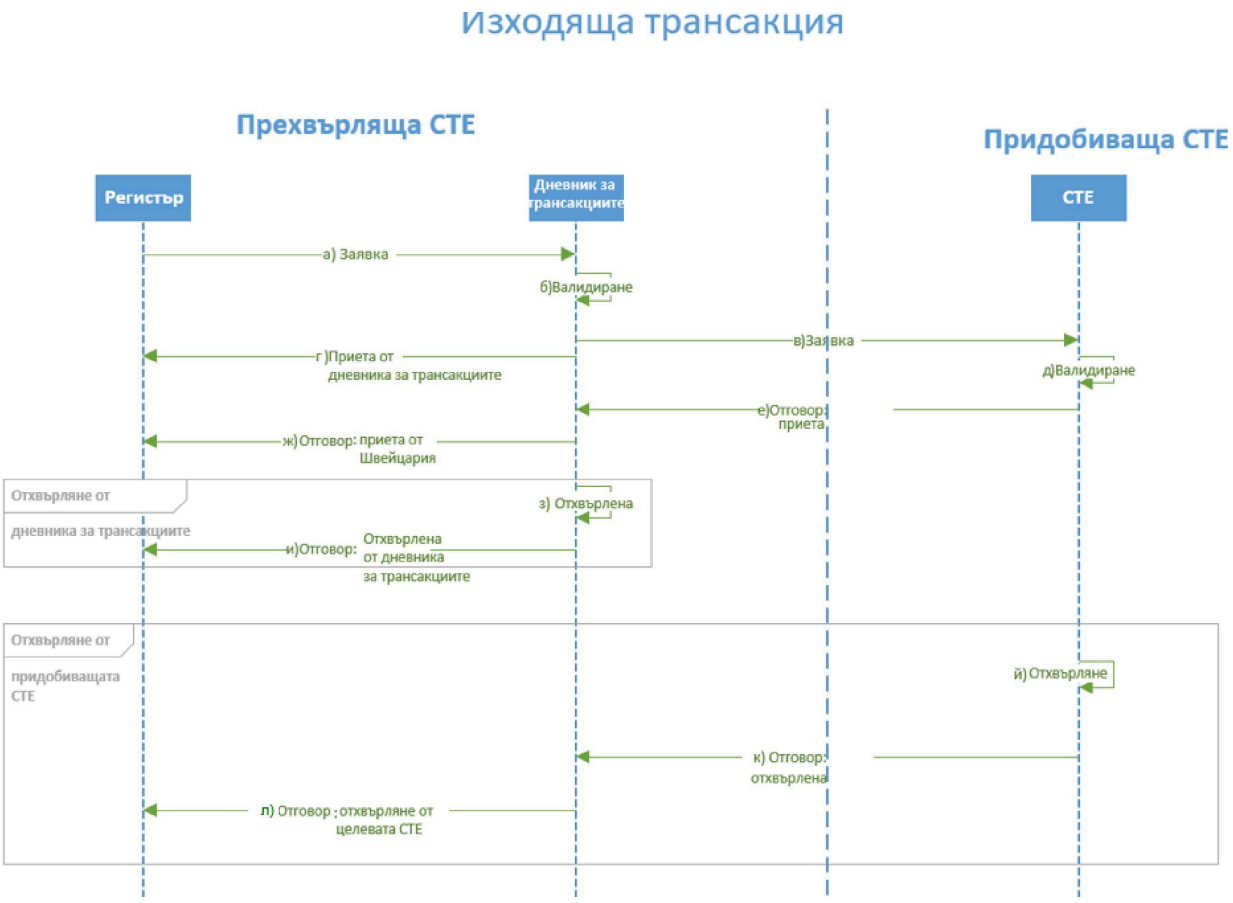
Постоянната връзка между регистрите се основава на предварително определени периоди за постъпване, които са последвани от поредица от определени събития. Заявките за трансакции, получени чрез връзката, ще постъпват само на предварително определени интервали от време и това включва техническо валидиране 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

Отразява гледната точка на прехвърлящата CTE. Конкретният поток е изобразен в диаграмата на последователността по-долу.



Основният поток показва следните стъпки (както в схемата по-горе):

а) в рамките на прехвърлящата CTE 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 CTE;

г) отговорът за приемане се изпраща до регистъра на CTE на произход.

д) целевата CTE валидира заявката за трансакция.

е) целевата CTE изпраща обратно отговора за приемане до дневника за трансакциите на CTE на произход.

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

Алтернативен поток „Отхвърляне от дневника за трансакциите“ (както в схемата по-горе, като се започва от буква а) в основния поток):

а) в системата 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 не валидира заявката;

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

Алтернативен поток „Отхвърляне от CTE“ (както в схемата по-горе, като се започва от буква г) в основния поток):

а) в рамките на CTE 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, когато е приложимо);

б) дневникът за трансакциите валидира трансакцията;

в) заявката за трансакция се изпраща до целевата CTE;

г) съобщението за приемане се изпраща до регистъра на CTE на произход;

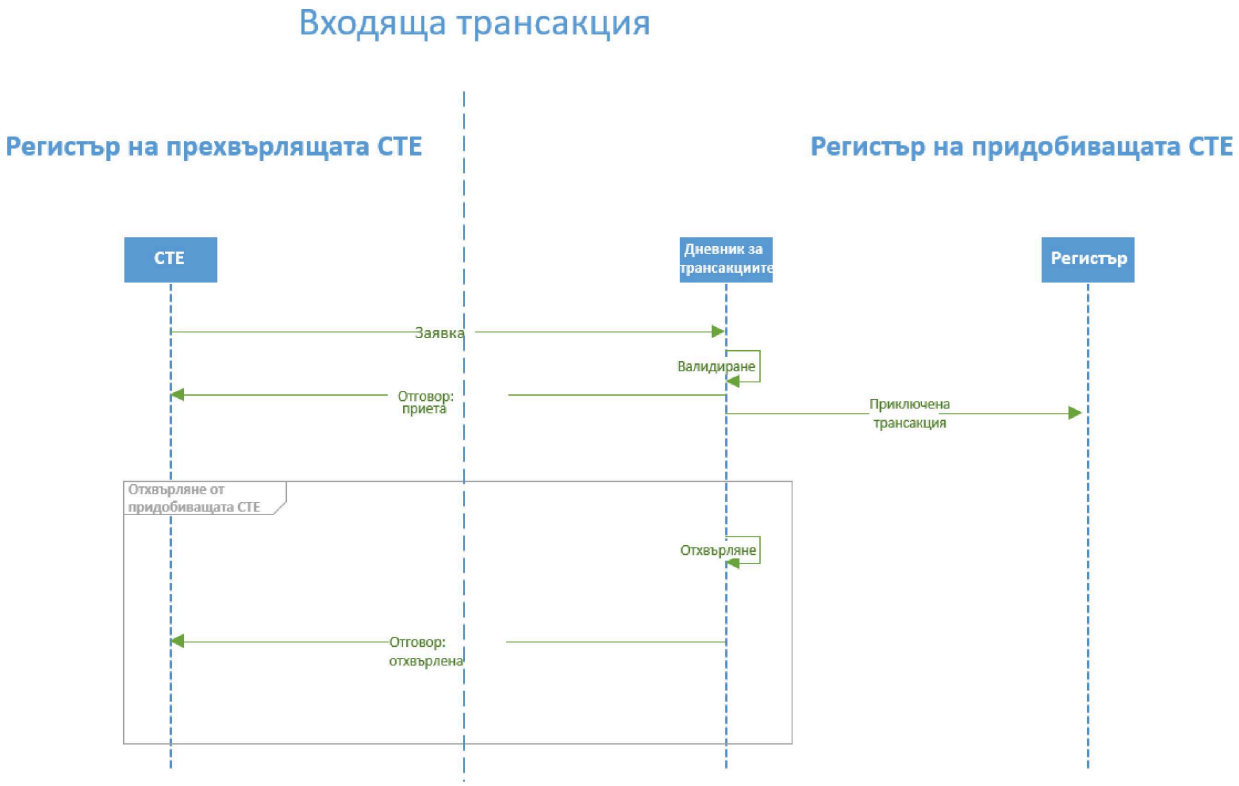
д) дневникът за трансакциите на придобиващата CTE не валидира трансакцията;

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

ж) дневникът за трансакциите изпраща отказа до регистъра.

Входящи трансакции

Отразява гледната точка на придобиващата CTE. Конкретният поток е изобразен в диаграмата на последователността по-долу.



На диаграмата е показано, че:

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

2) когато дневникът за трансакциите на придобиващата CTE откаже входящата заявка, заявката за трансакция не се изпраща до регистъра на придобиващата CTE.

Протокол

Цикълът на съобщенията за трансакция включва само две съобщения:

— прехвърлящата СТЕ à предложение за трансакция за придобиващата СТЕ;

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

  — „Приета“ (accepted): трансакцията е изпълнена;

  — „Отхвърлена“ (rejected): трансакцията е прекратена.

Състояние на трансакцията:

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

— 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“ (completed/terminated). 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“;

— придобиващата СТЕ ще определи като „прекратена“ всяка трансакция, чието състояние е било „предложена“ в продължение на 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;

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 виртуална частна мрежа (VPN). 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.

Като цяло Европейският съюз използва сигурни трансевропейски телематични услуги между администрациите (STESTA) като частна мрежа, базирана на интернет протокол. Следователно тази мрежа е подходяща и за постоянната връзка между регистрите.

3.2.3. *Прилагане на протокол IPsec*

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*

Постоянната връзка между регистрите разчита на множество равнища на криптиране за целите на сигурния обмен на данни между страните. Двете системи и техните различни среди са взаимосвързани на мрежово равнище посредством VPN тунели. 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 (CO), на който се доверяват и двете страни. Този CO проверява самоличността на притежателя на сертификита 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.

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 СН 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 обаче ще се извършва най-малко едно планирано съгласуване.

Независимо от това 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. **Изисквания за регистриране на данни**

За да се посрещне 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 представляват 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 съгласуване „одобрен“ или „несъответствия“. В постоянната връзка между регистрите съобщенията за съгласуване са неразделна част от обменените съобщения и следователно се съхраняват, както е описано в раздел „Архив на съобщенията“.

И двете страни регистрират всяка заявка и отговора по нея 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.

Дневници за вътрешен одит

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

3.5. **Изисквания за осъществяване на връзка**

При постоянната връзка между регистрите обменът на данни между двете системи не е напълно самостоятелен, което означава, че изисква оператори и процедури, за да се осъществи връзката. За целта в този процес подробно са описани някои функции и инструменти.

4. РАЗПОРЕДБИ ОТНОСНО ДОСТЪПНОСТТА

4.1. Проектиране на достъпа до комуникация

Архитектурата за постоянната връзка между регистрите в основата си представлява инфраструктура за ИКТ и софтуер, който 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 се превръща в съществен аспект, който трябва да бъде взет предвид при проектирането на постоянната връзка 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 постоянната връзка между регистрите установява устойчива VPN мрежа, 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 с другата страна за определен период от време, ако поради някаква причина тя не е достъпна.

Устойчивост на услугите

В постоянната връзка между регистрите обменът на данни между страните се извършва на предварително определени интервали от време. 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 постоянната връзка между регистрите се използва асинхронна комуникация;

— по време на автоматичния процес на съгласуване ще установи 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 вземат предвид и започват процедурите 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. Инициализиране, комуникация, възобновяване и изпитване

Всички различни елементи, включени в архитектурата на постоянната връзка между регистрите, 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 осъществяване на връзката се провеждат задължително всеки път, когато платформата промени състоянието на постоянната връзка между регистрите от „временно прекъсната“ на „осъществена“.

След това активирането състоянието на осъществена връзка изисква успешното изпълнение на предварително определен план за изпитване. Това потвърждава, че преди да започне подаването 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 посочат 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 осъществена връзка 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 администраторите на регистри 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 функционира.

4.2.2. *Изпитвания на комуникацията*

Тези изпитвания започват индивидуално от всяка страна и приключват в сътрудничество с другия край.

След като отделните елементи започнат да функционират, 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, както и дали има свързаност сайт-към-сайт на базата на интернет протокол. 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 администраторите на регистри във всеки край, както е описано подробно в раздели „Насоки за изпитване на сигурността“ и „Разпоредби относно оценката на риска“.

Едва след като всеки от четирите етапа/градивни елемента приключи с предвидим резултат, постоянната връзка между регистрите може да се счита за осъществена.

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 осъществена връзка само по себе си е ръчен процес.

Също така се предвижда 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 постоянната връзка между регистрите ще се осъществява 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 по 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 фиктивни 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, 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 едни от други.

По отношение на структурата на VPN комуникацията между трите среди трябва да бъде напълно независима, което се осигурява чрез използване на STESTA.

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 при необходимост, но може да не се прилага за всички стъпки, които администраторите на регистри предприемат.

Изискванията за сигурност се отчитат и се съобразяват 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/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 инфраструктурата за изпитване.

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

Ако съществува съмнение, че сигурността на Швейцарския регистър, SSTL, Регистъра на Съюза или EUTL е компрометирана, съответната страна незабавно информира другата и преустановява връзката между SSTL и EUTL.

Процедурите за обмен на информация, за вземане на решение за временно прекъсване и за вземане на решение 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 наложи поради:

— административни причини (например поддръжка,….), които са планирани;

— причини, свързани със сигурността (или сривове в ИТ инфраструктурата), които не са 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, всяка от страните гарантира съответно, 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 предвидената в ОРП процедура за управление на промени или процедура за управление на инциденти, свързани със сигурността.

Възобновяване на комуникацията

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

5.3 **Разпоредби относно нарушения 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 част на системата.

Информацията, пряко свързана с нарушението на сигурността, ще се счита за чувствителна, с обозначение „SPECIAL HANDLING: *ETS Critical*“ и с нея ще се работи в съответствие с указанията за работа, 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 се откриват слаби места, установени на същия принцип, както е определено в предходния раздел, 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 работи с тях на равнище „SPECIAL HANDLING: ETS critical“ в съответствие с указанията за работа с чувствителна информация.