Съвет на
Европейския съюз

Брюксел, 5 ноември 2018 г.
(OR. en)

Междуинституционално досие:
2018/0339(NLE)

13711/18
ADD 1

TRANS 488

БЕЛЕЖКА

От:	Генералния секретариат на Съвета
До:	Делегациите
№ предх. док.:	ST 13711/18 TRANS 448
№ док. Ком.:	ST 12727/18 TRANS 426 + ADD 1
Относно:	Решение на Съвета относно позицията, която да бъде заета от името на Европейския съюз в рамките на експертната група по Европейската спогодба за работата на екипажите на превозните средства, извършващи международни автомобилни превози към Икономическата комисия за Европа на Организацията на обединените нации

Приложение към посоченото по-горе решение на Съвета.

ПРИЛОЖЕНИЕ

Ново допълнение към AETR

Допълнение 4

Спецификации на TACHOnet

1. Обхват и цел

1.1. В настоящото допълнение са определени правилата и условията по отношение на свързването посредством eDelivery на договарящите страни по AETR към TACHOnet.

1.2. Договарящите страни, които се свързват към TACHOnet посредством eDelivery, спазват разпоредбите, определени в настоящото допълнение.

2. Определения

а) „договаряща страна“ или „страна“ означава всяка договаряща страна по AETR;

б) „eDelivery“ означава услугата, разработена от Европейската комисия, чрез която по електронен път могат да се предават данни между трети страни, като се осигуряват сведения във връзка с обработката на предаваните данни, включително доказателство за изпращането и получаването на данните, и се защитават предаваните данни срещу риска от всякакво непозволено изменение;

в) „TACHOnet“ означава системата за електронен обмен на информация относно картите на водачи между договарящите страни, посочена в член 31, параграф 2 от Регламент (ЕС) № 165/2014;

г) „централен възел“ означава информационната система, позволяваща маршрутизирането на съобщенията по TACHOnet между запитващата и отговарящата страна;

д) „запитваща страна“ означава договарящата страна, която изпраща по TACHOnet искане или уведомление, които след това централният възел насочва към подходящата отговаряща страна;

е) „отговаряща държава членка“ означава договарящата страна, до която е адресирано запитването или уведомлението по TACHOnet;

ж) „орган, компетентен за издаването на карти“ (ОКИК) означава субектът, който е упълномощен от дадена договаряща страна да издава и управлява тахографските карти;

3. Отговорности от общ характер

3.1. Нито една договаряща страна няма право да сключва споразумения за достъп до TACHOnet от името на друга страна или по някакъв друг начин да представлява другата договаряща страна на базата на настоящото допълнение. Нито една от договарящите страни не действа като подизпълнител на другата договаряща страна в операциите, посочени в настоящото допълнение.

3.2. Договарящите страни предоставят достъп до националния си регистър на картите на водачи чрез TACHOnet по начина и с нивото на обслужване, определени в поддопълнение 4.6.

3.3. Договарящите страни без забавяне се уведомяват взаимно, ако забележат нарушения или грешки в своята сфера на отговорност, които могат да застрашат нормалното функциониране на TACHOnet.

3.4. Всяка страна представя в секретариата на AETR лица за контакт за TACHOnet. Всяка промяна в точките за контакт трябва да бъде предоставена на секретариата на AETR в писмен вид.

4. Изпитвания за свързването към TACHOnet

4.1. Свързването на дадена договаряща страна към TACHOnet се удостоверява след успешното осъществяване на връзката, интеграцията и изпитванията на експлоатационните показатели в съответствие с инструкциите и под надзора на Европейската комисия.

4.2. В случай на неуспех при предварителните изпитвания Европейската комисия може временно да прекрати етапа на изпитване. Изпитванията се подновяват, когато договарящата страна съобщи на Европейската комисия за приемането на необходимите технически подобрения на национално равнище, които позволяват успешното провеждане на предварителните изпитвания.

4.3. Максималната продължителност на предварителните изпитвания е шест месеца.

5. Архитектура за доверителност

5.1. Поверителността, целостта и невъзможността за променяне на съобщенията по TACHOnet трябва да се гарантира от архитектурата за доверителност на TACHOnet.

5.2. Архитектурата за доверителност на TACHOnet трябва да се основава на услугата за инфраструктура за публични ключове (ИПК), създадена от Европейската комисия, изискванията за която са определени в поддопълнения 4.8 и 4.9.

5.3. В архитектурата за доверителност на TACHOnet участват следните субекти:

а) Сертифициращ орган, отговарящ за генерирането на цифровите сертификати, които регистриращият орган предоставя на националните органи на договарящите страни (чрез определени от тях доверени куриери), както и за създаването на техническата инфраструктура, свързана с издаването, оттеглянето и подновяването на цифровите сертификати.

б) Собственикът на домейн е отговорен за работата на централния възел, посочен в поддопълнение 4.1, и за валидирането и координирането на архитектурата за доверителност на TACHOnet.

в) Регистриращият орган е отговорен за регистрирането и одобряването на заявленията за издаване, оттегляне и подновяване на цифрови сертификати, както и за проверката на самоличността на доверените куриери.

г) Доверен куриер е лицето, определено от националните органи, което отговаря за предаването на публичния ключ на регистриращия орган и за получаването на съответния сертификат, генериран от сертифициращия орган.

д) Националният орган на договарящата страна:

i) генерира частните ключове и съответните публични ключове за включване в сертификатите, които се генерират от сертифициращия орган;

ii) изисква цифровите сертификати от сертифициращия орган;

iii) определя доверения куриер.

5.4. Сертифициращият орган и регистриращият орган се определят от Европейската комисия.

5.5. Всяка договаряща страна, която се свързва с TACHOnet, трябва да поиска издаването на цифров сертификат в съответствие с поддопълнение 4.9, за да подпише и криптира съобщенията по TACHOnet.

5.6. Даден сертификат може да бъде отменен в съответствие с поддопълнение 4.9.

6. Защита на данните и поверителност

6.1. Страните, в съответствие със законодателството за защита на данните на международно и национално равнище, и по-специално с Конвенцията за защита на лицата при автоматизираната обработка на лични данни, приемат всички необходими технически и организационни мерки, за да гарантират сигурността на данните по TACHOnet и да предотвратят изменението или загубата, или неразрешената обработка или достъп до такива данни (по-специално автентичността, поверителността на данните, проследимостта, целостта, наличността и невъзможността за променяне, и сигурността на съобщенията).

6.2. Всяка страна защитава националните си системи от неправомерно използване, зловредни програми, вируси, проникване в компютрите, нарушавания и незаконна промяна на данните и други подобни действия, извършени от трети страни. Страните се съгласяват да положат разумни от икономическа гледна точка усилия, за да избегнат предаването на каквито и да било вируси, времеви бомби, компютърни червеи или подобни елементи, или каквито и да било изпълними компютърни програми, които могат да окажат въздействие на компютърните системи на другата страна.

7. Разходи

7.1. Договарящите страни поемат своите разходи за разработка и експлоатация, свързани със системите и процедурите им за данни, така че да са в състояние да изпълнят задълженията си, произтичащи от настоящото допълнение.

7.2. Услугите, посочени в поддопълнение 4.1 и предоставяни от централния възел, са безплатни.

8. Възлагане на подизпълнители

8.1. Страните могат да възлагат за подизпълнение всяка от услугите, за които отговарят по силата на настоящото допълнение.

8.2. Възлагането на подизпълнители не освобождава страната от отговорността по силата на настоящото допълнение, включително отговорността за подходящото ниво на обслужване в съответствие с поддопълнение 4.6.

Поддопълнение 4.1

Общи аспекти на TACHOnet

1. Общо описание

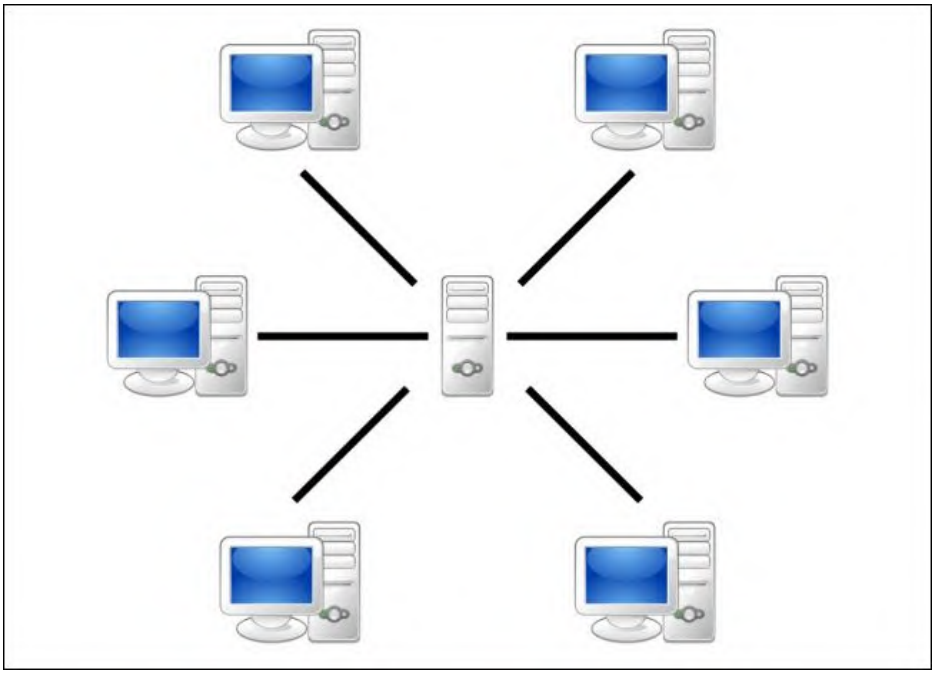
TACHOnet е електронна система за обмен на информация между договарящите страни по AETR, свързана с картите на водачи. TACHOnet насочва исканията за информация от запитващите страни до отговарящите страни, а отговорите на вторите до запитващата страна. Договарящите страни, бидейки част от TACHOnet, трябва да свържат към системата националните си регистри за картите на водачи.

2. Архитектура

Съобщителната система TACHOnet се състои от следните части:

2.1. Централен възел, който е в състояние да получи запитване от запитващата страна, да го валидира и да го обработи, като го препрати на отговарящите страни. Централният възел трябва да изчака всяка отговаряща страна да отговори, обединява всички отговори и изпраща обединения отговор на запитващата държава членка.

2.2. Национални системи на страните, които да са снабдени с интерфейс, способен както да изпраща запитвания до централния възел, така и да получава съответните отговори. Националните системи могат да използват собствено или закупено програмно осигуряване за изпращането и получаването на съобщения от централния възел.



3. Управление

3.1. Централният възел се управлява от Комисията, която отговаря за техническата експлоатация и поддръжката на централния възел.

3.2. Централният възел не трябва да съхранява данни за период, по-дълъг от шест месеца, освен данните за достъп и статистическите данни, определени в поддопълнение 4.7.

3.3. Централният възел не предоставя достъп до лични данни, с изключение на упълномощени служители на Европейската комисия, когато това е необходимо за целите на мониторинга, поддръжката и отстраняването на неизправности.

3.4. Всяка договаряща страна отговаря за:

3.4.1. Изграждането и управлението на своите национални системи, включително на интерфейса с централния възел.

3.4.2. Монтажа и поддръжката на своята национална система, както по отношение на апаратната част, така и на програмното осигуряване, независимо дали са собствени или закупени.

3.4.3. Правилната оперативна съвместимост на националната им система с централния възел, включително управлението на съобщенията за грешка, получени от централния възел.

3.4.4. Вземане на всички мерки за осигуряване на поверителността, целостта и наличието на информацията.

3.4.5. Работата на националните системи в съответствие с нивата на обслужване, определени в поддопълнение 4.6.

Поддопълнение 4.2

Функционални възможности на TACHOnet

1. Съобщителната система TACHOnet трябва да разполага със следните функционални възможности:

1.1. Check Issued Cards (проверка за издадени карти) (CIC): позволява на запитващата страна да изпрати Check Issued Cards Request (запитване за проверка за издадени карти) до една или до всички отговарящи държави членки, за да се определи дали даден заявител за карта вече притежава карта на водач, издадена от отговарящите страни. Отговарящите страни отговорят чрез Check Issued Cards Response (отговор на запитване за проверка за издадени карти).

1.2. Check Card Status (проверка на статуса на карта) (CCS): позволява на запитващата страна да поиска от отговарящата страна подробности за карта, издадена от втората, като изпрати Check Card Status Request (запитване за проверка на статуса на карта). Отговарящата страна отговоря на запитването чрез Check Card Status Response (отговор на запитване за проверка на статуса на карта).

1.3. Modify Card Status (промяна на статуса на карта) (MCS) позволява на запитващата страна да уведоми отговарящата страна чрез Modify Card Status Request (запитване за промяна на статуса на карта), че в статуса на дадена карта, издадена от втората, е настъпила промяна. Отговарящата страна отговоря чрез Modify Card Status Acknowledgement (потвърждение на промяната на статуса на карта).

1.4. Issued Card Driving Licence (издадена карта срещу свидетелство за управление) (ICDL): позволява на запитващата страна да уведоми отговарящата страна чрез Issued Card Driving Licence Request (запитване за издадена карта срещу свидетелство за управление), че първата е издала карта срещу свидетелство за управление, издадено от втората. Отговарящата страна отговоря чрез Issued Card Driving Licence Response (отговор за издадена карта срещу свидетелство за управление).

2. Трябва да бъдат включени и други видове съобщения, които се считат за подходящи за ефективното функциониране на TACHOnet, като например уведомления за грешка.

3. Националните системи трябва да разпознават статусите на картата, изброени в таблица 1, когато се използва някоя от функционалните възможности, описани в точка 1. Същевременно страните не са длъжни да въведат административна процедура, която да използва всички изброени статуси.

4. Когато дадена страна получи отговор или уведомление за статус, който не се използва в административните ѝ процедури, националната система трябва да преобразува статуса от полученото съобщение в подходяща стойност за въпросната процедура. Отговарящата страна не отхвърля съобщението, ако статусът от съобщението фигурира в таблица 1.

5. Статусът на карта, включен в таблица 1, не трябва да се използва за определяне на това дали дадена карта на водач е валидна за управлението на МПС. Когато чрез функционалната възможност CCS дадена страна изпраща запитване до регистъра на страната, издала картата, отговорът трябва да съдържа специалното за целта поле „валидна за управление“. Националните административни процедури трябва да са такива, че отговорите на CCS винаги да съдържат правилната стойност на „валидна за управление“.

Таблица 1

Статуси на картата

Статус на картата	**Определение**
Заявление	ОКИК е получил заявление за издаването на карта на водач. Тази информация е била регистрирана и съхранена в базата данни с генерираните ключове за търсене.
Одобрено	ОКИК е одобрил заявлението за тахографска карта.
Отхвърлено	ОКИК не е одобрил заявлението.
Индивидуализирана	Тахографската карта е била индивидуализирана.
Изпратена	Националният орган е изпратил картата на водач на съответния водач или на предоставящата агенция.
Връчена	Националният орган е връчил картата на водач на съответния водач.
Конфискувана	Компетентният орган е конфискувал картата на водач от водача.
Временно прекратена	На водача временно е конфискувана картата на водач.
Отнемане	ОКИК е решил да отнеме картата на водач. Картата е обявена за невалидна за постоянно.
Върната	Тахографската карта е върната на ОКИК и е обявено, че повече не е необходима.
Изгубена	Тахографската карта е обявена пред ОКИК за изгубена.
Откраднатa	Тахографската карта е докладвана на ОКИК за откраднатa. Откраднатa карта се счита за загубена.
Неизправна	Тахографската карта е докладвана на ОКИК за неизправна.
Изтекъл срок	Срокът на валидност на тахографската карта е изтекъл.
Заменена	Тахографската карта, която е докладвана за загубена, откраднатa или неизправна, е заменена с нова. Данните върху новата карта са същите, с изключение на това, че индексът за замяна в номера на картата е увеличен с единица.

Подновена	Тахографската карта е подновена поради промяна на административните данни или защото срокът ѝ на валидност изтича. Номерът на новата карта е същият, с изключение на това, че индексът за замяна в номера на картата е увеличен с единица.
В процес на замяна	ОКИК, който е издал дадена карта на водач, е получил уведомление, че е започнала процедура за замяна на въпросната карта с карта на водач, издадена от ОКИК на друга страна.
Заменена	ОКИК, който е издал дадена карта на водач, е получил уведомление, че процедурата за замяна на въпросната карта с карта на водач, издадена от ОКИК на друга страна, е приключила.

Поддопълнение 4.3

Разпоредби относно съобщенията по TACHOnet

1. Общи технически изисквания

1.1. Централният възел трябва да осигурява както синхронен, така и асинхронен интерфейс за обмен на съобщения. Страните имат възможност да изберат интерфейса с най-подходящата технология за свързване със своите приложения.

1.2. Всички съобщения, обменяни между централния възел и националните системи, трябва да са кодирани в UTF-8.

1.3. Националните системи трябва да могат да получават и обработват съобщения, съдържащи букви от гръцката азбука или кирилица.

2. Структура и определяне на схемата (XSD) на съобщенията XML

2.1. Общата структура на съобщенията XML трябва да е в съответствие с формата, определен от схемите XSD, инсталирани в централния възел.

2.2. Централният възел и националните системи трябва да предават и приемат съобщения, които отговарят на схемата XSD на съобщението.

2.3. Националните системи трябва да могат да изпращат, получават и обработват всички съобщения, съответстващи на някоя от функционалните възможности, определени в поддопълнение 4.2.

2.4. Съобщенията XML трябва да включват най-малкото минималните изисквания, определени в таблица 2.

Таблица 2

Минимални изисквания към съдържанието на XML съобщенията

Обща заглавна част		**Задължително**
Версия	Официалната версия на спецификациите XML ще се посочва посредством мястото за име, определено в XSD на съобщението, както и в атрибута за *версията* на заглавния елемент на всяко съобщение XML. Номерът на версията („n.m“) ще се определя като постоянна стойност във всяка версия на файла за определяне на схемата на XML (xsd).	Да
Идентификатор при изпитване	Незадължителен идентификатор при изпитване. Инициаторът на изпитването попълва идентификатора и всички участници в работния процес препращат/връщат същия идентификатор. При реална работа той следва да бъде игнориран и не се използва, ако е предоставен.	Не
Технически идентификатор	Универсален уникален идентификатор (UUID), който еднозначно определя всяко отделно съобщение. Подателят генерира UUID и попълва този атрибут. Тези данни не се използват със стопанска цел.	Да
Идентификатор на работния процес	Идентификаторът на работния процес (workflowId) представлява UUID и следва да бъде генериран от запитващата страна. Този идентификатор се използва след това във всички съобщения с цел взаимовръзка с работния процес.	Да
Изпратено в	Датата и часът (UTC) на изпращане на съобщението.	Да
Срок на изтичане	Това е незадължителен атрибут за дата и време (във формат UTC). Тази стойност се задава само от централния възел за препратени запитвания. Тя информира отговарящата страна за момента, в който запитването изтича. Тази стойност не се изисква в MS2TCN_<x>_Req и във всички съобщения за отговор. Тя не е задължителна, така че за всички видове съобщения може да се използва една и съща заглавна част, независимо от това дали се изисква атрибутът timeoutValue.	Не
От	Кодът по ISO 3166-1 Alpha 2 на страната, изпращаща съобщението, или „ЕС“.	Да
До	Кодът ISO 3166-1 Alpha 2 на страната, до която се изпраща съобщението, или „ЕС“.	Да

Поддопълнение 4.4

Услуги по транслитерация и NYSIIS (Система на щата Ню Йорк за идентификация и информация)

1. Алгоритъмът NYSIIS, въведен на централния възел, се използва за кодиране на имената на всички водачи в националния регистър.

2. При търсене на карта посредством функционалната възможност CIC като основен метод за търсене трябва да се използват ключовете NYSIIS.

3. В допълнение страните могат да използват индивидуализиран алгоритъм с цел намиране на допълнителни резултати.

4. В резултатите от търсенето трябва да е посочен методът на търсене, който е използван за намирането на даден запис — NYSIIS или индивидуализиран.

5. Ако дадена страна реши да записва уведомления ICDL, ключовете NYSIIS, съдържащи се в уведомлението, се записват като част от данните за ICDL. При търсене на данните за ICDL страната трябва да използва ключовете NYSIIS на името на заявителя.

Поддопълнение 4.5

Изисквания за сигурност

1. За обмена на съобщения между централния възел и националните системи се използва HTTPS.

2. Националните системи използват цифровите сертификати, посочени в поддопълнения 4.8 и 4.9, за целите на сигурността на предаването на съобщения между националната система и централния възел.

3. Националните системи използват, като минимум, сертификати с алгоритъм SHA-2 (SHA-256) за хеширане на подписа и публичен ключ с дължина 2048 бита.

Поддопълнение 4.6

Нива на обслужване

1. Националните системи трябва да осигуряват следното минимално ниво на обслужване:

1.1. Те трябва да са разполагаеми 24 часа в денонощието, 7 дни в седмицата.

1.2. Разполагаемостта им трябва да се следи чрез генерирането от централния възел на периодично съобщение за състоянието.

1.3. Степента им на разполагаемост трябва да бъде 98 % в съответствие със следната таблица (стойностите са закръглени до най-близката подходяща единица):

Разполагаемост от	означава неразполагаемост от		
	Дневно	Месечно	Годишно
98 %	0,5 часа	15 часа	7,5 дни

Страните се насърчават да спазват дневния процент на разполагаемост, но въпреки това се признава, че определени необходими дейности, например поддръжка на системата, изискват прекъсвания в работата за повече от 30 минути. Спазването на месечния и годишния процент на разполагаемост обаче е задължително.

1.4. Те трябва да отговарят на най-малко на 98 % от запитванията, изпратени до тях за един календарен месец.

1.5. Те трябва да отговорят на запитването до 10 секунди.

1.6. Общият срок на изтичане на запитването (времето през което запитващата страна може да чака отговор) не трябва да надвишава 20 секунди.

1.7. Те трябва да могат да обслужват по 6 запитвания в секунда.

1.8. Националните системи нямат право да изпращат запитвания до централния възел на TACHOnet с честота над 2 запитвания в секунда.

1.9. Всяка национална система трябва да може да се справя с евентуални технически проблеми в централния възел или в националните системи на други страни. Това включва, но не се ограничава до:

а) загуба на връзката с централния възел;

б) не се получава отговор на запитване;

в) получаване на отговор след изтичане на срока на съобщението;

г) получаване на непоискани съобщения;

д) получаване на невалидни съобщения.

2. Централният възел трябва:

2.1. да осигурява степен на разполагаемост от 98 %;

2.2. да предоставя на националните системи уведомления за евентуални грешки, или чрез съобщението за отговор или чрез специално за целта съобщение за грешка. Националните системи на свой ред трябва да приемат тези специални съобщения за грешка и да имат механизъм за интензифициране на работния процес, с цел да бъдат предприети подходящи действия за коригиране на съобщената грешка.

3. Поддръжка

Страните трябва да уведомяват другите страни и Комисията за всички планови дейности по поддръжка посредством уебприложението най-малко една седмица преди началото на тези дейности, ако това е възможно технически.

Поддопълнение 4.7

Регистриране при достъп и статистика на данните, събирани в централния възел

1. С цел гарантиране на правото на личен живот, данните за статистически цели трябва да са анонимни. Данни, идентифициращи конкретна карта, водач или свидетелство за управление не трябва да са достъпни за статистически цели.

2. Данните за регистрирането при достъп трябва да съдържат информация за всички сесии за целите на мониторинга и отстраняването на грешки, както и да позволяват съставянето на статистики за тези сесии.

3. Личните данни не трябва да се съхраняват в регистрите в продължение на повече от 6 месеца. Статистическата информация трябва да се съхранява без краен срок.

4. Статистическите данни, използвани за докладване, трябва да включват:

   а) запитващата страна;

   б) отговарящата страна;

   в) вида на съобщението;

   г) кода за статуса на отговора;

   д) датата и часа на съобщенията;

   е) часа на изпращането на отговора.

Поддопълнение 4.8

Общи разпоредби относно цифровите ключове и сертификати за TACHOnet

1. Генерална дирекция „Информатика“ на Европейската комисия посредством eDelivery предоставя услуга за ИПК[1] (наричана „услуга на МСЕ за ИПК“) на договарящите страни по AETR, които се свързват с TACHOnet (наричани по-нататък „националните органи“).

2. Процедурата за искане и оттегляне на цифрови сертификати, както и подробните правила и условия за нейното използване, са определени в допълнението.

3. Използване на сертификатите:

3.1. След издаването на сертификата националният орган[2] използва сертификата само в контекста на TACHOnet. Сертификатът може да се използва за:

а) удостоверяване на произхода на данните;

б) криптиране на данни;

в) осигуряване на откриването на нарушавания в целостта на данните.

3.2. Всяка употреба, която не е изрично разрешена като част от разрешеното използване на сертификата, е забранена.

4. Договарящите страни:

а) защитават своя частен ключ срещу неразрешено използване;

б) се въздържат да прехвърлят или разкриват своя частен ключ на трети страни, дори като представители;

---

1 ИПК (Инфраструктура за публични ключове) представлява набор от роли, политики, процедури и системи, необходими за създаване, управление, разпространение и оттегляне на цифрови сертификати.

2 Идентифициран от стойността на атрибута „O =“ в Subject Distinguished Name на издадения сертификат

в) осигуряват поверителност, цялост и наличност на частните ключове, генерирани, съхранявани и използвани за TACHOnet;

г) се въздържат от продължаващо използване на частния ключ след изтичане на срока на валидност или оттегляне на сертификата, с изключение на разглеждането на криптирани данни (напр. декриптиране на електронни писма). Ключовете с изтекъл срок, или се унищожават, или се съхраняват по начин, предотвратяващ използването им;

д) предоставят на регистриращия орган самоличностите на упълномощените представители, които имат право да искат оттеглянето на сертификати, издадени на организацията (заявленията за оттегляне съдържат парола за заявлението за оттегляне и подробности относно събитията, водещи до оттегляне);

е) предотвратяват злоупотребата с частния ключ, като поискат отменянето на сертификата на съответния публичен ключ в случай на компрометиране на частния ключ или на данните за активиране на частния ключ.

ж) отговорни са и спазват задължението да поискат отменяне на сертификата при обстоятелствата, посочени в политиките за сертифициране (ПС) и декларацията за практиките по сертифициране (ДПС) на сертифициращия орган;

з) без забавяне уведомяват регистриращия орган при загуба, кражба или евентуалното компрометиране на някой от ключовете за AETR, използвани в контекста на TACHOnet.

5. Отговорности

Без да се засяга отговорността на Европейската комисия при нарушаване на изисквания, определени в приложимото национално право, или по отношение на отговорността за действия, които не могат да бъдат изключени от това право, Европейската комисия не може да е отговорна или да носи отговорност по отношение на:

а) съдържанието на сертификата, отговорността за което е изключително на собственика на сертификата. Задължение на собственика на сертификата е да провери точността на съдържанието на сертификата;

б) използването на сертификата от неговия собственик.

Поддопълнение 4.9

Описание на услугата ИПК за TACHOnet

1. Въведение

ИПК (Инфраструктура за публични ключове) представлява набор от роли, политики, процедури и системи, необходими за създаване, управление, разпространение и оттегляне на цифрови сертификати[3]. Услугата на МСЕ за ИПК, предоставяна от eDelivery, позволява издаването и управлението на цифрови сертификати, използвани за осигуряване на поверителност, цялост и невъзможността за променяне на информацията, обменяна между точките за достъп (ТД).

Услугата ИПК, предоставяна от eDelivery, се основава на Trust Center Services TeleSec Shared Business CA (сертифициращ орган), за който се прилага политиката за сертифициране (ПС) / декларацията за практиките по сертифициране (ДПС) на сертифициращия орган TeleSec Shared-Business-CA, предлаган от T-Systems International GmbH[4].

Услугата ИПК издава сертификати, които са подходящи за подсигуряване на различни стопански процеси във и извън дружествата, организациите, публичните органи и институции, които изискват средно ниво на сигурност за доказване на автентичността, целостта и надеждността на крайния субект.

2. Процес на подаване на заявление за сертификат

2.1. Роли и отговорности

2.1.1. „Организация“ или „национален орган“, подаващи заявление за сертификат

2.1.1.1. Националният орган трябва да поиска сертификатите в контекста на проекта TACHOnet.

2.1.1.2 Националният орган:

а) поисква сертификатите от услугата на МСЕ за ИПК;

---

3 https://en.wikipedia.org/wiki/Public_key_infrastructure

4 Последната версия на ПС и ДПС може да бъде изтеглена на https://www.telesec.de/en/sbca-en/support/download-area/

б) генерира частните ключове и съответните публични ключове, които да бъдат включени в издадените от сертифициращия орган сертификати;

в) изтегля сертификата, когато бъде одобрен;

г) подписва и изпраща обратно на регистриращия орган:

i) идентификационния формуляр за лицата за контакт и доверените куриери,

ii) подписаното индивидуално пълномощно[5].

2.1.2. Доверен куриер

2.1.2.1. Националният орган определя доверен куриер.

2.1.2.2. Довереният куриер:

а) предава публичния ключ на регистриращия орган по време на процеса на идентификация и регистрация лице в лице;

б) получава съответния сертификат от регистриращия орган.

2.1.3. Собственик на домейн

2.1.3.1. Собственикът на домейн е ГД „Мобилност и транспорт“.

2.1.3.2. Собственикът на домейн:

а) валидира и координира мрежата TACHOnet и архитектурата за доверителност на TACHOnet, включително валидиране на процедурите за издаване на сертификати;

б) експлоатира централния възел на TACHOnet и координира дейността на страните по отношение на функционирането на TACHOnet;

в) извършва, заедно с националните органи, изпитванията за свързване към TACHOnet.

---

5 Пълномощното представлява правен документ, чрез който организацията упълномощава и разрешава на Европейската комисия, представлявана от посоченото длъжностно лице, отговорно за услугата на МСЕ за ИПК, да поиска генерирането на сертификат от нейно име от сертифициращия орган TeleSec Shared Business CA на T-Systems International GmbH. Вж. също така точка 6.

2.1.4. Регистриращ орган

2.1.4.1. Регистриращият орган е Съвместният изследователски център (СИЦ).

2.1.4.2. Регистриращият орган отговаря за проверката на самоличността на доверения куриер, за регистрирането и одобряването на заявленията за издаване, оттегляне и подновяване на цифрови сертификати.

2.1.4.3. Регистриращият орган:

а) присвоява уникалния идентификатор на националния орган;

б) удостоверява самоличността на националния орган, неговите точки за контакт и доверени куриери;

в) осъществява връзка с помощния екип за МСЕ по отношение на автентичността на националния орган, неговите точки за контакт и доверените куриери;

г) информира националния орган за одобряването или отхвърлянето на даден сертификат.

2.1.5. Сертифициращ орган

2.1.5.1. Сертифициращият орган отговаря за осигуряването на техническата инфраструктура за подаването на заявление, издаването и оттеглянето на цифрови сертификати.

2.1.5.2. Сертифициращият орган:

а) осигурява техническата инфраструктура за подаването на заявление за издаване на сертификати от страна на националните органи;

б) валидира или отхвърля дадено заявление за сертификат;

в) когато е необходимо комуникира с регистриращия орган във връзка с проверката на самоличността на организацията заявител.

2.2. Издаване на сертификати

2.2.1. Издаването на сертификата се извършва в съответствие със следните последователни стъпки, представени на фигура 1:

а) **Стъпка 1:** Идентифициране на доверения куриер;

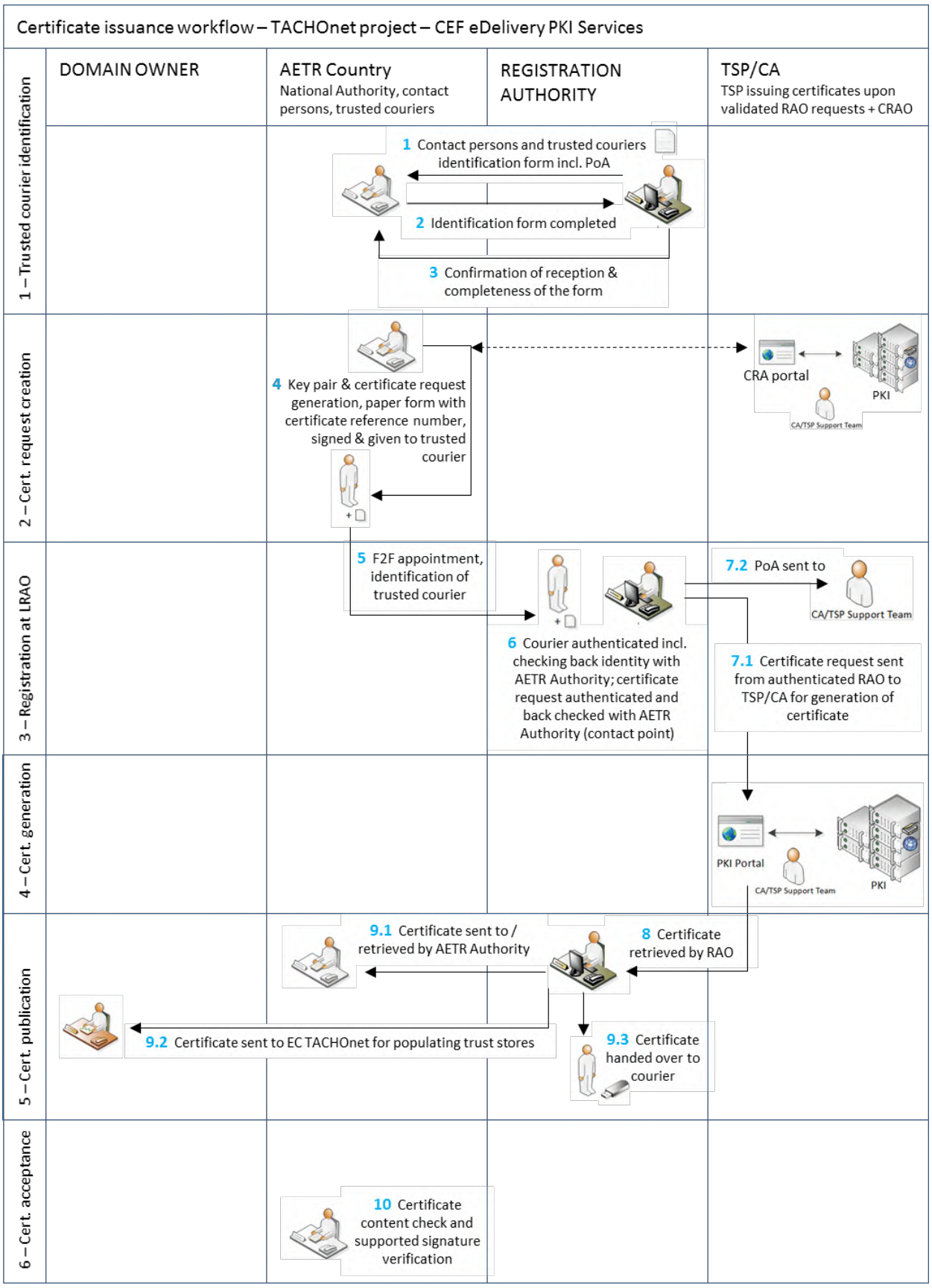
б) **Стъпка 2:** Създаване на заявлението за издаване на сертификат;

в) **Стъпка 3**: Регистриране в регистриращия орган;

г) **Стъпка 4:** Генериране на сертификата;

д) **Стъпка 5:** Публикуване на сертификата;

е) **Стъпка 6:** Приемане на сертификата.



Фигура 1 — Работен процес по издаването на сертификати

2.2.2. Стъпка 1: Идентифициране на доверения куриер

Следната процедура се извършва с цел идентифициране на доверения куриер:

а) Регистриращият орган изпраща на националния орган идентификационния формуляр на лицата за контакт и доверените куриери[6]. Този формуляр включва също така пълномощното, което организацията (управляващият орган на AETR) подписва.

б) Националният орган изпраща обратно на регистриращия орган попълнения формуляр и подписаното пълномощно.

в) Регистриращият орган потвърждава приемането и пълнотата на формуляра.

г) Регистриращият орган предоставя на собственика на домейн актуализирано копие на списъка на лицата за контакт и доверените куриери.

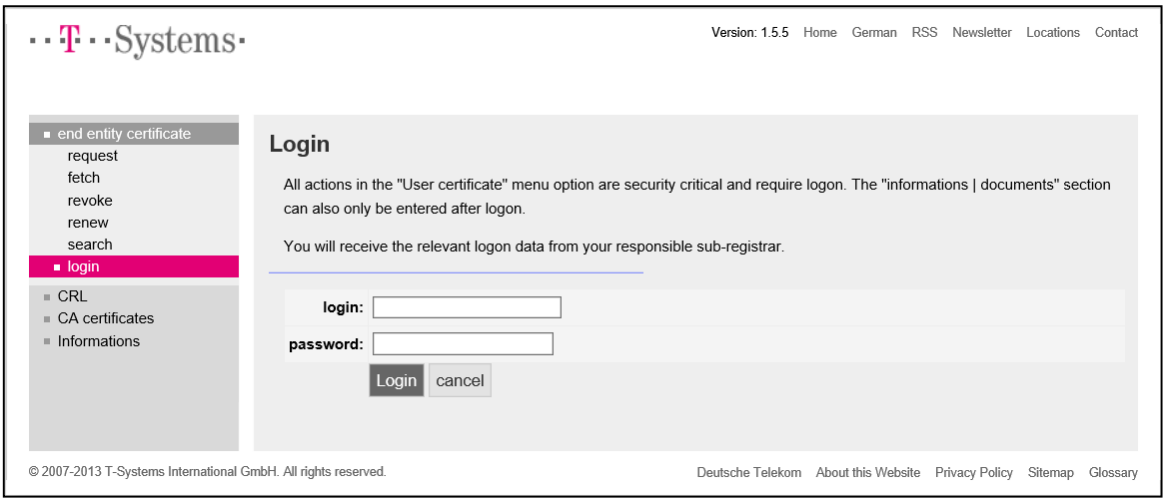
2.2.3. Стъпка 2: Създаване на заявлението за издаване на сертификат

2.2.3.1. подаването на заявлението и получаването на сертификата се извършват на един и същ компютър и с един и същ браузър.

2.2.3.2. За създаването на заявление за издаване на сертификат се извършва следният процес:

а) Организацията отива на потребителския уебинтерфейс, за да поиска сертификата на URL адрес https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: като въвежда потребителско име „**sbca/CEF_eDelivery.europa.eu**“ и парола „**digit.333**“

[6] Вж. точка 5

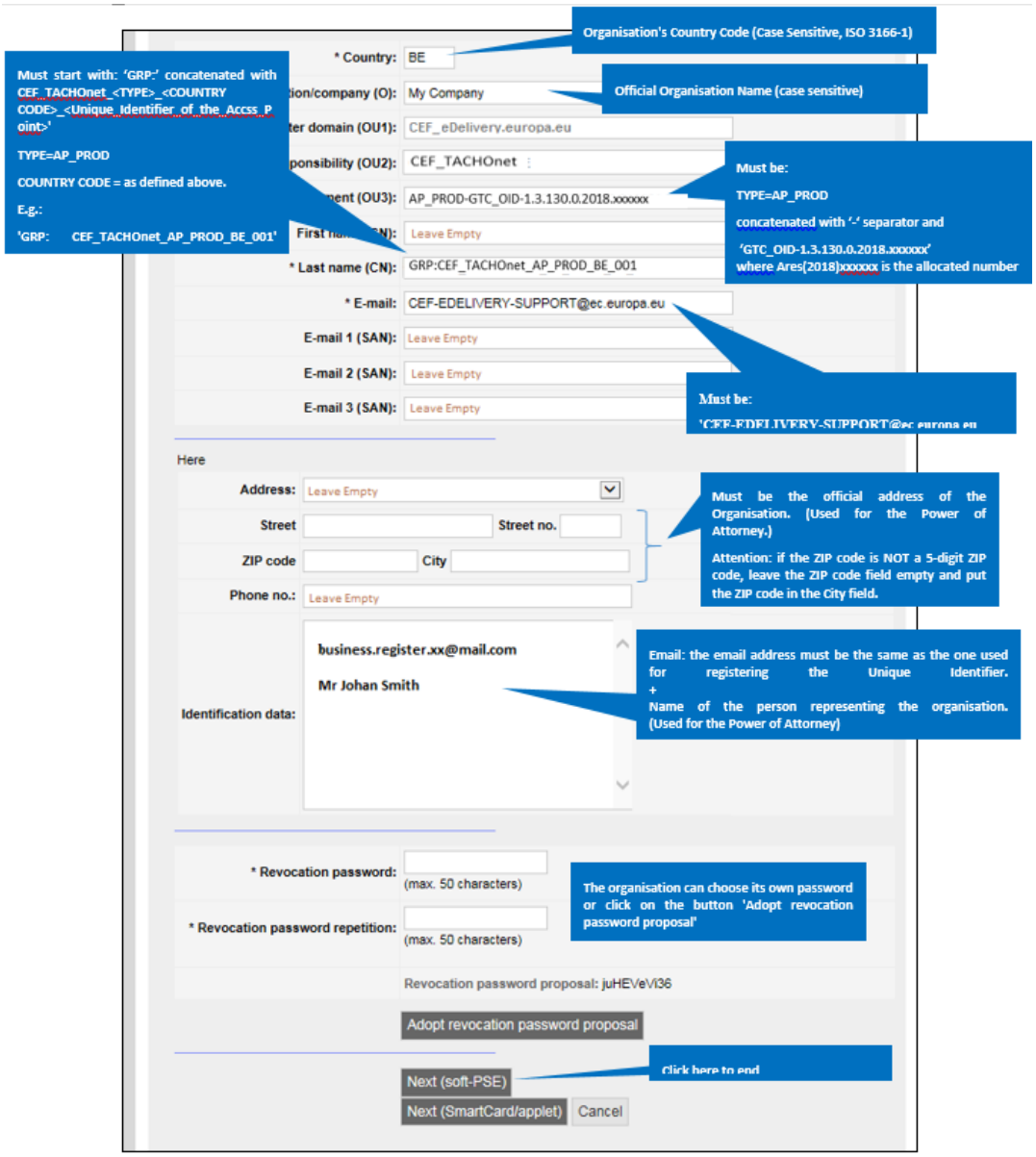


Фигура 2

б) Организацията натиска бутона „request“ в лявата страна на екрана и избира „CEF_TACHOnet“ от падащия списък.

Фигура 3

в) Организацията попълва формуляра за подаване на заявление за сертификат, показан на фигура 4, с информацията в таблица 3, като за завършване на процеса натиска бутона „Next (soft-PSE)“.


Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'
Must be:
TYPE=AP_PROD
concatenated with '-' separator and
'GTC_OID-1.3.130.0.2018.xxxxxx'
where Ares(2018)xxxxxx is the allocated number
Must be:
'CEF-EDELIVERY-SUPPORT@ec.europa.eu
Must be the official address of the Organisation. (Used for the Power of Attorney.)
Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.
Email: the email address must be the same as the one used for registering the Unique Identifier.
+
Name of the person representing the organisation. (Used for the Power of Attorney)
The organisation can choose its own password or click on the button 'Adopt revocation password proposal'
Click here to end
* Country:
BE
My Company
CEF_eDelivery.europa.eu
CEF_TACHOnet
AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Leave Empty
GRP:CEF_TACHOnet_AP_PROD_BE_001
CEF-EDELIVERY-SUPPORT@ec.europa.eu
E-mail 1 (SAN):
E-mail 2 (SAN):
E-mail 3 (SAN):
Here
Address:
Street
Street no.
ZIP code
City
Phone no.:
Identification data:
business.register.xx@mail.com
Mr Johan Smith
* Revocation password:
(max. 50 characters)
* Revocation password repetition:
(max. 50 characters)
Revocation password proposal: juHEVeVi36
Adopt revocation password proposal
Next (soft-PSE)
Next (SmartCard/applet)
Cancel

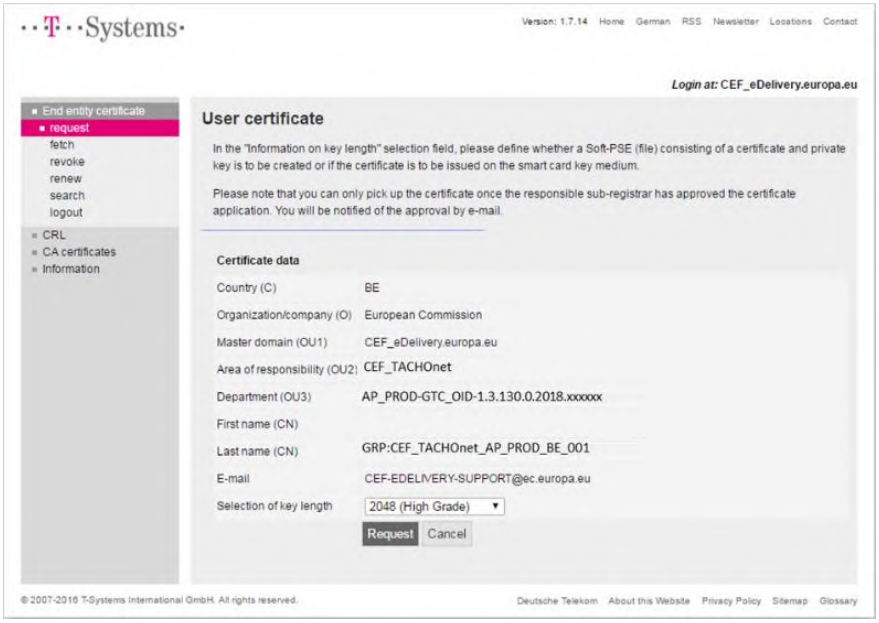
Фигура 4

Изисквани полета	Описание
Държава	**C = код на държавата**, местонахождение на собственика на сертификата, проверено посредством публичен указател; Ограничения: 2 знака, в съответствие със стандарт ISO 3166—1, alpha-2, регистърът на буквите има значение; Примери: DE, BE, NL, Особени случаи: UK (за Великобритания), EL (за Гърция)
Организация/Дружество (O)	**O = име на организацията на собственика на сертификата**
Главен домейн (OU1)	**OU = CEF_eDelivery.europa.eu**
Област на отговорност (OU2)	**OU = CEF_TACHOnet**
Отдел (OU3)	Задължителна стойност за „AREA OF RESPONSIBILITY“ Когато се прави заявление за сертификат, съдържанието трябва да се провери, като се използва положителен списък (бял списък). Ако информацията не отговаря на тази от списъка, заявлението се отхвърля. Формат: **OU=<TYPE>-<GTC_NUMBER>** Където „< TYPE>“, се заменя с AP_PROD: Access Point in Production environment (точка за достъп в работната среда). И където < GTC_NUMBER > е **GTC_OID 1.3.130.0.2018.xxxxxx**, където Ares(2018)xxxxxx е номер GTC на проекта TACHOnet. напр.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Собствено име (CN)	Трябва да бъде празно
Фамилно име (CN)	Трябва да започва с „GRP:“, последвано от общоприето наименование. Формат: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** напр.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-поща	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-поща 1 (SAN)	Трябва да бъде празно
E-поща 2 (SAN)	Трябва да бъде празно
E-поща 3 (SAN)	Трябва да бъде празно

Адрес	Трябва да бъде празно
Улица	Трябва да бъде официалният адрес на организацията на собственика на сертификата. (използваната за пълномощното)
Улица №	Трябва да бъде официалният адрес на организацията на собственика на сертификата. (използваният за пълномощното)
Пощенски код	Трябва да бъде официалният адрес на организацията на собственика на сертификата. (използваният за пълномощното) **Внимание**: ако пощенският код не е 5-цифрено число, полето за пощенския код се оставя празно, а пощенският код се въвежда в полето за името на града.
Град	Трябва да бъде официалният адрес на организацията на собственика на сертификата. (използваният за пълномощното) **Внимание**: ако пощенският код не е 5-цифрено число, полето за пощенския код се оставя празно, а пощенският код се въвежда в полето за името на града.
Тел.:	Трябва да бъде празно
Идентификационни данни	Адресът за електронна поща трябва да бъде същият като използвания за регистрирането на уникалния идентификатор. + Трябва да бъде името на лицето, представляващо организацията. (използвано за пълномощното) + **№ в търговския регистър** (това е задължително само за частните организации) **Вписан в местния съд на** (изисква се само за частни немски и австрийски организации)
Парола за оттеглянето	Задължително поле, попълнено от подателя на заявлението
Повторно въвеждане на паролата за оттеглянето	Задължително поле, попълнено от подателя на искането, повтаря се

Таблица 3. Пълни подробности за всяко необходимо поле

г) Избраната дължина на ключа е 2048(High Grade).



Фигура 5

д) Организацията записва референтния номер, за да получи сертификата.

Фигура 6

е) Помощният екип за МСЕ проверява за нови заявления за сертификати и проверява дали информацията в заявлението за издаване на сертификат е валидна, т.е. дали съответства на правилата за наименуване, посочени в допълнение 5.1 Конвенция за наименуване на сертификати.

ж) Помощният екип за МСЕ проверява дали информацията, въведена в заявлението, е във валиден формат.

з) Когато при проверката по точки 5 или 6 по-горе се установи грешка, помощният екип за МСЕ изпраща електронно писмо до адреса за електронна поща, посочен в „Идентификационните данни“ на формуляра за заявлението, а в копие се посочва собственикът на домейна, с което организацията се приканва да започне процеса отново. Неуспешното заявление за издаване на сертификат се анулира.

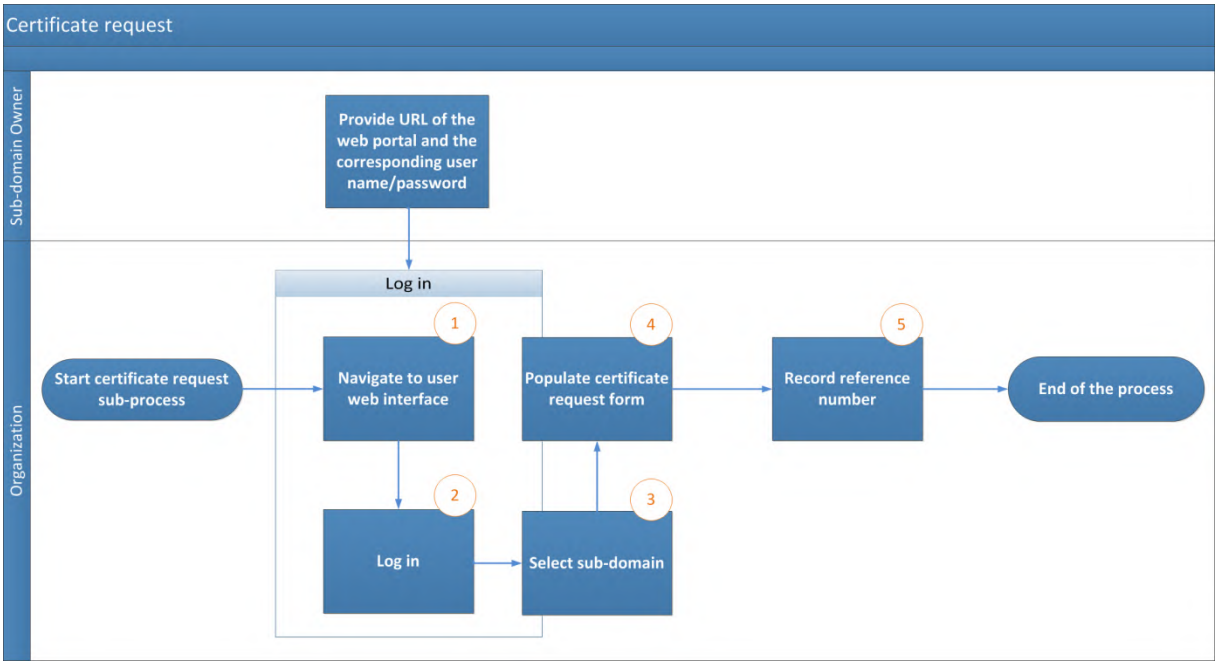
и) Помощният екип за МСЕ изпраща електронно писмо на регистриращия орган относно валидността на заявлението. Електронното писмо включва:

(1) наименованието на организацията, намиращо се в полето „Организация (O)“ на заявлението за сертификат;

(2) данните за сертификата, включително името на ТД, за което се издава сертификатът, намиращо се в поле „Last Name (CN)“ (фамилия) на заявлението за сертификат;

(3) референтния номер на сертификата

(4) адреса на организацията, адреса ѝ за електронна поща и името на лицето, което я представлява.



Фигура 7 — Процес на подаване на заявление за сертификат

2.2.4. Стъпка 3: Регистрация в регистриращия орган (Одобряване на сертификата)

2.2.4.1. Довереният куриер или точката за контакт уреждат среща с регистриращия орган чрез обмен на електронни писма, като се посочва довереният куриер, който ще осъществи срещата лице в лице.

2.2.4.2. Организацията изготвя пакета документи, състоящ се от:

а) попълненото и подписано пълномощно;

б) копие от валидния паспорт на доверения куриер, който ще осъществи срещата лице в лице. Това копие трябва да бъде подписано от една от точките за контакт на организацията, посочени в стъпка 1;

в) хартиения формуляр със заявлението за издаване на сертификат, попълнен и подписан от една от точките за контакт на организацията.

2.2.4.3. Регистриращият орган приема доверения куриер след проверка на самоличността в приемната част на сградата. Регистриращият орган извършва регистрацията на заявлението за издаване на сертификат лице в лице, като:

а) идентифицира и удостоверява самоличността на доверения куриер;

б) проверява физическите черти на доверения куриер по паспорта, представен от доверения куриер;

в) проверява валидността на паспорта, представен от доверения куриер;

г) проверява валидирания паспорт, представен от доверения куриер, спрямо копието от валидния паспорт на доверения куриер, подписано от една от посочените точки за контакт на организацията. Автентичността на подписа се удостоверява спрямо оригиналния „идентификационен формуляр на доверения куриер и точките за контакт“;

д) проверява попълненото и подписано пълномощно;

е) проверява хартиения формуляр със заявлението за издаване на сертификат и подписа върху него спрямо оригиналния „идентификационен формуляр на доверения куриер и точките за контакт“;

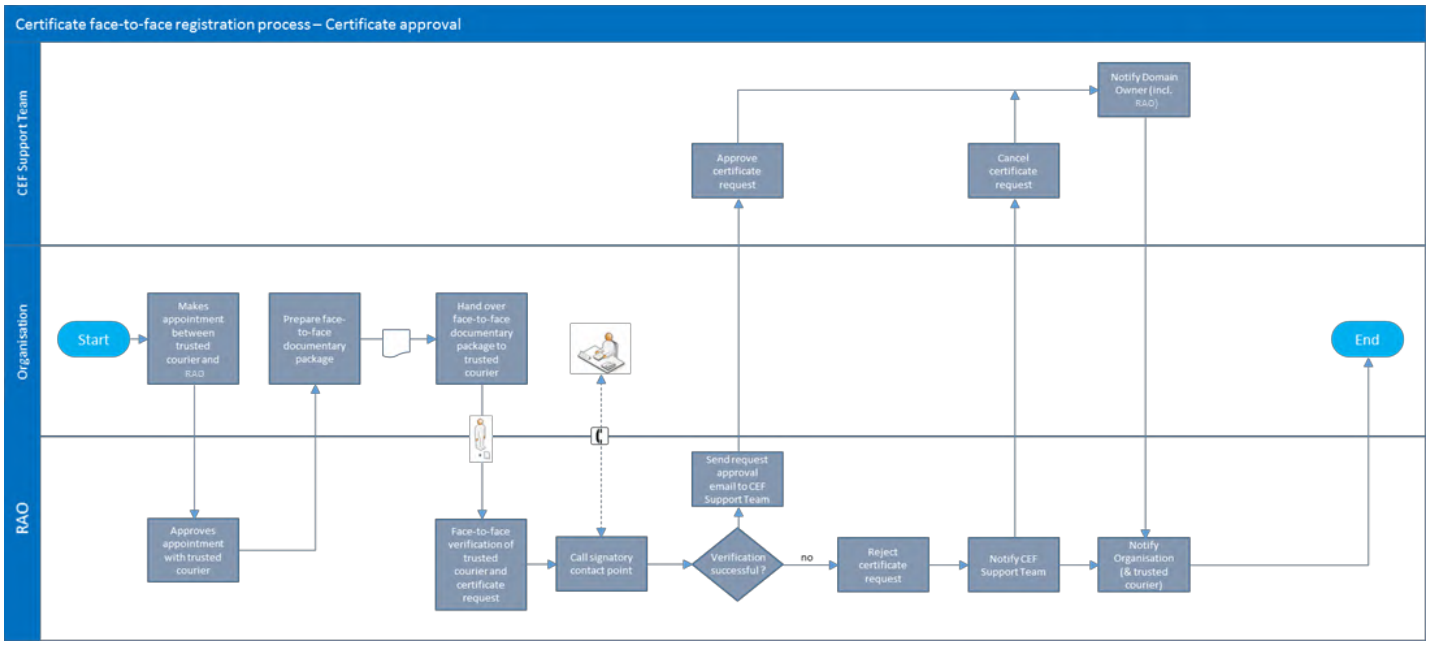
ж) приканва поставилата подписа си точка за контакт отново да провери самоличността на доверения куриер и съдържанието на заявлението за издаване на сертификат.

2.2.4.4. Регистриращият орган потвърждава на помощния екип за МСЕ, че националният орган наистина е упълномощен да управлява компонентите, за които иска сертификатите, и че съответният процес на регистриране лице в лице е бил успешен. Потвърждението се изпраща чрез защитено електронно писмо със сертификат „CommiSign“, като се прикачва сканирано копие на удостоверения лице в лице пакет документи и на подписания от регистриращия орган списък за проверка на процеса.

2.2.4.5. Ако регистриращият орган потвърди валидността на заявлението, процесът продължава съгласно определеното в точки 2.2.4.6 и 2.2.4.7. В противен случай издаването на сертификата се отхвърля и организацията се уведомява за това.

2.2.4.6. Помощният екип за МСЕ одобрява заявлението за сертификат и уведомява регистриращия орган за одобряването на сертификата.

2.2.4.7. Регистриращият орган уведомява организацията за това, че сертификатът може да бъде изтеглен от потребителския портал.



Фигура 8 — Одобряване на сертификата

2.2.5. Стъпка 4: Генериране на сертификата

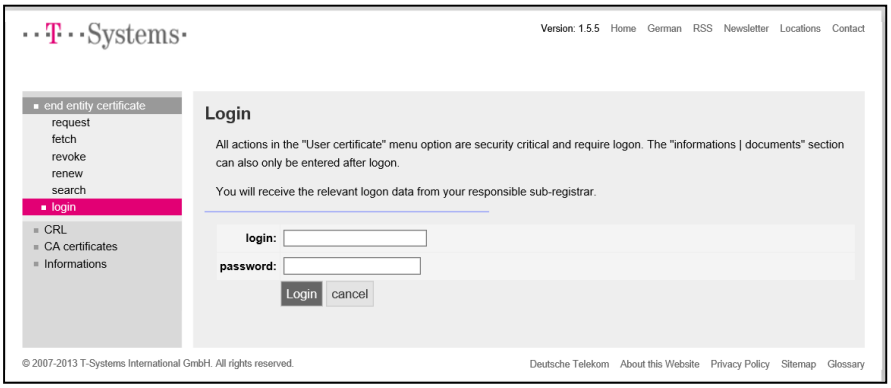
След одобряването на заявлението за сертификат, се пристъпва към генериране на сертификата.

2.2.6. Стъпка 5: Публикуване и изтегляне на сертификата

2.2.6.1. След одобряването на заявлението за издаване на сертификат, регистриращият орган изтегля сертификата и предава копие на доверителния куриер.

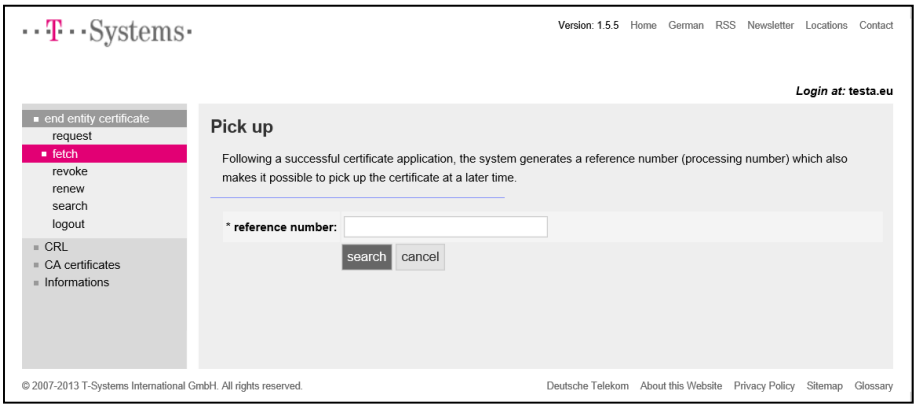
2.2.6.2. Организацията получава уведомление от регистриращия орган, че сертификатите могат да бъдат изтеглени. Организацията отива на потребителския портал на следния адрес:

2.2.6.3. Организацията отива на потребителския портал на следния адрес: https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en и се регистрира с потребителското име „**sbca/CEF_eDelivery.europa.eu**“ и паролата „**digit.333**“.



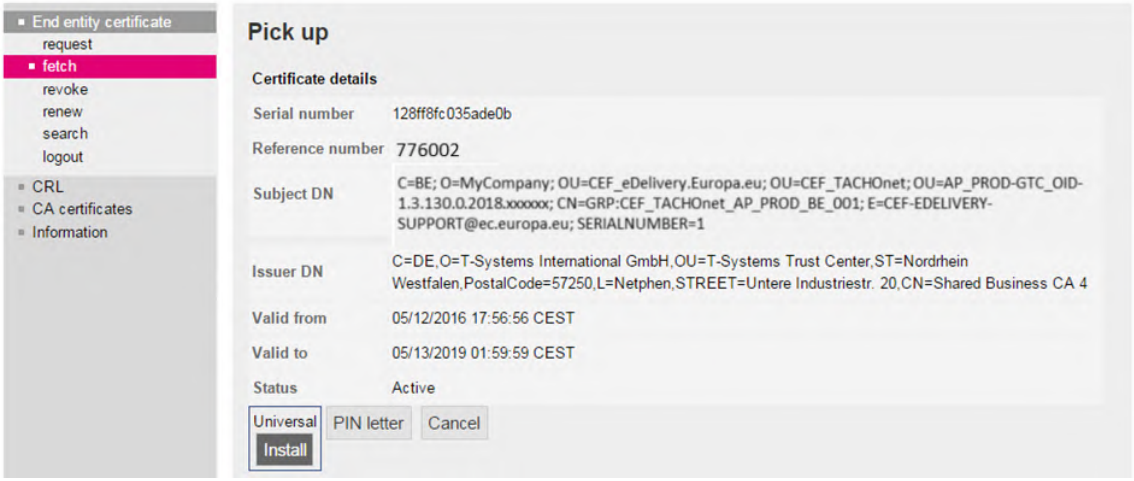
Фигура 9

2.2.6.4. Организацията натиска бутона „fetch“ вляво и въвежда референтния номер, записан в процеса на подаване на заявлението за издаване на сертификат;



Фигура 10

2.2.6.5. Организацията инсталира сертификатите, като натиска бутона за инсталиране.



Фигура 11

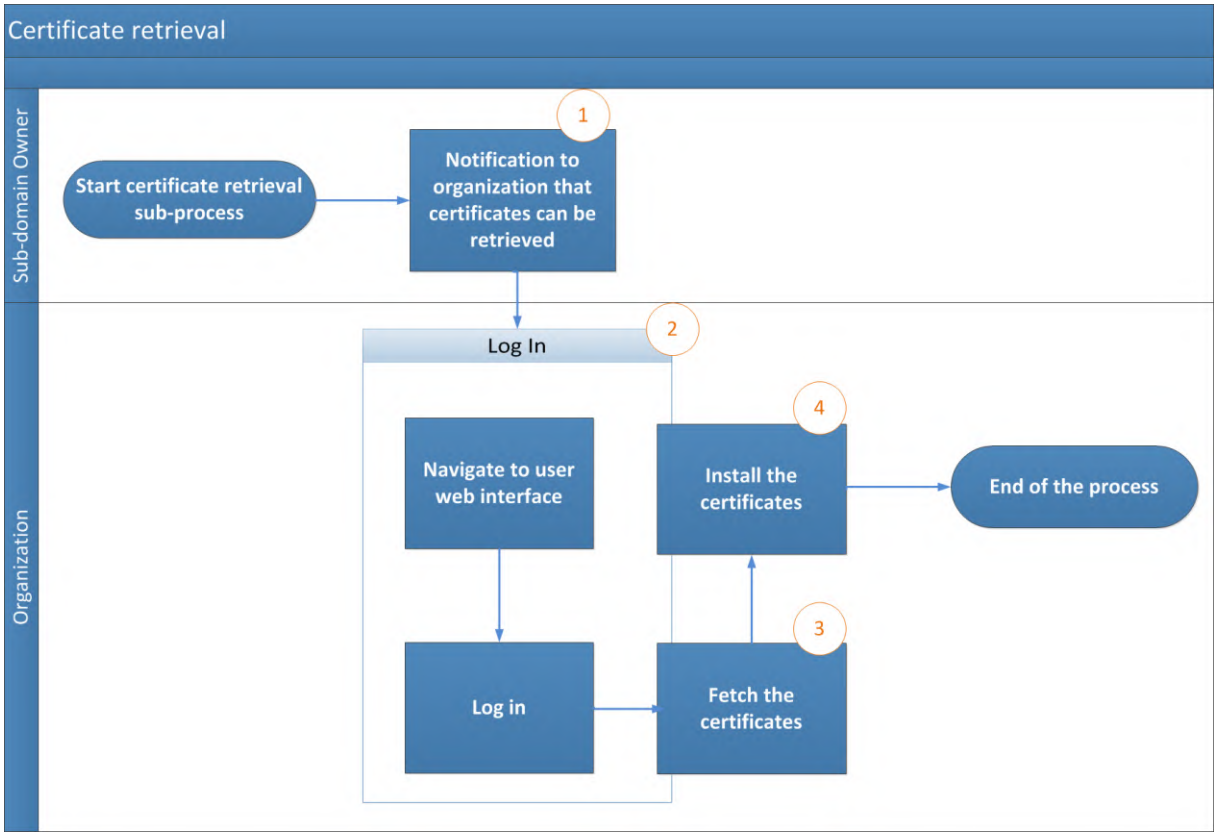
2.2.6.6. Сертификатът се инсталира на точката за достъп. Тъй като това е специфичен процес, организацията се обръща към своя доставчик на точката за достъп, за да получи описанието на този процес.

2.2.6.7. За инсталирането на сертификати в точката за достъп са необходими следните стъпки:

а) експортиране на частния ключ и сертификата,

б) създаване на keystore и truststore,

в) инсталиране на keystore и truststore на точката за достъп.

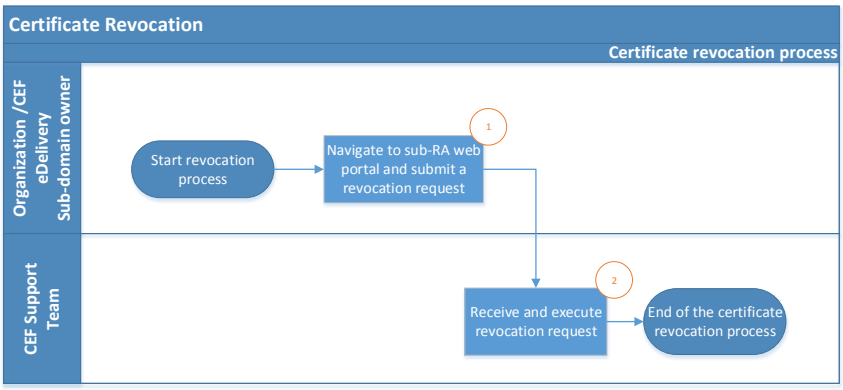


Фигура 12 — Изтегляне на сертификата

3. Процес на отменяне на сертификат

3.1. Организацията подава искане за отменяне чрез потребителския уебпортал;

3.2. Помощният екип за MCE отменя сертификата.



Фигура 13 — Отменяне на сертификат

4. Общи правила и условия за услугата на МСЕ за ИПК

4.1. Контекст

В качеството си на доставчик на решения за модула eDelivery на Механизма за свързване на Европа, ГД „Информатика“ предоставя услугата за ИПК[7] („услуга на МСЕ за ИПК“) на договарящите страни по AETR. Услугата на МСЕ за ИПК се използва от националните органи („крайните потребители“), участващи в TACHOnet.

ГД „Информатика“ притежава ИПК в рамките на решението за сертифициращ орган TeleSec Shared-Business-CA („SBCA“), който се експлоатира в доверителния център на звеното в групата T-Systems International GmbH („T-Systems“[8]). ГД „Информатика“ играе ролята на главен регистратор на домейна „CEF_eDelivery.europa.eu“ на SBCA. В тази роля за всеки проект ГД „Информатика“ създава поддомейни в рамките на домейна „CE_eDelivery.europa.eu“, като използва услугата на МСЕ за ИПК.

В настоящия документ са представени подробности за правилата и условията на поддомейна TACHOnet. ГД „Информатика“ изпълнява ролята на подрегистратор на този поддомейн. В това качество тя издава, оттегля и подновява сертификатите за този проект.

4.2. Отказ от отговорност

Европейската комисия не отговаря и не носи никаква отговорност по отношение на съдържанието на сертификата, отговорността за което е изключително на собственика на сертификата. Собственикът на сертификата отговаря за проверката на точността на съдържанието на сертификата.

Европейската комисия не отговаря и не носи никаква отговорност по отношение на използването на сертификата от неговия собственик в качеството му на трето юридическо лице извън Европейската комисия.

---

7 ИПК (Инфраструктура за публични ключове) представлява набор от роли, политики, процедури и системи, необходими за създаване, управление, разпространение и оттегляне на цифрови сертификати.

8 Доверената роля на оператора на доверителния център, разположен в доверителния център на T-Systems, също така включва функцията на вътрешен регистриращ орган.

Настоящият отказ от отговорност няма за цел да ограничи отговорността на Комисията при нарушаване на изисквания, определени в приложимото национално право, или да изключи отговорността ѝ по отношение на действия, които не могат да бъдат изключени от това право.

4.3. Разрешени/забранени употреби на сертификати

4.3.1. Разрешено използване на сертификати

Щом сертификатът бъде издаден, собственикът на сертификата[9] го използва само в контекста на TACHOnet. В този контекст сертификатът може да се използва за:

- удостоверяване на произхода на данните;
- криптиране на данни;
- осигуряване на откриването на нарушавания в целостта на данните.

4.3.2. Забранено използване на сертификати

Всяка употреба, която не е изрично разрешена като част от разрешеното използване на сертификата, е забранена.

4.4. Допълнителни задължения на собственика на сертификата

Подробните правила и условия на SBCA се определени от T-Systems в политиката за сертификатите (ПС) / декларацията за практиките по сертифициране (ДПС) на услугата SBCA[10]. Настоящият документ включва спецификации и насоки за сигурност по отношение на техническите и организационните аспекти и описва дейностите на оператора на доверителния център в ролите на сертифициращ орган (СО) и на регистриращ орган (РО), както и на делегираната трета страна от регистриращия орган (РО).

Заявления за издаване на сертификат могат да подават само субекти, на които е разрешено да участват в мрежата TACHOnet .

---

9 Идентифициран от стойността на атрибута „O =“ в Subject Distinguished Name на издадения сертификат

10 Най-новата версия на ПС/ДПС на SBCA на T-Systems е налична на https://www.telesec.de/en/sbca-en/support/download-area/.

Що се отнася до приемането на сертификати, се прилага точка 4.4.1 от политиката за сертификатите и декларацията за практиките по сертифициране („ПС/ДПС“) на SBCA, освен това условията за употреба и разпоредбите, описани в настоящия документ, се считат за приети от организацията, на която е издаден сертификатът („O=“), когато се използва за пръв път.

По отношение на публикуването на сертификата се прилага точка 2.2 от ПС/ДПС на SBCA.

Всички собственици на сертификати трябва да отговарят на следните изисквания:

(1) защитават своя частен ключ срещу неразрешено използване;

(2) въздържат се от прехвърляне или разкриване на своите частни ключове на трети страни;

(3) се въздържат от продължаващо използване на частния ключ след изтичане на срока на валидност или оттегляне на сертификата, с изключение на разглеждането на криптирани данни (напр. декриптиране на електронни писма).

(4) собственикът на сертификата отговаря за копирането или изпращането на ключа на крайния субект или субекти.

(5) собственикът на сертификата трябва да задължи крайния субект/всички крайни субекти да спазват настоящите правила и условия, включително ПС/ДПС на SBCA, когато боравят с частния ключ.

(6) Собственикът на сертификата трябва да предостави идентификационните данни на тези упълномощени представители, които имат право да поискат отменяне на сертификати, издадени на организацията, заедно с подробности за събитията, водещи до отменяне, както и паролата за отменяне.

(7) при сертификатите, свързани с групи лица и функции и/или юридически лица, след като дадено лице напусне групата крайни субекти (напр. прекратяване на трудовото правоотношение), собственикът на сертификата трябва да предотврати злоупотребата с частния ключ, като отмени сертификата.

(8) Собственикът на сертификата отговаря и иска отменяне на сертификата при обстоятелствата, посочени в точка 4.9.1 от ПС/ДПС на SBCA.

Що се отнася до подновяването или създаването на нов ключ за сертификат, се прилага точка 4.6 или 4.7 от ПС/ДПС на SBCA.

Що се отнася до изменението на сертификат, се прилага точка 4.8 от ПС/ДПС на SBCA.

Що се отнася до отменянето на сертификат, се прилага точка 4.9 от ПС/ДПС на SBCA.

5. Идентификационен формуляр за лицата за контакт и доверените куриери (образец)

Аз, *[име и адрес на представителя на организацията]***, потвърждавам, че следната информация е предназначена да се използва в контекста на заявлението, генерирането и извличането на цифрови сертификати за публичен ключ за точките за достъп до TACHOnet, като целта им е подпомагане на поверителността, целостта и невъзможността за промяна на съобщенията по TACHOnet:**

Данни на лицата за контакт**:**

– **Лице за контакт № 1**	– **Лице за контакт № 2**
– Фамилия:	– Фамилия:
– Име и презиме:	– Име и презиме:
– GSM:	– GSM:
– Телефон:	– Телефон:
– Имейл:	– Имейл:
– Образец на оригиналния подпис: –	– Образец на оригиналния подпис: – – –

Данни на доверените куриери**:**

– **Доверен куриер № 1**	– **Доверен куриер № 2**
– Фамилия:	– Фамилия:
– Име и презиме:	– Име и презиме:
– GSM:	– GSM:
– Имейл:	– Имейл:
– Държава на издаване на паспорта	– Държава на издаване на паспорта
– Номер на паспорта:	– Номер на паспорта:
– Крайна дата на валидност на паспорта:	– Крайна дата на валидност на паспорта:

Място, дата, фирмен печат или печат на организацията:

Подпис на упълномощения представител:

6. Документи

6.1. Индивидуално пълномощно (образец)

Образец на индивидуалното пълномощно, което трябва да бъде подписано и представено от доверителния куриер при регистрацията лице в лице в офисите на регистриращия орган, може да бъде намерен на следния адрес:

Please print the text of this document on your letterhead, add your company stamp and have it signed by the administrative contact or admin-c of the domain.
The power of attorney must be signed by an authorized representative of the organization (principal).

The Shared-Business-CA customer will then submit this document together with the order document to the T-Systems International GmbH Trust Center.

Individual power of attorney / Power of attorney granted to one person

I, ***[name and address of the end-user]***, empower as an authorized person of this organization *

[name of the company receiving the certificate]

(e. g. sample company, sample authority, to be registered in the O-field of the certificate *)

following company and/or person:

Company: **European Commission**
Address: **DG DIGIT, 28 rue Belliard, 1000 Brussels**
Represented by Mr/Mrs/Ms: **Adrien FERIAL**

On my behalf, by complying with all and any regulations and formalities (particularly Certificate Policy (CP) / Certification Practice Statement (CPS)), for authorisation to manage (i.e. issue, revoke, renew) X.509v3-certificates, including the complete key-material, issued by the certification authority „TeleSec Shared-Business-CA", in respect of the domain as above mentioned.

This power of attorney relates to issuing and management of the following certificate types (the applicable type has to be marked):

☒ user [1]: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server [2]: e.g. identity of web server, TLS/SSL client server authentication
Please enter additionally the country, organization, locality, state or province name of the server:
_____

☐ eMail-Gateway [3]: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

☒ The power of attorney is valid until further notice, but up to a **maximum of 27 months** [2] or **maximum of 36 months** [1,3] from date of issuance.

☐ The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month** [2] months or **maximum of 36 months** [1,3] from date of issuance.

Please note that a time limit on the power of attorney can cause that a request for certificate order, renewal or revocation may not be possible because the validity period of the authorization has been exceeded!

Place, date, company stamp or seal of the organisation (principal)

Signature of the authorized representative

6.2. Заявление за издаване на сертификат на хартиен носител (образец)

Образец на хартиен носител на заявлението за издаване на сертификат, което трябва да бъде подписано и представено от доверения куриер при регистрацията лице в лице в офисите на регистриращия орган, може да бъде намерен на следния адрес:

7. Речник на термините

Основните термини, използвани в настоящото поддопълнение, са определени в раздела, посветен на определенията за МСЕ на единния цифров уебпортал на МСЕ:

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions

Основните съкращения, използвани в настоящото поддопълнение, са определени в речника на термините за МСЕ, намиращ се на единния цифров уебпортал на МСЕ:

https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?spaceKey=CEFDIGITAL&title=CEF+Glossary