2025/1943

30.9.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1943 НА КОМИСИЯТА

от 29 септември 2025 година

за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на референтни стандарти за квалифицирани удостоверения за електронни подписи и квалифицирани удостоверения за електронни печати

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 28, параграф 6, и член 38, параграф 6 от него,

като има предвид, че:

(1) Квалифицираните удостоверения за електронни подписи и квалифицираните удостоверения за електронни печати играят решаваща роля в цифровата стопанска среда, като насърчават прехода от традиционни процеси на хартиен носител към електронни еквиваленти. Като установяват връзка между определени данни за валидиране на електронен подпис или данни за валидиране на електронен печат с дадено физическо или юридическо лице и потвърждавайки името на това лице квалифицираните удостоверения внасят повишават сигурността по отношение на самоличността на титуляря и на създателя на печата.

(2) Презумпцията за съответствие, предвидена в член 28, параграф 6 и член 38, параграф 6 от Регламент (ЕС) № 910/2014, следва да се прилага само когато квалифицираните удостоверителни услуги за издаване на квалифицирани удостоверения за електронни подписи и квалифицираните удостоверителни услуги за издаване на квалифицирани удостоверения за електронни печати отговарят на стандартите, определени в настоящия регламент. Тези стандарти следва да отразяват установените практики и да бъдат широко признати в съответните сектори. Те следва да бъдат адаптирани така, че да включват допълнителни проверки, гарантиращи сигурността и надеждността на квалифицираните удостоверителни услуги и на съдържанието на квалифицираните удостоверения.

(3) Ако доставчик на удостоверителни услуги спазва изискванията, посочени в приложението към настоящия регламент, надзорните органи следва да приемат, че са спазени съответните изисквания на Регламент (ЕС) № 910/2014, и надлежно да се съобразят с тази презумпция за предоставяне или потвърждаване на квалифицирания статут на удостоверителната услуга. Същевременно, доставчикът на квалифицирани удостоверителни услуги може да използва и други практики, за да докаже съответствие с изискванията на Регламент (ЕС) № 910/2014.

(4) Комисията редовно оценява нови технологии, практики, стандарти или технически спецификации. В съответствие със съображение 75 от Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([2]) Комисията следва да преразглежда и при необходимост да актуализира настоящия регламент, за да бъде той в съответствие с глобалното развитие, новите технологии, стандарти или технически спецификации и да следва най-добрите практики на вътрешния пазар.

(5) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([3]) и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([4]) се прилагат по отношение на дейностите по обработване на лични данни съгласно настоящия регламент.

([1]) ОВ L 257, 28.8.2014 г., стр. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност (ОВ L, 2024/1183, 30.4.2024 г., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([5]) и прие своето становище на 6 юни 2025 г.

(7) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 48 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Референтни стандарти и спецификации за квалифицирани удостоверения за електронни подписи и електронни печати

1. Референтните стандарти и спецификации, посочени в член 28, параграф 6 т Регламент (ЕС) № 910/2014, са определени в приложение I към настоящия регламент.

2. Референтните стандарти и спецификации, посочени в член 38, параграф 6 от Регламент (ЕС) № 910/2014, са определени в приложение II към настоящия регламент.

Член 2

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 29 септември 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

([5]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ПРИЛОЖЕНИЕ I

Списък на референтните стандарти и спецификации за квалифицираните удостоверения за електронни подписи

Стандартите ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2“), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1“), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2“) и ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5“) се прилагат със следните адаптации:

1. За ETSI EN 319 411-2

1) 2.1 Нормативни препратки

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); общи изисквания на политиката за доставчиците на удостоверителни услуги“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Изисквания на политиката и изисквания за сигурност за доставчиците на удостоверителни услуги, издаващи удостоверения; Част 1: Общи изисквания“, със следните адаптации:

Точка 2.1 Нормативните препратки към ETSI EN 319 411-1 V1.5.1 се изменят, както следва:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); общи изисквания на политиката за доставчиците на удостоверителни услуги“.

— [10] ETSI EN 319 412-2 V2.4.1 „Електронни подписи и инфраструктура (ESI); Профили на удостоверенията; Част 2: Профил на удостоверенията, издадени на физически лица“.

— [14] ETSI EN 319 412-1 V1.6.1 „Електронни подписи и инфраструктура (ESI); Профили на удостоверенията; Част 1: Преглед и общи структури на данните“.

— [3] ETSI EN 319 412-5 V2.5.1 „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 5: Декларации от типа QCStatements“.

— [5] ETSI EN 319 412-1 V1.6.1 „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 1: Преглед и общи структури на данните“.

— [6] CEN/TS 419261:2015 „Изисквания за сигурност на надеждни системи за управление на удостоверения и времеви печати“.

— [7] Европейска група за сертифициране на киберсигурността, подгрупа по криптография: „Договорени криптографски механизми“, публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA) ([1]).

— [8] Регламент за изпълнение (ЕС) 2024/482 на Комисията ([2]) за определяне на правила за прилагането на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета по отношение на приемането на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК).

— [9] Регламент за изпълнение (ЕС) 2024/3144 на Комисията ([3]) за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

— [10] ISO/IEC 15408:2022 (части 1—5): „Информационна сигурност, киберсигурност и защита на неприкосновеността на личния живот — критерии за оценка на сигурността на информационните технологии“.

— [11] FIPS PUB 140-3 (2019) „Изисквания за сигурност за криптографски модули“.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) ОВ L, 2024/3144, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 5.2 Изисквания към декларацията за практиките в областта на удостоверенията

— OVR-5.2-02 CP, определена в документацията на TSP, посочват изискванията за профилите на удостоверенията, които трябва да се използват.

3) 5.3 Наименование и идентификатор на CP

— OVR-5.3-01 При промени в CP, съгласно описаното в точка 4.2.2, които засягат приложимостта, идентификаторът на политиката се променя.

4) 6.1 Публикуване и отговорности по отношение на хранилището

— OVR-6.1-02 Информацията, посочена в DIS-6.1-04 от ETSI EN 319 411-1 [2], е публично и международно достъпна.

5) 6.2.2 Първоначално валидиране на идентичността

— REG-6.2.2-01A Събирането на атрибути и доказателства за самоличността на субекта, както и тяхното валидиране, се определят в съответствие с актовете за изпълнение, приети съгласно член 24, параграф 1в от Регламент (ЕС) № 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] и [QCP-n-qscd] Самоличността на физическото лице и, ако е приложимо, специфичните му атрибути се проверяват в съответствие с актовете за изпълнение, приети съгласно член 24, параграф 1в от Регламент (ЕС) № 910/2014 [i.1].

— БЕЛЕЖКА 1 празно

6) 6.3.3 Издаване на удостоверение

— GEN-6.3.3-01 Прилагат се изискванията GEN-6.3.3-01 до GEN-6.3.3-10, определени в ETSI EN 319 411-1 [2], точка 6.3.3.

— GEN-6.3.3-02 [CONDITIONAL] Ако се издава удостоверение на физическо лице, идентифицирано във връзка с юридическото лице, тогава атрибутите на субекта, идентифициращи организацията в удостоверението, ще представляват юридическото лице или подразделението на това юридическо лице, а идентификаторът на субекта в удостоверението ще бъде физическото лице.

— GEN-6.3.3-03 Идентификаторът на CP ще бъде [CHOICE]:

а) [QCP-n]

— както е посочено в точка 5.3, буква а), и/или

— OID, присъден от TSP, друга съответна заинтересована страна или допълнителна стандартизация за CP, с която се повишават съответните приложими изисквания на политиката, определени в настоящия документ.

б) [QCP-n-qscd]

— както е посочено в точка 5.3, буква в), и/или

— OID, присъден от TSP, друга съответна заинтересована страна или допълнителна стандартизация за CP, с която се повишават съответните приложими изисквания на политиката, определени в настоящия документ.

7) 6.3.5 Ползване на двойки ключове и удостоверения

— SDP-6.3.5-02A [CONDITIONAL] Ако TSP управлява QSCD за субекта, той е доставчик на квалифицирани удостоверителни услуги, който предоставя квалифицирана удостоверителна услуга за управлението на квалифицирано устройство за създаване на електронен подпис от разстояние в съответствие с Регламент (ЕС) № 910/2014 [i.1].

— SDP-6.3.5-11A Задълженията на абоната (вж. точка 6.3.4) включват, ако абонатът или субектът генерира ключовете на субекта:

а) задължение за генериране на ключовете на субекта посредством алгоритъм, отговарящ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за използването на удостоверения ключ, както е посочено в CP;

б) задължение за използване на дължината на ключа и алгоритъма, отговарящ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за използването на удостоверения ключ, както е посочено в CP, по време на срока на валидност на сертификата.

8) 6.3.10 Услуги, отнасящи се до статуса на удостоверението

— CSS-6.3.10-08 [CONDITIONAL] Ако са предоставени CRL, TSP запазва целостта и наличността на последната CRL поне за периода, посочен в CPS, както се изисква в CSS-6.3.10-12.

9) 6.4.4 Проверки на персонала

— OVR-6.4.4-02 Персоналът на TSP с доверителни функции и, ако е приложимо, неговите подизпълнители с доверителни функции, трябва да са способни да изпълнят изискването за „експертни знания, опит и квалификации“ вследствие официално обучение и квалификация, или практически опит, или комбинация от двете.

— OVR-6.4.4-03 Спазването на OVR-6.4.4-02 включва редовни (най-малко на всеки 12 месеца) актуализации във връзка с новите заплахи и настоящите практики в областта на сигурността.

— OVR-6.4.4-04 В допълнение към доверителните функции, определени в ETSI EN 319 401 [1] (точка 7.2-15), трябва да се поддържат доверителните функции на служителите по регистрацията и отмяната с отговорности, определени в TS 419261 [6]. В случаите, когато QTSP се управлява пряко или функционира от името на държава членка или орган от публичния сектор, тези допълнителни доверителни функции могат да бъдат изпълнявани от един или повече официални представители, действащи за и от името на служителите по регистрацията и отмяната, които са длъжностни лица в местните или регионалните администрации.

10) 6.4.9 Прекратяване на дейността на CA или RA

— OVR-6.4.9-02 Планът на TSP за осигуряване на непрекъснатост на обслужването е съобразен с изискванията, определени в актовете за изпълнение, приети съгласно член 24, параграф 5 от Регламент (ЕС) № 910/2014 [i.1].

11) 6.5.1 Генериране и инсталиране на двойки ключове

— OVR-6.5.1-01A Генерирането на двойки ключове на CA се извършва с помощта на алгоритъм, отговарящ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за целите на подписването от CA.

— OVR-6.5.1-01B Избраната дължина на ключа и алгоритъмът за ключ за подпис на CA трябва да отговарят на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за целите на подписването от CA.

— OVR-6.5.1-01C [CONDITIONAL] Ако CA генерира ключовете на субекта, генерираните от CA ключове трябва да отговарят на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за целите, посочени в CP, по време на срока на валидност на сертификата.

12) 6.5.2 Защита на частния ключ и контрол върху разработването на криптографски модули

— GEN-6.5.2-01 Прилагат се всички изисквания, определени в ETSI EN 319 411-1 [2], точка 6.5.2, с изключение на изискванията OVR-6.5.2-01, OVR-6.5.2-03 и OVR-6.5.2-04.

— GEN-6.5.2-02 Генерирането на двойки ключове на TSP, включително ключовете, използвани от службите за отмяна и регистрация, се извършва в защитено криптографско устройство, което е надеждна система, сертифицирана в съответствие със:

— Общи критерии за оценяване на сигурността на информационните технологии, както са определени в ISO/IEC 15408 [10] или в Общи критерии за оценяване на сигурността на информационните технологии, версия CC:2002, части 1—5, публикувани от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността, и сертифицирана като EAL 4 или по-високо; или

— Европейската схема за сертифициране на киберсигурността, основана на общи критерии (ECCK) [8] [9], и сертифицирана като EAL 4 или по-високо; или

— до 31.12.2030 г., FIPS PUB 140-3 [11] ниво 3.

Това сертифициране е спрямо целево ниво за сигурност или защитен профил, или документация за проект и сигурност на модула, която отговаря на изискванията на настоящия документ, въз основа на анализ на риска и като се вземат предвид физическите и други нетехнически мерки за сигурност.

Ако защитеното криптографско устройство е сертифицирано по ECCK [8] [9], то се конфигурира и използва в съответствие с тази сертификация.

— GEN-6.5.2-03 Частният ключ за подпис на CA се съхранява и използва в рамките на защитено криптографско устройство, отговарящо на изискванията на GEN-6.5.2-01 и GEN-6.5.2-02.

13) 6.5.7 Контрол на сигурността на мрежата

— OVR-6.5.7-02 Проверката на уязвимостта, изисквана по REQ-7.8-13 на ETSI EN 319 401 [1], се извършва поне веднъж на тримесечие.

— OVR-6.5.7-03 Проверката на изпитване за пробив, изисквана по REQ-7.8-17X на ETSI EN 319 401 [1], се извършва поне веднъж годишно.

— OVR-6.5.7-04 Защитните стени трябва да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на доставчика на удостоверителни услуги.

14) 6.6.1 Профил на удостоверенията

— GEN-6.6.1-05 Сертификатът включва един от идентификаторите на политиката, посочени в GEN-6.3.3-03 [CHOICE]. Сертификатът може да включва други OID, присъдени от TSP.

2. За ETSI EN 319 412-2

1) 2.1 Нормативни препратки

— [2] ETSI EN 319 412-5 V2.5.1 „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 5: Декларации от типа QCStatements“.

— [9] Европейска група за сертифициране на киберсигурността, подгрупа по криптография „Договорени криптографски механизми“, публикувани от ENISA.

2) 4.2.2 Подписване

— GEN-4.2.2-2 Алгоритъмът за електронни подписи се избира в съответствие със съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [9].

— БЕЛЕЖКА празно.

3) 4.2.3.1 Юридически лица издатели

— GEN-4.2.3.1-3 Ако е известно, че съществува подходящ регистрационен номер, идентичността на издателя трябва да съдържа атрибут organizationIdentifier със стойност въпросния регистрационен номер, както е посочен в съответния официален документ, установяващ този регистрационен номер.

4) 4.2.5 Информация за публичния ключ на субекта

— GEN-4.2.5-2 Публичният ключ на субекта се избира в съответствие със съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [9].

— БЕЛЕЖКА празно.

5) 4.2.6 Сериен номер

— GEN-4.2.6-01 Серийният номер на удостоверението (според посоченото в IETF RFC 5280 [1], точка 4.1.2.2) трябва да бъде уникален за всяко удостоверение, издадено от TSP.

ПРИЛОЖЕНИЕ II

Списък на референтните стандарти и спецификации за квалифицираните удостоверения за електронни печати

Стандартите ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2“), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1“), ETSI EN 319 412-3 V1.3.1 („ETSI EN 319 412-3“), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2“) и ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5“) се прилагат със следните адаптации:

1. За ETSI EN 319 411-2

1) 2.1 Нормативни препратки

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); общи изисквания на политиката за доставчиците на удостоверителни услуги“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Изисквания на политиката и изисквания за сигурност за доставчиците на удостоверителни услуги, издаващи удостоверения; Част 1: Общи изисквания“, със следните адаптации:

Точка 2.1 Нормативните препратки към ETSI EN 319 411-1 V1.5.1 се изменят, както следва:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); общи изисквания на политиката за доставчиците на удостоверителни услуги“.

— [10] ETSI EN 319 412-2 V2.4.1 „Електронни подписи и инфраструктура (ESI); Профили на удостоверенията; Част 2: Профил на удостоверенията, издадени на физически лица“.

— [14] ETSI EN 319 412-1 V1.6.1 „Електронни подписи и инфраструктура (ESI); Профили на удостоверенията; Част 1: Преглед и общи структури на данните“.

— [3] ETSI EN 319 412-5 V2.5.1 „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 5: Декларации от типа QCStatements“.

— [5] ETSI EN 319 412-1 V1.6.1 „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 1: Преглед и общи структури на данните“.

— [6] CEN/TS 419261:2015 „Изисквания за сигурност на надеждни системи за управление на удостоверения и времеви печати“ (изготвени от CEN).

— [7] Европейска група за сертифициране на киберсигурността, подгрупа по криптография: „Договорени криптографски механизми“, публикувани от ENISA.

— [8] Регламент за изпълнение (ЕС) 2024/482 за определяне на правила за прилагането на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета по отношение на приемането на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК).

— [9] Регламент за изпълнение (ЕС) 2024/3144 за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

— [10] ISO/IEC 15408:2022 (части 1—5) „Информационна сигурност, киберсигурност и защита на неприкосновеността на личния живот — критерии за оценка на сигурността на информационните технологии“

— [11] FIPS PUB 140-3 (2019) „Изисквания за сигурност за криптографски модули“.

2) 5.2 Изисквания към декларацията за практиките в областта на удостоверенията

— OVR-5.2-02 CP, определена в документацията на TSP, посочват изискванията за профилите на удостоверенията, които трябва да се използват.

3) 5.3 Наименование и идентификатор на CP

— OVR-5.3-01 При промени в CP, съгласно описаното в точка 4.2.2, които засягат приложимостта, идентификаторът на политиката се променя.

4) 6.1 Публикуване и отговорности по отношение на хранилището

— OVR-6.1-02 Информацията, посочена в DIS-6.1-04 от ETSI EN 319 411-1 [2], е публично и международно достъпна.

5) 6.2.2 Първоначално валидиране на идентичността

— REG-6.2.2-01A Събирането на атрибути и доказателства за самоличността на субекта, както и тяхното валидиране, се определят в съответствие с актовете за изпълнение, приети съгласно член 24, параграф 1в от Регламент (ЕС) № 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] и [QCP-l-qscd] Самоличността на юридическото лице и, ако е приложимо, специфичните му атрибути се проверяват в съответствие с актовете за изпълнение, приети съгласно член 24, параграф 1в от Регламент (ЕС) № 910/2014 [i.1].

— БЕЛЕЖКА 3 вж. бележка 2.

6) 6.3.3 Издаване на удостоверение

— GEN-6.3.3-01 Прилагат се изискванията GEN-6.3.3-01 до GEN-6.3.3-10, определени в ETSI EN 319 411-1 [2], точка 6.3.3.

— GEN-6.3.3-02 Идентификаторът на CP ще бъде [CHOICE]:

а) [QCP-l]

— както е посочено в точка 5.3, буква б), и/или

— OID, присъден от TSP, друга съответна заинтересована страна или допълнителна стандартизация за CP, с която се повишават съответните приложими изисквания на политиката, определени в настоящия документ.

б) [QCP-l-qscd]

— както е посочено в точка 5.3, буква г), и/или

— OID, присъден от TSP, друга съответна заинтересована страна или допълнителна стандартизация за CP, с която се повишават приложимите изисквания на политиката, определени в настоящия документ.

7) 6.3.5 Ползване на двойки ключове и удостоверения

— SDP-6.3.5-02A [CONDITIONAL] Ако TSP управлява QSCD за субекта, той е доставчик на квалифицирани удостоверителни услуги, който предоставя квалифицирана удостоверителна услуга за управлението на квалифицирано устройство за създаване на електронен печат от разстояние в съответствие с Регламент (ЕС) № 910/2014 [i.1].

— SDP-6.3.5-11A Задълженията на абоната (вж. точка 6.3.4) включват, ако абонатът или субектът генерира ключовете на субекта:

а) задължение за генериране на ключовете на субекта посредством алгоритъм, отговарящ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA[7], за използването на удостоверения ключ, както е посочено в CP; и също така

б) задължение за използване на дължината на ключа и алгоритъма, отговарящ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA[7], за използването на удостоверения ключ, както е посочено в CP, по време на срока на валидност на сертификата.

8) 6.3.10 Услуги, отнасящи се до статуса на удостоверението

— CSS-6.3.10-08 [CONDITIONAL] Ако са предоставени CRL, TSP запазва целостта и наличността на последната CRL поне за периода, посочен в CPS, както се изисква в CSS-6.3.10-12.

9) 6.4.4 Проверки на персонала

— OVR-6.4.4-02 Персоналът на TSP с доверителни функции и, ако е приложимо, неговите подизпълнители с доверителни функции, трябва да са способни да изпълнят изискването за „експертни знания, опит и квалификации“ вследствие официално обучение и квалификация, или практически опит, или комбинация от двете.

— OVR-6.4.4-03 Спазването на OVR-6.4.4-02 включва редовни (най-малко на всеки 12 месеца) актуализации във връзка с новите заплахи и настоящите практики в областта на сигурността.

— OVR-6.4.4-04 В допълнение към доверителните функции, определени в ETSI EN 319 401 [1] (точка 7.2-15), трябва да се поддържат доверителните функции на служителите по регистрацията и отмяната с отговорности, определени в TS 419261 [6]. В случаите, когато QTSP се управлява пряко или функционира от името на държава членка или орган от публичния сектор, тези допълнителни доверителни функции могат да бъдат изпълнявани от един или повече официални представители, действащи за и от името на служителите по регистрацията и отмяната, които са длъжностни лица в местните или регионалните администрации.

10) 6.4.9 Прекратяване на дейността на CA или RA

— OVR-6.4.9-02 Планът за осигуряване на непрекъснатост на обслужването е съобразен с изискванията, определени в актовете за изпълнение, приети съгласно член 24, параграф 5 от Регламент (ЕС) № 910/2014 [i.1]].

11) 6.5.1 Генериране и инсталиране на двойки ключове

— OVR-6.5.1-01A Генерирането на двойки ключове на CA се извършва с помощта на алгоритъм, отговарящ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за целите на подписването от CA.

— OVR-6.5.1-01B Избраната дължина на ключа и алгоритъмът за ключ за подпис на CA трябва да отговарят на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за целите на подписването от CA.

— OVR-6.5.1-01C [CONDITIONAL] Ако CA генерира ключовете на субекта, генерираните от CA ключове трябва да отговарят на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [7] и публикувани от ENISA, за целите, посочени в CP, по време на срока на валидност на сертификата.

12) 6.5.2 Защита на частния ключ и контрол върху разработването на криптографски модули

— GEN-6.5.2-01 Прилагат се всички изисквания, определени в ETSI EN 319 411-1 [2], точка 6.5.2, с изключение на изискванията OVR-6.5.2-01, OVR-6.5.2-03 и OVR-6.5.2-04.

— GEN-6.5.2-02 Генерирането на двойки ключове на TSP, включително ключовете, използвани от службите за отмяна и регистрация, се извършва в защитено криптографско устройство, което е надеждна система, сертифицирана в съответствие със:

  — Общи критерии за оценяване на сигурността на информационните технологии, както са определени в ISO/IEC 15408 [10] или в Общи критерии за оценяване на сигурността на информационните технологии, версия CC:2002, части 1—5, публикувани от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността, и сертифицирана като EAL 4 или по-високо; или

  — Европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) [8] [9], и сертифицирана като EAL 4 или по-високо; или

  — до 31.12.2030 г., FIPS PUB 140-3 [11] ниво 3.

Това сертифициране е спрямо целево ниво за сигурност или защитен профил, или документация за проект и сигурност на модула, която отговаря на изискванията на настоящия документ, въз основа на анализ на риска и като се вземат предвид физическите и други нетехнически мерки за сигурност.

Ако защитеното криптографско устройство е сертифицирано по ЕССК [8] [9], то се конфигурира и използва в съответствие с тази сертификация.

— GEN-6.5.2-03 Частният ключ за подпис на CA се съхранява и използва в рамките на защитено криптографско устройство, отговарящо на изискванията на GEN-6.5.2-01 и GEN-6.5.2-02.

13) 6.5.7 Контрол на сигурността на мрежата

— OVR-6.5.7-02 Проверката на уязвимостта, изисквана по REQ-7.8-13 на ETSI EN 319 401 [1], се извършва поне веднъж на тримесечие.

— OVR-6.5.7-03 Проверката на изпитване за пробив, изисквана по REQ-7.8-17X на ETSI EN 319 401 [1], се извършва поне веднъж годишно.

— OVR-6.5.7-04 Защитните стени трябва да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на доставчика на удостоверителни услуги.

14) 6.6.1 Профил на удостоверенията

— GEN-6.6.1-05 Сертификатът включва един от идентификаторите на политиката, посочени в GEN-6.3.3-02 [CHOICE].

2. За ETSI EN 319 412-3

1) 2.1 Нормативни препратки

— [2] ETSI EN 319 412-2 V2.4.1 „Електронни подписи и инфраструктура (ESI); Профили на удостоверенията; Част 2: Профил на удостоверенията, издадени на физически лица“.

2) 4.2.1 Субект

— LEG-4.2.1-6 Атрибутът organizationIdentifier съдържа идентификация на организацията на субекта, различна от наименованието на организацията. Ако е известно, че съществува подходящ регистрационен номер, атрибутът organizationIdentifier трябва да е със стойност въпросния регистрационен номер, както е посочен в съответния официален документ, установяващ този регистрационен номер.

3. За ETSI EN 319 412-2:

1) 2.1 Нормативни препратки

— [2] ETSI EN 319 412-5 V2.5.1 „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 5: Декларации от типа QCStatements“.

— [9] Европейска група за сертифициране на киберсигурността, подгрупа по криптография: „Договорени криптографски механизми“, публикувани от ENISA.

2) 2.2 Информативни препратки

— [i.7] празно.

3) 4.2.2 Подписване

— GEN-4.2.2-2 Алгоритъмът за електронни подписи се избира в съответствие със съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [9].

— БЕЛЕЖКА празно.

4) 4.2.3.1 Юридически лица издатели

— GEN-4.2.3.1-3 Ако е известно, че съществува подходящ регистрационен номер, идентичността на издателя трябва да съдържа атрибут organizationIdentifier със стойност въпросния регистрационен номер, както е посочен в съответния официален документ, установяващ този регистрационен номер.

5) 4.2.5 Информация за публичния ключ на субекта

— GEN-4.2.5-2 Публичният ключ на субекта се избира в съответствие със съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [9].

— БЕЛЕЖКА празно.

6) 4.2.6 Сериен номер

— GEN-4.2.6-01 Серийният номер на удостоверението (според посоченото в IETF RFC 5280 [1], точка 4.1.2.2) трябва да бъде уникален за всяко удостоверение, издадено от TSP.