2025/1946

30.9.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1946 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 услуги по квалифицирано съхраняване на квалифицирани електронни подписи и квалифицирани 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 34, параграф 2, и член 40 от него,

като има предвид, че:

(1) Услугите по квалифицирано съхранение на квалифицирани електронни подписи и на квалифицирани електронни печати гарантират дългосрочната цялост, автентичността, доказателството за съществуване и достъпността на доказателствата за съхранение на тези електронни подписи и електронни печати. Това позволява да се доказва тяхната правна валидност за продължителни периоди от време и гарантира, че те могат да бъдат валидирани независимо от бъдещи технологични промени. Тези услуги се предоставят независимо или като част от друга квалифицирана удостоверителна услуга, като например квалифицирани услуги за електронно архивиране.

(2) Презумпцията за съответствие, предвидена в член 34, параграф 1а и член 40 от Регламент (ЕС) № 910/2014, следва да се прилага само когато квалифицираните услуги за съхраняване за квалифицирани електронни подписи и за квалифицирани 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 и в тях да бъдат включени допълнителни проверки, гарантиращи сигурността и надеждността на квалифицираната удостоверителна услуга, както и способността за проверка на квалифицирания статут и техническата валидност на подписите и печатите с течение на времето.

(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.

([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).

(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.

(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

Референтните стандарти и спецификации, посочени в член 34, параграф 2, и член 40 от Регламент (ЕС) № 910/2014, са определени в приложението 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

([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).

([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

Списък на референтните стандарти и спецификации, посочени в член 2

Стандартите ETSI TS 119 511 V1.1.1 (2019-06) („ETSI TS 119 511“) и ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4“) се прилагат със следните адаптации:

1. За ETSI TS 119 511

1) 2.1 Нормативни препратки:

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

— [2] ETSI TS 119 612 (V2.3.1) „Електронни подписи и инфраструктура (ESI); Доверителни списъци“.

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

— [6] Регламент за изпълнение (ЕС) 2024/482 на Комисията ([1]) 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).

— [7] Регламент за изпълнение (ЕС) 2024/3144 на Комисията ([2]) за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

— [8] Европейска група за сертифициране на киберсигурността, подгрупа по криптография: „Договорени криптографски механизми“, публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA) ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Електронни подписи и инфраструктура (ESI); Политики за подписване; Част 4: Правила за приложимост на подписа (политика за валидиране) за европейските квалифицирани електронни подписи/печати с използване на доверителни списъци“.

— [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“

2) 3.1 Термини

— защитено криптографско устройство: устройство, което съхранява частния ключ на ползвателя, защитава този ключ срещу компрометиране и изпълнява функции за подписване или декриптиране от името на потребителя.

3) 6.4 Профили на съхраняване

— OVR-6.4-08A [WTS][WOS] Очакваната валидност на доказателствата отговаря на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА 3 празно

4) 6.5 Политика за доказателствата за съхранение

— OVR-6.5-04A Използваните криптографски алгоритми отговарят на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА 1 празно

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

5) 7.2 Човешки ресурси

— OVR-7.2-02 Персоналът на PSP 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-7.2-03 Спазването на OVR-7.2-02 включва редовни актуализации (най-малко на всеки 12 месеца) във връзка с новите заплахи и настоящите практики в областта на сигурността.

6) 7.5 Криптографски контрол

— OVR-7.5-05 [CONDITIONAL] Когато PSP подписва (част от) доказателство за съхранение, частният ключ за подпис на PSP се съхранява и използва в рамките на защитено криптографско устройство, което е надеждна система, сертифицирана в съответствие със:

а) 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:2022, 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

б) ЕССК [6] [7] и сертифицирана като EAL 4 или по-високо; или

в) до 31.12.2030 г., FIPS PUB 140-3 [5] 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 [6] [7], то се конфигурира и използва в съответствие с тази сертификация.

— OVR-7.5-06 [CONDITIONAL] празно.

— OVR-7.5-07 [CONDITIONAL] Когато PSP подписва (част от) доказателство за съхранение, всички резервни копия на личните подписващи ключове на PSP трябва да бъдат защитени, за да се гарантира тяхната цялост и поверителност, посредством защитеното криптографско устройство, преди да бъдат съхранявани извън него.

— OVR-7.5-08 Частният ключ за подпис на PSP се експортира и импортира в друго защитено криптографско устройство само когато това експортиране и импортиране се осъществява по сигурен начин и в съответствие със сертифицирането на тези устройства.

7) 7.8 Мрежова сигурност

— OVR-7.8-03 Проверката на уязвимостта, изисквана по REQ-7.8-13 на ETSI EN 319 401 [1], се извършва поне веднъж на тримесечие.

— OVR-7.8-04 Проверката на изпитване за пробив, изисквана по REQ-7.8-17X на ETSI EN 319 401 [1], се извършва поне веднъж годишно.

— OVR-7.8-05 Защитните стени трябва да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на PSP.

8) 7.14 Криптографски мониторинг

— OVR-7.14-03A Оценката на криптографските алгоритми в OVR-7.14.01 и OVR-7.14.02 отговарят на съгласуваните криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

9) 7.12 Прекратяване на дейност на TSP и планове на TSP за осигуряване на непрекъснатост на обслужването

— OVR-7.12-01A 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.2].

10) 7.17 Верига на доставки

— OVR-7.17-01 Прилагат се изискванията, посочени в ETSI EN 319 401 [1], точка 7.14.

11) Приложение A (нормативно): Услуга по квалифицирано съхраняване на QES съгласно определеното в член 34 от Регламент (ЕС) № 910/2014

— OVR-A-02 [PDS][PDS+PGD]

а) услугата по съхраняване запазва цялата информация, необходима за проверка на квалифицирания статут на електронния подпис или печат, която няма да бъде публично достъпна до края на периода на съхраняване;

б) услугата по съхраняване гарантира, че във всеки един момент през периода на съхраняване информацията, която се съхранява, е такава, че когато се предоставя като входяща информация за процеса, посочен в точка 4.4 от ETSI TS 119 172-4 [9], резултатът от този процес ясно определя дали, към момента на съхраняването, цифровият подпис или печат са били технически подходящи за използване на квалифициран електронен подпис на ЕС или квалифициран електронен печат на ЕС.

— OVR-A-03 [PDS][PDS+PGD] Времевите печати, използвани в доказателството за съхранение, са квалифицирани времеви печати в съответствие с Регламент (ЕС) № 910/2014 [i.2].

2. За ETSI TS 119 172-4

1) 2.1 Нормативни препратки:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Процедури за създаване и валидиране на цифрови подписи за AdES; Част 1: Създаване и валидиране“.

— Всички препратки към „ETSI TS 119 102-1 [1]“ се разбират като препратки към „ETSI EN 319 102-1 [1]“.

— [2] ETSI TS 119 612 (V2.3.1) „Електронни подписи и инфраструктура (ESI); Доверителни списъци“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Електронни подписи и инфраструктура (ESI); Изисквания по отношение на политиката и сигурността на приложенията за създаване на подпис и валидиране на подпис“.

2) 4.2 Ограничения и процедури за валидиране, изискване REQ-4.2-03, раздел „X.509 ограничения при валидирането“, буква в):

— i) Ако сертификатът за краен субект представлява котва на доверие, не се прилагат RevocationChecking-Constraints.

— ii) Ако сертификатът за краен субект не представлява котва за доверие, за RevocationCheckingConstraints се задава „eitherCheck“, както е определено в ETSI TS 119 172-1 [3], точка A.4.2.1, таблица A.2, редове (m) 2.1.

— iii) Ако сертификатът за краен субект представлява котва за доверие, не се прилагат RevocationFreshness-Constraints, определени в ETSI TS 119 172-1 [3], точка A.4.2.1, таблица A.2, редове (m) 2.2.

— iv) Ако сертификатът за краен субект не представлява котва за доверие, RevocationFreshnessConrestrictions, определени в ETSI TS 119 172-1 [3], точка A.4.2.1, таблица A.2, редове (m) 2.2, се прилагат за сертификата за подпис с максимална стойност 0, като се гарантира, че информацията за отмяната се приема само ако е била издадена след променливата best-signature-time. Не се задава стойност за RevocationFreshnessConstraints за сертификати, различни от сертификата за подпис, включително сертификати, поддържащи времеви печати.

3) 4.3 Изисквания относно валидирането на подписите и правилата за проверка на приложимостта

— REQ-4.3-02 Приложенията за валидиране на подписа трябва да са в съответствие с ETSI TS 119 101 [13].

4) 4.4 Процес на проверка на техническата приложимост (правила)

— REQ-4.4.2-03 Ако някоя от проверките, посочени в REQ-4.4.2-01, е неуспешна, тогава:

— процесът спира;

— подписът се определя технически като неопределен, т.е. нито като квалифициран електронен подпис на ЕС, нито като квалифициран електронен печат на ЕС;

— горният резултат и резултатите от процесите на всички междинни процеси се отразяват в доклада за проверка на правилата за приложимост на подписа.