2025/1942

30.9.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1942 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 услугите по квалифицирано валидиране на квалифицирани електронни подписи и услугите по квалифицирано валидиране на 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 г. 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 33, параграф 2 и член 40 от него,

като има предвид, че:

(1) Услугите по квалифицирано валидиране за квалифицирани електронни подписи и квалифицирани електронни печати гарантират целостта, автентичността и точността на процеса и резултатите от валидирането съответно на квалифицираните електронни подписи и квалифицираните електронни печати. Тези квалифицирани удостоверителни услуги играят решаваща роля в цифровата стопанска среда, като насърчават прехода от традиционни процеси на хартиен носител към електронни еквиваленти.

(2) Презумпцията за съответствие, предвидена в член 33, параграф 2 и член 40 от Регламент (ЕС) № 910/2014, следва да се прилага само когато услугите по квалифицирано валидиране на квалифицирани електронни подписи и квалифицирани електронни печати отговарят на техническите стандарти, 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 квалифицираните удостоверителни услуги, както и способността за проверка на квалифицирания статус и техническата валидност на квалифицираните електронни подписи и квалифицираните електронни печати.

(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 статус 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 33, 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 за услугите по квалифицирано валидиране за квалифицирани електронни подписи и за услугите по квалифицирано валидиране за квалифицирани електронни печати

Прилагат се стандартите ETSI TS 119 441 V1.2.1 (2023-10) ([1]) („ETSI TS 119 441“) и ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) („ETSI TS 119 172-4“) със следните адаптации:

1. За ETSI TS 119 441

1) 2.1 Нормативни препратки

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

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

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

— [4] ISO/IEC 15408-1:2022 — Информационна сигурност, киберсигурност и защита на неприкосновеността. Критерии за оценяване на сигурността на информационните технологии.

— [5] празно.

— [6] FIPS PUB 140-3 (2019) „Изисквания за сигурността на криптографските модули“.

— [7] Регламент за изпълнение (ЕС) 2024/482 на Комисията ([3]) 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).

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) „Електронни подписи и инфраструктури (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“.

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Електронни подписи и инфраструктури (ESI); Процедури за създаване и валидиране на цифрови подписи за AdES; Част 2: Доклад за валидирането на подписа“.

— [10] Европейска група за сертифициране на киберсигурността, подгрупа по криптография: „Договорени криптографски механизми“, публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA) ([4]).

— [11] Регламент за изпълнение (ЕС) 2024/3144 на Комисията ([5]) за изменение на Регламент за изпълнение (ЕС) 2024/4822 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

— [12] ETSI EN 319 411-1 „Електронни подписи и инфраструктури (ESI); Изисквания на политиката и изисквания за сигурност за доставчиците на удостоверителни услуги, издаващи удостоверения; Част 1: Общи изисквания“

([1]) ETSI TS 119 441 — Електронни подписи и инфраструктури (ESI); Изисквания към политиката на TSP, който предоставя услуги по валидиране на подпис, V1.2.1, (2023-10).

([2]) ETSI TS 119 172-4 — Електронни подписи и инфраструктури (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, V1.1.1 (2021-05).

([3]) ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([5]) ОВ L, 2024/3144, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Информативни препратки

— [i.11] празно.

3) 3.3 Съкращения

— ЕССК — Европейска схема за сертифициране на киберсигурността, основана на общи критерии

4) 4.3.3 Процес

— БЕЛЕЖКА 10 Вж. ETSI EN 319 102-1 [3] за насоки и ETSI TS 119 172-4 [8] за допълнителни насоки за случая на квалифициран подпис на ЕС или квалифициран печат на ЕС.

5) 6.1 Декларация за практиката при услугата по валидиране на подпис

— OVR-6.1-02 Декларацията за практиката при услугата по валидиране на подпис е построена съгласно приложение A.

— OVR-6.1-03 Декларацията за практиката при услугата по валидиране на подпис изброява или посочва поддържаните политики за тази услуга (напр. чрез OID) и дава тяхно кратко описание.

6) 6.3 Политика за сигурност на информацията

— OVR-6.3-02 Политиката за сигурност трябва да документира прилаганите механизми за сигурност и неприкосновеност на личните данни с цел тяхната защита.

7) 7.2 Човешки ресурси

— OVR-7.2-02 Персоналът на SVSP 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.

8) 7.5 Криптографски контрол

— OVR-7.5-02 [CONDITIONAL] Когато се подписват доклади за валидиране, публичният сертификат за подпис на SVSP, съответстващ на частния ключ за подпис на SVSP, се издава от надежден CA в съответствие с политиката за предоставяне на удостоверения NCP+, както е посочено в ETSI EN 319 411-1 [12]. Той се издава при спазване на съответната политика за предоставяне на удостоверения, посочена в ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDITIONAL] Когато се подписват доклади за валидиране, частният ключ за подпис на SVSP 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 [4] 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 [7] [11] и сертифицирана като EAL 4 или по-високо; или

  в) до 31.12.2030 г., FIPS PUB 140-3 [6] 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 [7] [11], то се конфигурира и използва в съответствие с тази сертификация.

— OVR-7.5-04 празно.

— OVR-7.5-06 Частният ключ за подпис на SVSP 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.

9) 7.7 Сигурност на операциите

— OVR-7.7-02 За да се гарантира, че системите, на които се разработва приложението, прилагат подходящи мерки за сигурност и се адаптират към специфични среди на приложение, SVA използва среда за прилагане, в която мерките за сигурност се поддържат актуални.

— OVR-7.7-03 За SVA се прилагат следните изисквания, посочени в ETSI TS 119 101 [1], точка 5.2: GSM 1.3.

10) 7.8 Мрежова сигурност

— OVR-7.8-02 Ако е разрешен дистанционният достъп до системи за съхранение или обработка на поверителни данни, трябва да бъде приета официална политика, която се описва като част от елементите, изисквани по OVR-6.3-02.

— OVR-7.8-04 Проверката на уязвимостта, изисквана по REQ-7.8-13 на ETSI EN 319 401 [1], се извършва поне веднъж на тримесечие.

— OVR-7.8-05 Проверката на изпитване за пробив, изисквана по REQ-7.8-17X на ETSI EN 319 401 [1], се извършва поне веднъж годишно.

— OVR-7.8-06 Защитните стени трябва да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на SVSP.

11) 7.12 Прекратяване на дейност на услугата по валидиране на подпис и съответни планове за осигуряване на непрекъснатост на обслужването

— OVR-7.12-02 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].

12) 7.14 Верига на доставки

— OVR-7.14-01 Прилагат се изискванията, посочени в ETSI EN 319 401 [2], точка 7.14.

13) 8.1 Процес на валидиране на подпис

— VPR-8.1-07 SVA трябва да спазва изискванията в ETSI TS 119 101 [1], точки 7.4 SIA 1 — SIA 4.

— VPR-8.1-11 [CONDITIONAL] Когато услугата по валидиране на подпис има за цел да валидира квалифицирани електронни подписи или квалифицирани електронни печати съгласно член 32, параграф 1 (или съответно член 40) от Регламент (ЕС) № 910/2014 [i.1], процесът на валидиране трябва да е съобразен с изискванията по ETSI TS 119 172-4 [8].

14) 8.2 Протокол за валидиране на подпис

— SVP-8.2-03 Отговора за валидиране на подпис трябва да съдържа OID на политиката за услугата по валидиране на подпис.

15) 8.4 Доклад за валидирането на подпис

— SVR-8.4-02 Докладът за валидиране трябва да е в съответствие с ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDITIONAL] Когато политиката за валидиране на подпис не се изготвя изцяло от услугата по валидиране на подпис, освен валидираните ограничения в доклада трябва да се опишат и ограниченията, които са били игнорирани или отменени.

— SVR-8.4-15 В доклада за валидиране ясно се посочва произходът на всяко доказателство за съществуване (в рамките на подписа, от клиента, от сървъра).

— SVR-8.4-16 Докладът за валидиране трябва да носи подпис на доклад за валидиране, който е цифровият подпис на SVSP.

— SVR-8.4-17 [CONDITIONAL] Когато се подписват доклади за валидиране, форматът и целта на подписа трябва да съответстват на ETSI TS 119 102-2 [9].

16) 9 Рамка за определяне на политиките при услугите за валидиране, изградена върху политика за удостоверителни услуги, определена в настоящия документ:

— OVR-9-05 [CONDITIONAL] Когато се изгражда политика за услуга по валидиране на подпис по отношение на политика за удостоверителни услуги, определена в настоящия документ, трябва да се извърши оценка на риска, за да се оценят бизнес изискванията и да се определят изискванията за сигурност, които да бъдат включени в политиката за посочената общност и приложимостта.

— OVR-9-06 [CONDITIONAL] Когато се изгражда политика за услуга по валидиране на подпис по отношение на политика за удостоверителни услуги, определена в настоящия документ, политиката се одобрява и изменя в съответствие с определен процес на преразглеждане, включително отговорностите за поддържане на политиката.

— OVR-9-07 [CONDITIONAL] Когато се изгражда политика за услуга по валидиране на подпис по отношение на политика за удостоверителни услуги, определена в настоящия документ, трябва да е налице определен процес на преразглеждане, за да се гарантира, че политиката е подкрепена от декларациите за практиките.

— OVR-9-08 [CONDITIONAL] Когато изгражда политика за услуга по валидиране на подпис по отношение на политика за удостоверителни услуги, определена в настоящия документ, TSP предоставя на своята потребителска общност поддържаните от него политики.

— OVR-9-09 [CONDITIONAL] Когато изгражда политика за услуга по валидиране на подпис по отношение на политика за удостоверителни услуги, определена в настоящия документ, на абонатите се предоставят преразглежданията на политиките, които поддържа доставчикът на платежни услуги.

17) Приложение Б (нормативно) Услуга за квалифицирано валидиране за QES съгласно определеното в член 33 от Регламент (ЕС) № 910/2014:

— VPR-B-02 [CONDITIONAL] Ако SVSP е QSVSP, изпълнението трябва да съответства на ETSI TS 119 172-4 [8].

— БЕЛЕЖКА 2 празно.

— OVR-B-04 [CONDITIONAL] Ако SVSP е QSVSP, изпитванията в OVR-B-03 проверяват различни случаи на употреба, положителни и отрицателни.

— VPR-B-11 [CONDITIONAL] Ако SVSP е QSVSP, SVSP контролира изчисляването на хеша (или извършва изчислението от страната на сървъра, или контролира клиента, ако това е разрешено от страната на клиента).

— БЕЛЕЖКА 5 празно.

— БЕЛЕЖКА 6 празно.

— VPR-B-15 [CONDITIONAL] Ако SVSP е QSVSP, за да се изпълнят изискванията по VPR-B-13—VPR-B-14, докладът за валидирането трябва да съответства на ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDITIONAL] Ако SVSP е QSVSP, изпълнението трябва да съответства на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [10] за използване на подходящи криптографски техники при предоставянето на квалифицирани услуги за валидиране на QES.

18) Приложение B (информативно) Връзки на изискванията с Регламент (ЕС) № 910/2014, раздел „Осигуряване на валидиране в съответствие с член 32, параграф 1“, втора алинея:

— За да се гарантира, че са проверени всички условия, изисквани съгласно членове 32, параграф 1, и член 40 от Регламент (ЕС) № 910/2014 [i.1], е необходим правилен алгоритъм за валидиране.

Той дава същия детерминистичен резултат за подпис или печат, представени за валидиране.

Политиката за валидиране на подпис е от решаващо значение за тази цел.

ETSI TS 119 172-4 [8], въз основа на алгоритъма за валидиране, посочен в ETSI EN 319 102-1 [3], е публикуван с тази цел.

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 (2024-11) „Електронни подписи и инфраструктури (ESI); Доверителни списъци“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Електронни подписи и инфраструктури (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 на 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 на 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 на доверие, RevocationFreshnessConstraints, 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 24 часа. Не се задава стойност за RevocationFreshnessConstraints за сертификати, различни от сертификата за подпис, включително сертификати, поддържащи времеви печати.

3) 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:

а) процесът спира;

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

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