2025/1929

30.9.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1929 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 обвързването на датата и часа с данните и установяването на точността на източниците на часовото време при предоставянето на квалифицирани електронни времеви 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 42, параграф 2 от него,

като има предвид, че:

(1) Квалифицираните електронни времеви печати играят решаваща роля в цифровата стопанска среда, като насърчават прехода от традиционни процеси на хартиен носител към електронни еквиваленти. Чрез обвързването на информацията за датата и часа с електронните данни квалифицираните електронни времеви печати спомагат за гарантиране на точността на датата и часа, както и на целостта на цифровите документи, с които са обвързани датата и часът.

(2) Презумпцията за съответствие, предвидена в член 42, параграф 1а от Регламент (ЕС) № 910/2014, следва да се прилага само когато квалифицираните удостоверителни услуги за издаване на квалифицирани времеви 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 квалифицираната удостоверителна услуга и на обвързването на датата и часа с данните и на точността на източника на часовото време.

(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 изпълнение, 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

Референтните стандарти и спецификации, посочени в член 42, параграф 2 от Регламент (ЕС) № 910/2014, са определени в приложението към настоящия регламент.

Член 2

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

Списък на референтните стандарти и спецификации за услугите за квалифицирани времеви печати

Прилагат се стандартите ETSI EN 319 421 V1.3.1 ([1]) („ETSI EN 319 421“) и ETSI EN 319 422 V1.1.1 ([2]) („ETSI EN 319 422“) със следните адаптации:

1. За ETSI EN 319 421

1) 2.1 Нормативни препратки:

— [3] 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“.

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

— [5] ETSI EN 319 422 V1.1.1 (2016-03) „Електронни подписи и инфраструктури (ESI); Протокол за времевите печати и профили на токените с времеви печати“.

— [6] празно.

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

— [10] Регламент за изпълнение (ЕС) 2024/482 на Комисията ([4]) от 31 януари 2024 година 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).

— [11] Регламент за изпълнение (ЕС) 2024/3144 на Комисията от 18 декември 2024 година за изменение на Регламент за изпълнение (ЕС) 2024/482 ([5]) по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение.

2) 3.1 Термини

— срок на валидност на сертификатите: интервал от време от notBefore до notAfter включително, по време на който удостоверяващият орган (CA) гарантира, че ще поддържа информация за статуса на сертификата.

3) 3.3 Съкращения

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

4) 6.2 Декларация за практиката при удостоверителните услуги

— OVR-6.2-03 TSA включва в своята декларация за оповестяване на информация декларации относно достъпността на своята услуга за времеви печат.

5) 7.3 Сигурност на персонала

— OVR-7.3-02 Персоналът на TSA 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-7.3-03 Спазването на OVR-7.3-02 включва редовни актуализации (най-малко на всеки 12 месеца) във връзка с новите заплахи и настоящите практики в областта на сигурността.

([1]) EN 319 421 — Електронни подписи и инфраструктури (ESI). Изисквания по отношение на политиката и сигурността за доставчиците на удостоверителни услуги, издаващи времеви печати, V1.3.1.
([2]) EN 319 422 — Електронни подписи и инфраструктури (ESI). Протокол за времевите печати и профили на токените с времеви печати, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) ОВ L, 2024/3144, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Генериране на ключове за TSU

— TIS-7.6.2-03 Генерирането на ключовете на TSU се извършва 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 [3] 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 [10] [11] и сертифицирана като EAL 4 или по-високо; или

в) до 31.12.2030 г., FIPS PUB 140-3 [7] 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 [10] [11], то се конфигурира и използва в съответствие с тази сертификация.

— TIS-7.6.2-04 празно.

— БЕЛЕЖКА 3 празно.

— TIS-7.6.2-05A Алгоритъмът за генериране на ключове за TSU, получената дължина на ключа за подпис и алгоритъмът за подпис, използвани съответно за подписване на времеви печати и на удостоверения за публични ключове за TSU, трябва да са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността [9] и публикувани от ENISA.

— БЕЛЕЖКА 4 празно.

— TIS-7.6.2-06 Ключът за подпис за TSU 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) 7.6.3 Защита на частни ключове за TSU

— TIS-7.6.3-02 Частният ключ за TSU 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 [3] 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

б) Европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) [10] [11], и сертифицирана като EAL 4 или по-високо; или

в) до 31.12.2030 г., FIPS PUB 140-3 [7] 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 [10] [11], то се конфигурира и използва в съответствие с тази сертификация.

— TIS-7.6.3-03 празно.

— БЕЛЕЖКА 2 празно.

8) 7.6.7 Край на жизнения цикъл на ключа за TSU

— TIS-7.6.7-03A Датата на изтичане на срока на валидност на частните ключове за TSU трябва да е в съответствие с договорените криптографски механизми [9].

— БЕЛЕЖКА 1 празно.

9) 7.10 Мрежова сигурност

— OVR-7.10-05 Проверката на уязвимостта, изисквана по REQ-7.8-13 на ETSI EN 319 401 [1], се извършва поне веднъж на тримесечие.

— OVR-7.10-06 Проверката на изпитване за пробив, изисквана по REQ-7.8-17X на ETSI EN 319 401 [1], се извършва поне веднъж годишно.

— OVR-7.10-07 Защитните стени трябва да бъдат конфигурирани така, че да предотвратяват всякакви протоколи и достъп, които не са необходими за функционирането на TSA.

10) 7.14 Прекратяване на дейност на TSA и съответни планове за осигуряване на непрекъснатост на обслужването

— OVR-7.14-01A 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.4].

2. За ETSI EN 319 422

1) 2.1 Нормативни препратки

— [5] празно.

— [6] празно.

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

— [9] RFC 9110 HTTP семантика.

2) 4.1.3 Алгоритми за хеширане, които трябва да се използват

— Прилага се следната точка:

Алгоритмите за хеширане, използвани за хеширане на информацията, която трябва да получи времеви печат, очакваната валидност на времевите печати и избраните хеш функции спрямо времето, трябва да са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

3) 4.2.3 Алгоритми, които трябва да бъдат поддържани

— Прилага се следната точка:

Алгоритмите за подпис на токените с времеви печати са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

4) 4.2.4 Дължини на ключовете, които трябва да бъдат поддържани

— Прилага се следната точка:

Дължините на ключовете на алгоритмите за подпис за избрания алгоритъм за подпис са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA.

— БЕЛЕЖКА празно.

5) 5.1.3 Алгоритми, които трябва да бъдат поддържани

— Прилага се следната точка:

Алгоритмите за хеширане за данните на времевия печат, които трябва да бъдат поддържани, очакваната валидност на времевите печати и избраните хеш функции спрямо времето, трябва да са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

6) 5.2.3 Алгоритми, които трябва да бъдат използвани

— Прилага се следната точка:

Алгоритмите за хеширане, използвани за хеширане на информацията, която трябва да получи времеви печат, и алгоритмите за подпис на токените с времеви печати трябва да са в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

7) 6.3 Изисквания за дължината на ключа

— Прилага се следната точка:

Дължината на ключа на избрания алгоритъм за подпис на удостоверението на TSU е в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

8) 6.5 Изисквания за алгоритъма

— Прилага се следната точка:

Публичният ключ на TSU и удостоверението за подпис на TSU използват подходящи криптографски техники в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

— БЕЛЕЖКА празно.

9) 7 профила на транспортните протоколи, които трябва да бъдат поддържани

— Клиентът, който поставя времеви печат, и сървърът, който поставя времеви печат, трябва да поддържат протокола за времеви печат чрез HTTPS [9], както е определено в точка 3.4 от IETF RFC 3161 [1].

10) 8 идентификатора на обекти на криптографските алгоритми

— Прилага се следната точка:

Публичният ключ на TSU и удостоверението за подпис на TSU използват подходящи криптографски техники в съответствие с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [8].

11) 9.1 Декларация за съответствие с правилата

— Ако даден токен с времеви печат бъде обявен от TSA за квалифициран електронен времеви печат в съответствие с Регламент (ЕС) № 910/2014 [i.2], той трябва да съдържа разширение от типа QcStatements в полето за разширение на токена с времеви печат със синтаксиса, определен в IETF RFC 3739 [i.3], точка 3.2.6.

— Разширението QcStatements трябва да съдържа декларация от типа „esi4-qtstStatement-1“, както е определено в приложение Б.

— Разширението QcStatements не се отбелязва като критично.