РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2026/1735 НА КОМИСИЯТА

от 15 юли 2026 година

за изменение на Регламент за изпълнение (ЕС) 2025/1569 по отношение на приложимите стандарти и спецификации

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 45г, параграф 5, член 45д, параграф 2, член 45е, параграф 6 и член 45е, параграф 7 от него,

като има предвид, че:

(1) С цел да се осигури най-високо равнище на хармонизация между държавите членки за разработването на европейските портфейли за цифрова самоличност, техническите спецификации за портфейлите се основават на работата, извършена въз основа на Препоръка (ЕС) 2021/946 на Комисията ([2]), и по-специално рамката за техническа архитектура и технически справки. Тъй като рамката за техническа архитектура и технически справки претърпя значително развитие след приемането на Регламент за изпълнение (ЕС) 2025/1569 на Комисията ([3]), Регламент за изпълнение (ЕС) 2025/1569 следва да бъде съответно изменен, за да се приведе в съответствие с новите стандарти и спецификации.

(2) В съответствие с целите на Регламент (ЕС) № 910/2014 бяха избрани редица стандарти, за да се изпълнят изискванията, приложими към издаването, управлението и проверката на електронни удостоверения за атрибути. Тези стандарти следва да отразяват установените практики и да бъдат широко признати в съответните сектори. Когато е необходимо тези стандарти следва да бъдат адаптирани или допълнени, за да се гарантира високо равнище на сигурност и цялостност на електронните удостоверения за атрибути, като същевременно се улесни трансграничната оперативна съвместимост и ефективното функциониране на вътрешния пазар. В съответствие с тази цел с настоящия регламент се актуализират изискванията, които се прилагат към издаването и отмяната на квалифицирани електронни удостоверения за атрибути и електронни удостоверения за атрибути, издавани от орган от публичния сектор или от името на орган от публичния сектор, отговарящ за автентичен източник, и се въвеждат изисквания за подписването и подпечатването на резултатите от проверката спрямо автентични източници.

(3) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([4]) и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([5]) 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]) Препоръка (ЕС) 2021/946 на Комисията от 3 юни 2021 година относно общ инструментариум на Съюза за координиран подход към европейска рамка за цифрова самоличност (ОВ L 210, 14.6.2021 г., стр. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Регламент за изпълнение (ЕС) 2025/1569 на Комисията от 29 юли 2025 г. за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на квалифицирани електронни удостоверения за атрибути и електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от името на този орган (ОВ L, 2025/1569, 30.7.2025 г., ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) Беше проведена консултация с Европейския надзорен орган по защита на данните в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([6]), който предостави своето становище на 17 април 2026 г. ([7])

(5) 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

Изменения в Регламент за изпълнение (ЕС) 2025/1569

Регламент за изпълнение (ЕС) 2025/1569 се изменя, както следва:

1) В член 3 параграф 2 се заменя със следното:

„2. Когато доставчиците на квалифицирани електронни удостоверения за атрибути и доставчиците на електронни удостоверения за атрибути, издадени от орган от публичния сектор, отговарящ за автентичен източник, или от негово име, издават електронни удостоверения за атрибути, които са включени в схеми, регистрирани в каталога на схемите за удостоверяване на атрибути, те спазват изискванията на съответната схема за удостоверяване на атрибути. Политиките и процедурите, установени от издателите на удостоверения с цел съответствие с изискванията на схемите за удостоверяване на атрибути, са част от оценяването на съответствието, установено в Регламент (ЕС) № 910/2014.“

2) Член 4 се изменя, както следва:

а) параграф 1 се заличава;

б) параграф 3 се заменя със следното:

„3. Доставчиците на квалифицирани електронни удостоверения за атрибути и доставчиците на електронни удостоверения за атрибути, издавани от орган от публичния сектор, отговарящ за автентичен източник, или от негово име, когато тези удостоверения са издадени със срок на валидност над 24 часа, отменят тези удостоверения най-малкото при следните обстоятелства:

а) по искане на лицето, на което е издадено електронното удостоверение за атрибути или, когато е приложимо, на лицето, за което се отнася удостоверението;

б) когато на доставчика стане известно, че е налице компрометиране на сигурността или надеждността на квалифицираните електронни удостоверения за атрибути или електронните удостоверения за атрибути, издадени от орган от публичния сектор, отговарящ за автентичен източник, или от негово име;

в) в други ситуации, съгласно с изискванията на правото на Съюза или националното право.“;

в) параграф 4 се заменя със следното:

„4. Доставчиците на квалифицирани електронни удостоверения за атрибути и доставчиците на електронни удостоверения за атрибути, издавани от орган от публичния сектор, отговарящ за автентичен източник, или от негово име, трябва да въведат техники за отмяна и методи за управление, които са съобразени с неприкосновеността на личния живот и предотвратяват възможността за установяване на връзка и проследяване. Техниките за отмяна отговарят на изискванията, определени в приложение II.“

([6]) 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).

([7]) Официални коментари на ЕНОЗД по проекта за регламент за изпълнение по отношение на приложимите стандарти и спецификации за регистрацията на доверяващи се на портфейл страни |Европейски надзорен орган по защита на данните.

3) Член 9 се изменя, както следва:

а) след параграф 2 се добавя следният параграф 2а:

„2а. Механизмът за проверка отговаря на спецификациите, определени в приложение IV.“;

б) параграф 4 се заменя със следното:

„4. В резултата от проверката се посочва дали атрибутът е бил проверен или не, както и органът от публичния сектор, отговарящ за автентичния източник, или, когато е приложимо, органът от публичния сектор, определен да действа от името на автентичния източник, спрямо който атрибутът е бил проверен.

Резултатът от проверката се подписва или подпечатва от органа от публичния сектор, отговарящ за автентичен източник, или от посочения посредник, признат на национално равнище, като се използва поне усъвършенстван електронен подпис, основан на квалифицирано удостоверение за електронни подписи, или усъвършенстван електронен печат, основан на квалифицирано удостоверение за електронни печати, според случая.“

4) Приложение I се заменя с текста на приложение I към настоящия регламент.

5) Приложение II се заменя с текста в приложение II към настоящия регламент.

6) Текстът на приложение III към настоящия регламент се добавя като приложение IV.

Член 2

Влизане в сила

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

Член 1, параграф 3 се прилага от 1 януари 2027 г.

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

Съставено в Брюксел на 15 юли 2026 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

„ПРИЛОЖЕНИЕ I

Списък на референтните стандарти и спецификации, посочени в член 3

ETSI TS 119 471 V1.1.1 (2025-05) се прилага със следните адаптации:

1) 2.1 Normative references (Нормативни препратки):

[1] ETSI EN 319 401 V3.2.1 (2026-01): „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); общи изисквания на политиката за доставчиците на удостоверителни услуги“;

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

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

[4] Регламент за изпълнение (ЕС) 2024/482 на Комисията ([1]);

[5] Регламент за изпълнение (ЕС) 2024/3144 на Комисията ([2]);

[6] 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 Terms (Термини):

Добавя се следният термин:

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

3) 4. EAA trust services (Удостоверителни услуги за електронни удостоверения за атрибути (EAA)

— Точка 4.2.2.2 „Verification of attributes against authentic sources“ (Проверка на атрибутите спрямо автентични източници) не се прилага.

— REQ-EAASP-4.2.2.3-02: EAASP удостоверява автентичността пред инстанцията на EUDI Wallet, като прилага механизми за взаимно удостоверяване на автентичността, които използват валиден сертификат за достъп.

— REQ-EAASP-4.2.2.3-03: EAASP валидира блока на EUDI Wallet и проверява *дали инстанцията на EUDI Wallet е отменена*.

— Точка *4.3.2 „EUDIW Specific“ (Специфики за EUDI Wallet) не се прилага*.

4) 6.1 EAAS practice statement (Декларация за практиката при услугите за EAA):

— REQ-EAASP-6.1-02: Доставчикът на услуги за EAA (EAASP) документира механизма за отмяна в декларацията за практиката при услугите за EAA

5) 6.3 Information security policy (Политика за сигурност на информацията):

— REQ-EAASP-6.3-02: EAASP установява процедури за уведомяване на надзорния орган за всички промени в предоставянето на удостоверителната услуга за електронни удостоверения за атрибути и за намерението за прекратяване на тези дейности в съответствие със стопанските изисквания и съответните законови и подзаконови актове, включително в съответствие с изискванията на актовете за изпълнение, приети съгласно член 24, параграф 5 от Регламент (ЕС) № 910/2014. EAASP уведомява надзорния орган най-малко:

— един месец преди извършването на каквато и да е промяна;

— три месеца преди планираното прекратяване на предоставянето на удостоверителна услуга.

([1]) Регламент за изпълнение (ЕС) 2024/482 на Комисията от 31 януари 2024 г. 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) (ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Регламент за изпълнение (ЕС) 2024/3144 на Комисията от 18 декември 2024 г. за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение (ОВ L, 2024/3144, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5 Cryptographic controls (Криптографски контрол):

— REQ-EAASP-7.5.2-05: void

— REQ-EAASP-7.5.2-06: void

— REQ-EAASP-7.5.3-01A: Въвеждат се подходящи механизми за контрол на сигурността за управлението на криптографски ключове, криптографски алгоритми и криптографски устройства през целия им жизнен цикъл, като се следва, когато е целесъобразно, подход на криптогъвкавост.

— REQ-EAASP-7.5.3-01B: За целите на предоставянето на своите удостоверителни услуги EAASP избира и използва подходящи криптографски техники, съобразени с договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от ENISA [2].

— REQ-EAASP-7.5.3-02: EAASP гарантира, че защитеното криптографско устройство, което използва за цифровия подпис или печат на EAA, е устройство за създаване на квалифициран подпис или печат и че всички други цифрови подписи или печати, използвани за предоставяне на удостоверителната услуга за електронни удостоверения за атрибути, или на част от нея, са създадени чрез 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 Общи критерии за оценяване на сигурността на информационните технологии, версия 3.1 (CC3.1), до 31.8.2027 г, или във версия CC:2022, части 1—5, публикувани от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността, или както е посочено в ISO/IEC 15408 [6], и сертифицирана като EAL 4 или по-високо; или

б) Европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) [4] [5], и сертифицирана като EAL 4 или по-високо; или

в) FIPS-140-2level 3 да се използва до 31.8.2027 г. за съществуващи сертифицирани системи или FIPS PUB 140-3 [3] level 3 до 31.12.2030 г.

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 [4] [5], то се конфигурира и използва в съответствие с тази сертификация.

— REQ-EAASP-7.5.5-01: void

— REQ-EAASP-7.5.5-02: void

— REQ-EAASP-7.5.5-04: void

7) 7.9 Vulnerabilities and Incident management (Уязвимости и управление на инциденти):

— REQ-EAASP-7.9-02: При дейностите по мониторинг се взема предвид чувствителността на всяка информация, която се събира или анализира.

8) 7.12 EAASP and EAAS termination and termination plans (Прекратяване на дейността и планове за прекратяване на дейността на EAASP и EAAS):

— REQ-EAASP-7.12-04: Планът на EAASP за прекратяване е съобразен с изискванията, определени в актовете за изпълнение, приети съгласно член 24, параграф 5 от Регламент (ЕС) № 910/2014 [i.1].“

ПРИЛОЖЕНИЕ II

„*ПРИЛОЖЕНИЕ II*

Технически спецификации, посочени в членове 3 и 4

Доставчиците на квалифицирани електронни удостоверения за атрибути и доставчиците на електронни удостоверения за атрибути, издавани от орган от публичния сектор, отговарящ за автентичен източник, или от негово име, издават своите удостоверения в съответствие най-малко с един от стандартите в списъка от приложение II към Регламент за изпълнение (ЕС) 2024/2979 на Комисията ([1]) и прилагат съответните техники за отмяна, също посочени в приложение II към Регламент за изпълнение (ЕС) 2024/2979 на Комисията.“

([1]) Регламент за изпълнение (ЕС) 2024/2979 на Комисията от 28 ноември 2024 г. за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на целостта и основните функции на европейските портфейли за цифрова самоличност (ОВ L, 2024/2979, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ПРИЛОЖЕНИЕ III

„ПРИЛОЖЕНИЕ IV

Списък на стандартите и техническите спецификации, посочени в член 9

Механизмите за проверка, посочени в член 9, са съобразени с едно или и с двете от следните условия при следните адаптации:

а) техническите спецификации, посочени в точка 6.1.1 от ETSI TS 119 478 V1.1.1 (2026-01) — Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); спецификация на интерфейси във връзка с автентични източници;

— REQ-ASIP-6.1.1.2-04-01 [CONDITIONAL]: В случай, че attributeVerificationResult е http://uri.etsi.org/19478/VerificationResult/Match или http://uri.etsi.org/19478/VerificationResult/MatchWithVariation attributeVerificationResult може да съдържа елемент attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [CONDITIONAL]: В случай че върнатият attributeVerificationResult е http://uri.etsi.org/19478/VerificationResult/Match и attributeVerificationResult съдържа елемент attributeValue, елементът attributeValue трябва да съдържа стойността, посочена в заявката.

— REQ-ASIP-6.1.1.2-04-03 [CONDITIONAL]: В случай че върнатият attributeVerificationResult е http://uri.etsi.org/19478/VerificationResult/MatchWithVariation и attributeVerificationResult съдържа елемент attributeValue, елементът attributeValue трябва да съдържа стойността на атрибута, както е съхранена в автентичния източник.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDITIONAL]: В случай, че fragmentVerificationResult е http://uri.etsi.org/19478/VerificationResult/Match или http://uri.etsi.org/19478/VerificationResult/MatchWithVariation attributeVerificationResult може да съдържа елемент fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDITIONAL]: В случай че върнатият fragmentVerificationResult е http://uri.etsi.org/19478/VerificationResult/Match и attributeVerificationResult съдържа елемент fragmentValue, елементът fragmentValue трябва да съдържа стойността, посочена в заявката.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDITIONAL]: В случай че върнатият fragmentVerificationResult is http://uri.etsi.org/19478/VerificationResult/MatchWithVariation и attributeVerificationResult съдържа елемент fragmentValue, елементът fragmentValue трябва да съдържа стойността на фрагмента на атрибута, както е съхранена в автентичния източник.

б) техническите спецификации, посочени в точка 6.2.3 от ETSI TS 119 478 V1.1.1 (2026-01) — Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); спецификация на интерфейси във връзка с автентични източници.

— REQ-ASIP-6.2.3.2.1-08-04: Елементът AttributeVerificationResponse може да съдържа точно един дъщерен елемент измежду TextValue, XMLValue или AttributeProperties.“