2026/1731

22.7.2026 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2026/1731 НА КОМИСИЯТА

от 15 юли 2026 година

за изменение на регламенти за изпълнение (ЕС) 2024/2977, (ЕС) 2024/2979, (ЕС) 2024/2980 и (ЕС) 2024/2982 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 5а, параграф 23 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 регламенти за изпълнение (ЕС) 2024/2977 ([3]), (ЕС) 2024/2979 ([4]), (ЕС) 2024/2980 ([5]) и (ЕС) 2024/2982 ([6]) на Комисията, тези регламенти за изпълнение следва да се изменят, за да се приведат в съответствие с нови стандарти, спецификации и процедури.

В съответствие с целите на Регламент (ЕС) № 910/2014 бяха избрани редица стандарти, за да се изпълнят тези специфични изисквания. Тези стандарти следва да отразяват установените практики и да бъдат широко признати в съответните сектори. Например, тъй като форматът W3C VCDM се използва като референтен формат за удостоверенията, по-специално в образователния сектор, европейските портфейли за цифрова самоличност следва също да поддържат този формат, когато са налични новите профили във формат W3C VCDM. Когато е необходимо тези стандарти следва да бъдат адаптирани или допълнени, за да се гарантира сигурността и достоверността на европейските портфейли за цифрова самоличност, като същевременно се улесни трансграничната оперативна съвместимост и ефективното функциониране на вътрешния пазар.

(2) За всеки случай на употреба на портфейла, при която се изисква представяне на портретна снимка на ползвателя на портфейла, технологичните решения за портфейла трябва да поддържат функционалността за избирателно разкриване и разкриването трябва да бъде под пълния контрол на ползвателя. За да се защити възможността за вземане на решения относно разкриването, както и портретната снимка срещу неволно или неразрешено искане за разкриване, архитектурното проектиране на европейските портфейли за цифрова самоличност следва да предвижда механизми за предупреждение и регистриране на всички трансакции, свързани с използването на портретната снимка. За да се гарантира, че ползвателят на портфейла е наясно, че споделя биометрични данни, в предупрежденията следва да се

([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) 2024/2977 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 данните за идентификация на лица и електронните удостоверения за атрибути, издадени за европейските портфейли за цифрова самоличност (ОВ L, 2024/2977, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) 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).

([5]) Регламент за изпълнение (ЕС) 2024/2980 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 уведомленията до Комисията относно екосистемата на европейските портфейли за цифрова самоличност (ОВ L, 2024/2980, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Регламент за изпълнение (ЕС) 2024/2982 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 протоколите и интерфейсите, които трябва да се поддържат от европейската рамка за цифрова самоличност (ОВ L, 2024/2982, 4.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

посочва, че искането включва споделяне на биометрични данни, и изрично да се изисква от ползвателя да потвърди разкриването. Когато доверяваща се страна обработва портретна снимка с цел уникално идентифициране на физическо лице или за потвърждаване на заявената от това лице самоличност, се прилагат член 6 и 9 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([7]), както и всички други изисквания на посочения регламент, включително че обработването на портретната снимка от доверяващите се страни следва да бъде ограничено до необходимото за предвижданата употреба. Предвижданата употреба следва да се съобщава на ползвателя на портфейла, заедно с искането за разкриване, на ясен и разбираем език. За да оцени надлежно чувствителността на биометричните данни, ползвателят на портфейла следва изрично и конкретно да потвърди разкриването на портретната снимка. Липсата на отговор или предварително отбелязаните с отметка полета не следва да се смятат за потвърждение от ползвателя на портфейла. Изричното потвърждение на ползвателя на портфейла следва да бъде техническа предпазна мярка и само по себе си не предоставя правно основание за обработване. Както е посочено в член 9, параграф 4 от Регламент (ЕС) 2016/679, държавите членки могат да запазят или да въведат допълнителни условия, включително и ограничения, по отношение на обработването на генетични данни, биометрични данни или данни за здравословното състояние.

(3) За да се осигури достатъчно време на държавите членки да адаптират своите национални процедури, портретната снимка на ползвател на портфейл може да бъде част от задължителните данни за идентификация на лице при физическите лица едва от 11 август 2028 г. Когато тези изображения се получават от съществуващи документи за самоличност, като лични карти или паспорти, се прилагат съответните изисквания, определени съответно в регламенти (ЕС) 2025/1208 ([8]) или (ЕО) № 2252/2004 на Съвета ([9]).

(4) Регламент (ЕС) № 910/2014 изисква портфейлите да могат да показват марка за доверие на ЕС за портфейл за цифрова самоличност като проверимо, просто и разпознаваемо указание, че портфейлът е предоставен в съответствие с регламента. Използването на подобна марка за доверие ще спомогне за ефективното функциониране на вътрешния пазар, ще гарантира лоялна конкуренция и ще защити интересите на потребителите. За да се позволи използването на подобна марка за доверие, следва да бъдат установени нейните визуални и технически характеристики.

(5) Както е посочено в член 12б от Регламент (ЕС) № 910/2014, контролиращите достъпа предприятия трябва да осигуряват на доставчиците на европейски портфейли за цифрова самоличност и на издателите на средства за електронна идентификация, за които е извършено уведомяване, ефективна оперативна съвместимост и — за целите на оперативната съвместимост — достъп до същата операционна система, хардуерни или софтуерни характеристики. Тази ефективна оперативна съвместимост и достъп трябва да се осигуряват безплатно и независимо от това дали тези хардуерни или софтуерни характеристики са част от операционната система, дали са на разположение на контролиращото достъпа предприятие или се използват от него при предоставянето на такива услуги. Тъй като всички технологични решения за портфейл следва да поддържат общ набор от протоколи и интерфейси, за да се гарантират използваемостта, сигурността и оперативната съвместимост във всички държави членки, контролиращите достъпа предприятия следва да осигурят функционирането на характеристиките на операционната система, хардуера или софтуера, които са необходими за прилагане на протоколите и интерфейсите, посочени в приложение XII към настоящия регламент. В този контекст при потоци между устройства онлайн, както за проверка на физическа близост, така и за пренос на данни между две устройства, контролиращите достъпа предприятия следва да предпочитат локален канал за обмен, като позволява Client To Authenticator Protocol (CTAP), версия 2.3 ([10]), пред използването на услугите на CTAP Hybrid tunnel (хибриден тунел на CTAP).

(6) За да се даде достатъчно време на държавите членки, доставчиците на удостоверения за регистрация на доверяваща се на портфейл страна и доставчиците на портфейли да осигурят възможност портфейлните блокове да удостоверяват автентичността и да валидират удостоверения за регистрация на доверяваща се на портфейл страна, това изискване следва да се прилага едва от 11 август 2028 г.

(7) Регламент (ЕС) 2016/679 и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([11]) се прилагат по отношение на дейностите по обработване на лични данни съгласно настоящия регламент.

([7]) 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).

([8]) Регламент (ЕС) 2025/1208 на Съвета от 12 юни 2025 година относно повишаване на сигурността на личните карти на гражданите на Съюза и на документите за пребиваване, издавани на гражданите на Съюза и на членовете на техните семейства, които упражняват правото си на свободно движение (ОВ L, 2025/1208, 20.6.2025 г., ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Регламент (ЕО) 2252/2004 на Съвета от 13 декември 2004 г. относно стандартите за отличителните знаци за сигурност и биометричните данни в паспортите и документите за пътуване, издавани от държавите членки (ОВ L 385, 29.12.2004 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Стандарт, предложен от Fido Alliance, Client to Authenticator Protocol — CTAP (протокол за връзка между клиента и удостоверителя), 26 февруари 2026 г.

([11]) 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).

(8) С Европейския надзорен орган по защита на данните беше проведена консултация в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([12]) и той предостави своето становище на 17 април 2026 г. ([13])

(9) 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) 2024/2977

Регламент за изпълнение (ЕС) 2024/2977 се изменя както следва:

1) Добавя се следният член 3а:

„*Член 3а*

Защита на портретната снимка

1. В допълнение към изискванията за информация съгласно Регламент (ЕС) 2016/679 доставчиците на портфейли гарантират, че технологичните решения за портфейл, които предоставят, изпращат предупреждения до ползвателите на портфейла, когато доверяващите се на портфейла страни поискат разкриване на портретната снимка, като в тях се посочва, че искането предполага споделяне на биометрични данни и изисква потвърждение за избирателно разкриване на портретната снимка.

2. За прилагането на избирателно разкриване на портретната снимка на доверяваща се на портфейл страна доставчиците на портфейли гарантират, че технологичните решения за портфейл изискват от ползвателя на портфейла изрично и конкретно да потвърди предоставянето на портретната снимка.

3. Доверяващи се на портфейл страни не съхраняват портретната снимка, освен ако обработването ѝ е необходимо за целите на идентификацията и удостоверяването на автентичността в съответствие с правото на Съюза в областта на защитата на данните или когато това е предвидено в правото на Съюза или в националното право, в съответствие с правото на Съюза в областта на защитата на данните. Портретната снимка не се предава на трети държави или международни организации, освен ако това не е разрешено от правото на Съюза в областта на защитата на данните.“

2) В член 4 параграф 1 се заменя със следното:

„1. Електронните удостоверения за атрибути, издадени за портфейлни блокове, отговарят на поне един от стандартите, посочени в приложение II към Регламент за изпълнение (ЕС) 2024/2979.“

3) В член 5 параграф 4, буква б) се заменя със следното:

„б) когато удостоверението за портфейлен блок на портфейлния блок, за който са били издадени данните за идентификацията на лица, е отменено;“.

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

([12]) 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).

([13]) Официални коментари на ЕНОЗД по проекта за регламент за изпълнение по отношение на приложимите стандарти и спецификации и за поправка на Регламент за изпълнение (ЕС) 2024/2980 | Европейски надзорен орган по защита на данните.

Член 2

Изменения в Регламент за изпълнение (ЕС) 2024/2979

Регламент за изпълнение (ЕС) 2024/2979 се изменя както следва:

1) В член 3 параграф 2 се заличава.

2) В член 5, параграф 1 буква а) се заменя със следното:

„а) извършват криптографски операции по портфейла, включващи критични активи, запазени в защитено криптографско устройство на портфейла и които не се изискват за удостоверяване на автентичността на ползвателя на портфейла, само в случаите, когато тези приложения са удостоверили успешно автентичността на ползвателите на портфейла;“.

3) Добавя се следният член 5а:

„*Член 5а*

Криптографски механизми

За целите на член 4, параграф 2 доставчиците на портфейли използват само криптографските механизми, посочени в приложение Iа.“

4) Член 6 се изменя, както следва:

а) параграф 1 се заменя със следното:

„1. Доставчиците на портфейли издават удостоверения за портфейлен блок за всеки портфейлен блок. Доставчиците на портфейли подписват или подпечатват удостоверенията за портфейлен блок по такъв начин, че подписите или печатите да могат да бъдат валидирани чрез сертификат от списъка в съответствие с раздел 2, точка 1, буква з) от приложение II към Регламент за изпълнение (ЕС) 2024/2980.“;

б) параграф 2 се заменя със следното:

„2. Доставчиците на портфейли гарантират, че удостоверенията за портфейлен блок, посочени в параграф 1, отговарят на техническите спецификации, посочени в приложение Iб.“;

в) в параграф 3 буква б) се заменя със следното:

„б) предоставят механизми за сигурна идентификация и удостоверяване на автентичността на ползвателите на портфейла, които не зависят от портфейлните блокове;“.

5) В член 9 параграф 2, буква б) се заменя със следния текст:

„б) името, данните за контакт и уникалния идентификационен код на съответната доверяваща се на портфейла страна и държавата членка, в която е установена тази доверяваща се на портфейла страна;“.

6) В член 10 параграф 1 се заменя със следното:

„1. Доставчиците на портфейли гарантират, че електронните удостоверения за атрибути, издадени в съответствие с техническите спецификации, които са приложими за общите включени политики за оповестяване, посочени в приложение III, могат да бъдат обработени от портфейлните блокове, които предоставят.“

7) Член 12 се изменя, както следва:

а) параграф 2, буква в) се заменя със следното:

„в) създаване на подписи или печати в съответствие най-малко със задължителния формат за подпис или печат, посочен в приложение IV;“;

б) параграф 3 се заменя със следното:

„3. Приложенията за създаване на подписи могат или да бъдат интегрирани в инстанции на портфейла, или да бъдат външни за тях.“;

в) добавя се следният параграф:

„4. Приложенията за създаване на подписи, използвани от портфейлните блокове, поддържат най-малко програмния интерфейс на приложението, посочен в приложение IV.“

8) В член 14 параграф 1 се заличава.

9) Добавя се следният член 14а:

„*Член 14а*

Марка за доверие на ЕС за портфейл за цифрова самоличност

1. Доставчиците на портфейли гарантират, че портфейлните блокове показват марката за доверие на ЕС за портфейл за цифрова самоличност. Марката за доверие на ЕС за портфейл за цифрова самоличност е с формата, посочена в приложения VI и VII.

2. Доставчиците на портфейли гарантират, че портфейлните блокове позволяват достъпа на ползвателите до информацията, която им позволява да проверят статуса на сертифициране на технологичното решение за портфейл. За тази цел доставчиците на портфейли гарантират, че след регистрацията на технологично решение за портфейл съответните модули на портфейла включват URL адресите, предоставени от Европейската комисия за целите на подобна проверка. Доставчиците на портфейли гарантират, че техните портфейлни блокове имат достъп до данните на марката за доверие на ЕС за портфейл за цифрова самоличност, които отговарят на техническите спецификации, посочени в приложение VIII.

3. Еталонните цветове за марката за доверие на ЕС за портфейл за цифрова самоличност са Pantone 661 и 116 или синьо (100 % циан, 67 % магента, 0 % жълто, 40 % черно) и жълто (0 % циан, 20 % магента + 100 % жълто + 0 % черно), когато се използва четирицветна технология; Когато се използва цветовият модел RGB, еталонните цветове са синьо (0 червено + 51 зелено + 153 синьо) и жълто (255 червено + 204 зелено + 0 синьо).

4. Единствено когато използването на цвят не е осъществимо, марката за доверие на ЕС за портфейл за цифрова самоличност може да се използва в черно и бяло, както е посочено в приложение VII.

5. Когато марката за доверие на ЕС за портфейл за цифрова самоличност се използва на тъмен фон, тя може да се използва в негатив, като се използва същият цвят на фона. Когато марката за доверие на ЕС за портфейл за цифрова самоличност се използва цветно на цветен фон, което затруднява различаването ѝ, може да се използва отграничаващ контур около марката за доверие на ЕС за портфейл за цифрова самоличност, за да се подобри контрастът с фоновите цветове.

6. Марката за доверие на ЕС за портфейл за цифрова самоличност е с минимален размер 64 × 85 пиксела при 150 dpi.

7. Доставчиците на портфейли гарантират, че марката за доверие на ЕС за портфейл за цифрова самоличност се използва по начин, който дава възможност за ясно посочване на портфейлния блок, за който се отнася марката за доверие на ЕС за портфейл за цифрова самоличност. Марката за доверие на ЕС за портфейл за цифрова самоличност може да бъде свързана с графични или текстови елементи, ясно указващи портфейлния блок, за който тя се използва, при условие че те не променят нейната разпознаваемост като марка за доверие на ЕС за портфейл за цифрова самоличност, нито засягат връзката със списъка на сертифицираните европейски портфейли за цифрова самоличност, посочен в член 5г от Регламент (ЕС) № 910/2014.

8. Когато доставчиците на портфейли са отменили удостоверение за портфейлен блок, те гарантират, че марката за доверие на ЕС за портфейл за цифрова самоличност вече не се показва от съответния портфейлен блок.“

10) Добавят се приложения Iа и Iб, както е посочено в приложение II и приложение III към настоящия регламент.

11) Приложение II се заменя с приложение IV към настоящия регламент.

12) Приложение III се заменя с приложение V към настоящия регламент.

13) Приложение IV се изменя в съответствие с приложение VI към настоящия регламент.

14) Приложение V се заличава.

15) Текстът от приложение VII към настоящия регламент се вмъква като приложение VI.

16) Текстът от приложение VIII към настоящия регламент се вмъква като приложение VII.

17) Текстът от приложение IX към настоящия регламент се вмъква като приложение VIII.

Член 3

Изменения в Регламент за изпълнение (ЕС) 2024/2980

Регламент за изпълнение (ЕС) 2024/2980 се изменя както следва:

1) В член 5 параграф 2 се заменя със следното:

„2. Когато е приложимо, Комисията създава, поддържа и публикува списък, в който събира предоставената от държавите членки информация относно доставчиците на портфейли, доставчиците на данни за идентификация на лица, доставчиците на удостоверения за достъп на доверяваща се на портфейл страна и доставчиците на удостоверения за регистрация на доверяваща се на портфейл страна, както е посочено в приложение II, раздели 2, 3, 4 и 5.“

2) Приложение II към Регламент за изпълнение (ЕС) 2024/2980 се изменя съгласно посоченото в приложение X към настоящия регламент.

Член 4

Изменения в Регламент за изпълнение (ЕС) 2024/2982

Регламент за изпълнение (ЕС) 2024/2982 се изменя както следва:

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

„2) представянето на атрибути за данни за идентификация на лица и електронни удостоверения за атрибути на доверяващи се на портфейл страни;“.

2) Член 3 се изменя, както следва:

а) параграф 1 се заменя със следното:

„1) установяват автентичността и валидират удостоверенията за достъп на доверяваща се на портфейла страна, когато си взаимодействат с доверяващи се на портфейл страни без да делегират изпълнението на тези процеси на браузър на операционна система или друго междинно приложение;“;

б) параграф 2 се заличава;

в) параграф 3 се заменя със следното:

„3) установяват автентичността и валидират заявки, подадени с помощта на удостоверения за достъп на доверяваща се на портфейл страна;“;

г) параграф 4 се заменя със следното:

„4) удостоверяват автентичността и валидират удостоверението за регистрация на доверяваща се на портфейла страна;“;

д) параграф 5 се заменя със следното:

„5) показват на ползвателите на портфейла информацията, съдържаща се в удостоверенията за достъп на доверяващата се на портфейла страна;“;

е) параграф 8 се заличава;

ж) параграф 9 се заменя със следното:

„9) не представят каквито и да било атрибути на доверяващите се на портфейла страни, обект на заявка, докато не бъдат изпълнени следните стъпки:

а) потвърждение, че включените политики за разкриване на информация са обработени в рамките на портфейлния блок в съответствие с член 10 от Регламент за изпълнение (ЕС) 2024/2979;

б) проверка дали ползвателите на портфейла частично или изцяло са одобрили представянето.“

3) В член 4 параграф 1 се заменя със следното:

„1. Доставчиците на портфейли гарантират, че технологичните решения за портфейла поддържат посочените в приложение I протоколи и интерфейси за издаване на данни за идентификация на лица и електронни удостоверения за атрибути на портфейлни блокове.“

4) Член 5 се изменя, както следва:

а) параграфи 1 и 2 се заменят със следното:

„1. Доставчиците на портфейли гарантират, че технологичните решения за портфейл поддържат протоколи и интерфейси за представяне на атрибути на доверяващи се на портфейла страни от разстояние и, когато е подходящо, в близост, в съответствие с посочените в приложение II технически спецификации.

2. Доставчиците на портфейли гарантират, че по искане на ползвателите портфейлните блокове отговарят на успешно удостоверените и валидирани заявки от доверяващи се на портфейла страни, посочени в член 3, в съответствие с посочените в приложение II технически спецификации.“;

б) параграф 5 се заличава.

5) Член 8 се заменя със следното:

„*Член 8*

Влизане в сила

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

Член 3, параграф 4 се прилага от 11 август 2028 г.

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

6) Приложението се заличава.

7) Текстът от приложение XI към настоящия регламент се добавя като приложение I.

8) Текстът от приложение XII към настоящия регламент се добавя като приложение II.

Член 5

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 15 юли 2026 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

„ПРИЛОЖЕНИЕ

Технически спецификации за данни за идентификация на лица, посочени в член 3, параграф 3

1) Раздел 1: Набор от данни за идентификация на физическо лице

Таблица 1

Задължителни данни за идентификация на физическото лице при избирателно разкриване

Идентификатор на данни	Определение
`family_name`	Настоящо(и) фамилно(и) име(на) на ползвателя, за когото се отнасят данните за идентификация на лице.
`given_name`	Настоящо(и) собствено(и) име(на), включително бащино(и) име(на), когато това е приложимо, на ползвателя, за когото се отнасят данните за идентификация на лице.
`birth_date`	Ден, месец и година, в която е роден ползвателят, за когото се отнасят данните за идентификация на лице.
`birth_place`	Държавата, означена с alpha-2 код, както е посочено в ISO 3166-1, или районът, провинцията или областта, или общината, агломерацията, градът или селото, където е роден ползвателят, за когото се отнасят данните за идентификация на лице.
`nationality`	Един или повече alpha-2 кодове на държави, както е посочено в ISO 3166-1, представляващи националността на ползвателя, за когото се отнасят данните за идентификация на лице.
`portrait`	Освен в случай, че ползвателят изрично откаже това, когато е приложимо, лицево изображение на ползвателя, за когото се отнасят данните за идентификация на лице, в съответствие с изискванията за качество за цялостно изображение анфас, както е посочено в ISO/IEC 39794-5, или, за обратна съвместимост, ISO/IEC 19794-5, точки 8.2, 8.3 и 8.4, предоставено като кодирани данни за изображение, без заглавните части или блоковете, посочени в точка 5 от ISO/IEC 19794-5, освен за самите данни на изображението (формат JPEG) — прилага се от 11 август 2028 г.

— Държавите членки могат да осигурят на ползвателя възможност да откаже включването на портретната снимка в данните за идентификация на лица.

— Държавите членки гарантират, че избирателното разкриване се прилага за всеки идентификатор на данни, включително портретната снимка.

— Когато датата на раждане на физическото лице не е известна, държавите членки избират подходящи стойности, които отговарят на спецификациите, посочени в раздели 4.1 или 4.2 (според случая) от настоящото приложение.

— Когато гражданството на физическото лице е неизвестно, държавите членки използват стойността „QU“.

— Когато физическото лице не е гражданин на държава членка, държавите членки използват стойността „QS“.

— Когато ползвателят избере да не включва портретната снимка, държавите членки не попълват тази стойност.

Таблица 2

Незадължителни данни за идентификация на физическото лице при избирателно разкриване

Идентификатор на данни	Определение
адрес_на_пребиваване	Пълният адрес на мястото, където ползвателят, за когото се отнасят данните за идентификация на лице, пребивава в момента или може да се осъществи контакт с него (име на улица, номер на сграда, град и др.).
resident_country	Държавата, в която понастоящем пребивава ползвателят, за когото се отнасят данните за идентификация на лице, като alpha-2 код на държава, както е посочено в ISO 3166-1.
resident_state	Районът, провинцията или областта, където понастоящем пребивава ползвателят, за когото се отнасят данните за идентификация на лице.
resident_city	Общината, агломерацията, градът или селото, където понастоящем пребивава ползвателят, за когото се отнасят данните за идентификация на лице.
resident_postal_code	Пощенския код на мястото, където понастоящем пребивава ползвателят, за когото се отнасят данните за идентификация на лице.
resident_street	Името на улицата, където понастоящем пребивава ползвателят, за когото се отнасят данните за идентификация на лице, включително номера на жилището и всяка приставка или наставка.
personal_administrative_-number	Стойност, зададена за ползвателя, за когото се отнасят данните за идентификация на лица, която е уникална сред всички лични административни номера, издадени от доставчика на данни за идентификация на лица. Когато държавите членки решат да включат този атрибут, те описват в своите схеми за електронна идентификация, съгласно които се издават данните за идентификация на лица, прилаганата от тях политика по отношение на стойностите на този атрибут, включително, когато е приложимо, специфични условия за обработката на тази стойност.
family_name_birth	Фамилно(и) име(на) на ползвателя, за когото се отнасят данните за идентификация на лица, към момента на раждане.
given_name_birth	Собствено(и) име(на), включително бащино(и) име(на) на ползвателя, за когото се отнасят данните за идентификация на лица, към момента на раждане.
sex	Стойностите са някои от следните: 0 = неизвестен; 1 = мъжки; 2 = женски; 3 = друг; 4 = интерсекс; 5 = различен; 6 = неопределен; 9 = не се прилага; За стойности 0, 1, 2 и 9 се прилага ISO/IEC 5218.
email_address	Адрес на електронна поща на ползвателя, за когото се отнасят данните за идентификация на лице [в съответствие с RFC 5322 ([1])].

Идентификатор на данни	Определение
mobile_phone_number	Номер на мобилния телефон на ползвателя, за когото се отнасят данните за идентификация на лице, като се започне със символа „+“ като префикс на международния код и кода на държавата, следван само от цифрите на номера.

([1]) P. Resnick, Ed., "Internet Message Format," RFC 5322, октомври 2008 г.

2) Раздел 2: Набор от данни за идентификация на юридическо лице

Таблица 3

Задължителни данни за идентификация на юридическото лице

Идентификатор на данни
настоящо юридическо наименование
уникален идентификатор, създаден от изпращащата държава членка в съответствие с техническите спецификации за целите на трансграничната идентификация, който да остава непроменен, колкото е възможно по-дълго време

— Когато идентификатор на данни не е известен за лицето или не може да бъде издаден по друг начин като част от набора от данни за идентификация на лицето, държавите членки използват вместо това подходяща за ситуацията стойност на атрибут.

Таблица 4

Незадължителни данни за идентификация на юридическото лице

Идентификатор на данни
настоящ адрес
регистрационен номер по ДДС
данъчен номер
Европейски единен идентификатор, посочен в Директива (ЕС) 2017/1132 на Европейския парламент и на Съвета ([1])
идентификационен код на правния субект (ИКПС), посочен в Регламент за изпълнение (ЕС) 2022/1860 на Комисията ([2])
идентификационен номер на икономически оператор (EORI номер), посочен в Регламент за изпълнение (ЕС) № 1352/2013 на Комисията ([3])
акцизен номер, предвиден в член 2, параграф 12 от Регламент (ЕС) № 389/2012 на Съвета ([4])

([1]) Директива (ЕС) 2017/1132 на Европейския парламент и на Съвета от 14 юни 2017 г. относно някои аспекти на дружественото право (OB L 169, 30.6.2017 г., стр. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Регламент за изпълнение (ЕС) 2022/1860 на Комисията от 10 юни 2022 г. за определяне на технически стандарти за изпълнение за прилагането на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета по отношение на стандартите, форматите, честотата, както и методите и механизмите за отчитане (OB L 262, 7.10.2022 г., стр. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Регламент за изпълнение (ЕС) № 1352/2013 на Комисията от 4 декември 2013 г. за установяване на формулярите, предвидени в Регламент (ЕС) № 608/2013 на Европейския парламент и на Съвета относно защитата на правата върху интелектуалната собственост, осъществявана от митническите органи (OB L 341, 18.12.2013 г., стр. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Регламент (ЕС) № 389/2012 на Съвета от 2 май 2012 г. относно административното сътрудничество в областта на акцизите и за отмяна на Регламент (ЕО) № 2073/2004 (OB L 121, 8.5.2012 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3) Раздел 3: Набор от метаданни за данните за идентификация на лица

Таблица 5

Метаданни за данните за идентификация на лица

Идентификатор на данни	Определение	Наличие
`issuing_authority`	Наименование на административния орган, издал данните за идентификация на лица, или alpha-2 кодът на държавата по ISO 3166 на съответната държава членка, ако няма отделен орган, който има право да издава данни за идентификацията на лица.	задължително
`issuing_country`	alpha-2 кодът на държавата, както е посочено в ISO 3166-1, за държавата или територията на доставчика на данните за идентификацията на лица.	задължително
`expiry_date`	Дата (и ако е възможен час), когато изтича административният срок на валидност на данните за идентификация на лица.	незадължително
`document_number`	Номер на данните за идентификация на лица, зададен от доставчика на данни за идентификация на лица.	незадължително
`issuing_jurisdiction`	Код на подразделение на държавата на юрисдикцията, издала данните за идентификация на лица, както е посочено в ISO 3166-2:2020, точка 8. Първата част на кода е същата като стойността за издаващата държава.	незадължително
`issuance_date`	Дата (и ако е възможен час), когато започва административният срок на валидност на данните за идентификация на лица.	незадължително

4) Раздел 4: Кодиране на атрибути на данни за идентификация на физически лица

— Данните за идентификация на физическо лице се издават в съответствие със стандартите, определени в точка 5 (формат SD-JWT VC) и точка 6 (формат ISO/IEC-mdoc) от приложение II към Регламент за изпълнение (ЕС) 2024/2979, както е приложимо за електронните удостоверения за атрибути. Точки 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 и 6.2.5 не се прилагат.

— Кодирането на данните за идентификация на физически лица трябва да отговаря на техническите спецификации в раздели 4.1 и 4.2 от настоящото приложение.

4.1 Encoding of natural person identification data in ISO/IEC-mdoc format (Кодиране на данни за идентификация на физически лица във формат ISO/IEC-mdoc)

— Видът на удостоверението за данните за идентификация на лица във формат ISO/IEC mdoc е „eu.europa.ec.eudi.pid.1“. Идентификаторът на именното пространство за атрибутите на данните за идентификация на лица, посочени в настоящото приложение, е „eu.europa.ec.eudi.pid.1“.

— Когато данните за идентификация на лица включват данни, за които идентификаторите на данни не са посочени в настоящото приложение, тези данни се определят в рамките на местно именно пространство на данни за идентификация на лице, за което се използва общият формат eu.europa.ec.eudi.pid. [код на държавата по ISO 3166-1 alpha-2 или код на региона по ISO 3166-2], следван незадължително от точка и номер на версия.

— Когато се използва местно именно пространство, неговата схема, включително всички идентификатори на данни, техните определения, изисквания за наличност и формати на кодиране, се публикуват в съответствие с член 8 от Регламент за изпълнение (ЕС) 2025/1569 на Комисията ([1]).

— Данните за идентификация на лица и техните метаданни, посочени в раздели 1 и 3 от настоящото приложение, се включват в елементите на данните за идентификация на лица по смисъла на спецификациите за формата ISO/IEC mdoc.

— Елементът deviceKey в рамките на елемента deviceKeyInfo, който е член на примерен обект от типа MobileSecurityObject, трябва да съдържа публичен ключ.

— Този публичен ключ съответства на частен ключ, който се съхранява в защитеното криптографско устройство на портфейла („WSCD“) на ползвателя на портфейла.

— Защитената заглавна част на цифровия подпис CB-AdES, с който се подписват данни за идентификация на лица във формат ISO/IEC-mdoc, съдържа параметрите в заглавната част x5u и x5t, посочени в RFC 9360 ([2]).

— Алгоритъмът за изчисляване на хеш стойности, използван в параметъра header x5t, е SHA-256.

— Изискванията за кодиране на данните за идентификация на лица във формат ISO/IEC-mdoc са посочени в таблица 6:

Таблица 6

Изисквания за кодиране на данни за идентификация на физически лица във формат ISO/IEC-mdoc

Идентификатор на данни	Идентификатор на атрибути	Формат на кодиране
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) 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).

([2]) J. Schaad, „CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates“(https://datatracker.ietf.org/doc/rfc9360/).

Идентификатор на данни	Идентификатор на атрибути	Формат на кодиране
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate или full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate или full-date

— При обозначаването на формата на кодиране на атрибутите, посочени в таблица 6, се използват видовете представяне, посочени в RFC 8610 ([3]), със следните допълнителни изисквания:

а) tstr се кодира в UTF-8;

б) tstr поддържа пълния обхват на unicode;

в) tstr има максимална дължина от 150 знака;

г) датата се кодира, както е посочено в RFC 8943 ([4]);

д) пълната дата се тълкува като #6.1004(tstr), където таг 1004 е посоченият в RFC 8943;

е) атрибутът tdate съдържа низ date-time, както е посочено в RFC 3339 ([5]);

ж) атрибутът full-date съдържа низ full-date, както е посочено в RFC 3339, в съответствие с RFC 8943;

з) освен ако не е посочено друго, при представянето на дата в атрибутите:

— не се използват части от секунди;

— не се използва локално отклонение от UTC и отклонението във времето, посочено в RFC 3339, е със стойност „Z“.

и) цяло число от основни типове 0 и 1 трябва да бъде възможно най-малко, както е посочено в RFC 8949 ([6]), раздел 4.2;

й) place_of_birth съдържа най-малко една от следните двойки с ключови стойности: „country“, „region“ или „locality“.

к) дължината в bstr, tstr, array или map се изразява възможно най-кратко, както е посочено в RFC 8949, раздел 4.2;

([3]) C. Vigano and H. Birkholz, „Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures“, RFC 8610, юни 2019 г.
([4]) M. Jones, A. Nadalin and J. Richter, „Concise Binary Object Representation (CBOR) Tags for Date“, RFC 8943, ноември 2020 г.
([5]) G. Klyne and C. Newman, „Date and Time on the Internet: Timestamps“, RFC 3339, юли 2002 г.
([6]) C. Bormann and P. Hoffman, „Concise Binary Object Representation (CBOR)“, RFC 8949, декември 2020.

л) атрибутът nationality се кодира като масив от alpha-2 кодове на държави, както е посочено в ISO 3166-1. Когато се използва обозначаване CDDL, както е посочено в RFC 8610, кодирането на този атрибут е:

— nationalities = [+ CountryCode]

— CountryCode = tstr; alpha-2 код на държава, посочен в ISO 3166-1;

— когато ползвател на портфейл, за когото се отнасят данните за идентификация на лице, има множество гражданства и доставчикът на данни за идентификация на лице удостоверява тези множество граждански, доставчикът на данни за идентификация на лице може да включи всички граждански в данните за идентификация на лице;

— атрибутът place_of_birth се кодира като вид place_of_birth. Когато се използва обозначаване CDDL, както е посочено в RFC 8610, кодирането на този атрибут е:

place_of_birth =

{

? 'country' : tstr; един alpha-2 код на държава, посочен в ISO 3166-1

? 'region': tstr; име на района, провинцията или областта

? 'locality': tstr; име на общината, агломерацията, града или селото

}

4.2 Изисквания за кодиране на данни за идентификация на физически лица във формат SD-JWT VC

— Данните за идентификация на лица и техните метаданни, посочени в настоящия раздел, се включват в данните за идентификация на лица като твърдения по смисъла на спецификациите за формата SD-JWT VC.

— Всички твърдения в издадените данни за идентификация на лица, посочени в предходното тире, трябва да могат избирателно да се оповестяват поотделно, с изключение на твърденията, определени като неизбирателно оповестими във формат SD-JWT VC.

— В таблица 7 е посочено кодирането на наименования на твърдения, които са публични наименования.

— В таблица 8 е посочено кодирането на наименования на твърдения, които са присъщи на данни за идентификация на лица.

— Низът JSON, използван в данните за идентификация на лица, кодирани във формат SD-JWT VC, трябва да бъде кодиран в UTF-8 и да поддържа пълния обхват на unicode, освен ако изрично не е посочено друго в таблица 8 по-долу или в позоваванията в нея.

— Твърденията nbf и exp в JWT, съгласно определеното в RFC 7519 ([7]), трябва да се използват за изразяване на срока на техническа валидност на данните за идентификация на лица, които са в съответствие с формата SD-JWT VC.

([7]) J. Jones, et al., „JSON Web Token (JWT),“ RFC 7519, май 2015 г.

— Данните за идентификация на лица трябва да включват твърдение cnf, както е определено в RFC 7800 ([8]), което е публичен ключ, генериран от частен ключ, съхраняван в защитеното криптографско устройство на портфейла на ползвателя на портфейла.

— Защитената заглавна част на цифровия подпис, с който се подписват данни за идентификация на лица във формат SD-JWT VC, съдържа параметрите в заглавната част x5u и header x5t#S256, посочени в RFC 7515 ([9]).

Таблица 7

Изисквания за кодиране на данни за идентификация на физически лица във формат SD-JWT VC с използване на публични наименования

Идентификатор на данни	Идентификатор на атрибути	Формат на кодиране
family_name	family_name	низ
given_name	given_name	низ
birth_date	birthdate	низ, ISO 8601-1, формат YYYY-MM-DD
birth_place	place_of_birth	структура JSON
nationality	nationalities	масив от низове
resident_address	address.formatted	низ
resident_country	address.country	низ
resident_state	address.region	низ
resident_city	address.locality	низ
resident_postal_code	address.postal_code	низ
resident_street	address.street_address	низ
family_name_birth	birth_family_name	низ
given_name_birth	birth_given_name	низ
email_address	email	низ
mobile_phone_number	phone_number	низ
portrait	picture	низ; URL за данни, съдържащ портретна снимка, кодирана с base64, във формат JPEG

([8]) M. Jones, et al., „Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)“, RFC 7800, април 2016 г.
([9]) M. Jones, et al., „JSON Web Signature (JWS)“, RFC 7515, май 2015 г.

Таблица 8

Изисквания за кодиране на данни за идентификация на физически лица във формат SD-JWT VC с използване на лични наименования

Идентификатор на данни	Идентификатор на атрибути	Формат на кодиране
expiry_date	date_of_expiry	низ, ISO 8601-1, формат YYYY-MM-DD
issuance_date	date_of_issuance	низ, ISO 8601-1, формат YYYY-MM-DD
personal_administrative_-number	personal_administrati-ve_number	низ
sex	sex	число
issuing_authority	issuing_authority	низ
issuing_country	issuing_country	низ
document_number	document_number	низ
issuing_jurisdiction	issuing_jurisdiction	низ

— Основният вид данни за идентификация на лица е „urn:eudi:pid:1“, включен в твърдението vct. Всички данни за идентификация на лица използват типове в именното пространство „urn:eudi:pid:“.

— Когато данните за идентификация на лица включват атрибути, които не са посочени в настоящото приложение, тези атрибути се определят в рамките на вътрешен тип.

— Когато се използва местен тип, неговата схема, включително всички идентификатори на данни, техните определения, изисквания за наличност и формати на кодиране, се определят в схема и се публикуват в съответствие с член 8 от Регламент за изпълнение (ЕС) 2025/1569.

5) Раздел 5: Подробности за доверителната инфраструктура

Списъкът на доставчиците на данни за идентификация на лица, предоставени от Комисията в съответствие с Регламент за изпълнение (ЕС) 2024/2980 позволява да се удостовери автентичността на данните за идентификация на лица.“

ПРИЛОЖЕНИЕ II

„*ПРИЛОЖЕНИЕ Ia*

Криптографски механизми, посочени в член 5а

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

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

ПРИЛОЖЕНИЕ III

„ПРИЛОЖЕНИЕ Iб

Технически спецификации за удостоверенията за портфейлен блок, посочени в член 6, параграф 2а

1) Удостоверението за портфейлен блок се състои от едно или повече удостоверения за инстанция на портфейла и едно или повече удостоверения на ключове.

2) Удостоверението за инстанция на портфейл и удостоверенията за ключ отговарят на следните изисквания:

а) Изисквания за формата

— FR-WIA-1: Удостоверението за инстанция на портфейла трябва да е JSON Web Token (JWT), както е посочено в RFC 7519 ([1]), подписано или подпечатано от доставчика на портфейла чрез компактен подпис JAdES baseline B.

— FR-WIA-1.1: Удостоверението за инстанция на портфейла е удостоверение за портфейл, както е посочено в допълнение Д към OpenID for Verifiable Credential Issuance v1.0 ([2]) („OID4VCI“), и разширено съгласно посоченото в C-WIA-1 и C-WIA-2 по-долу.

— FR-KA-1: Удостоверението за ключ трябва да е JWT, както е посочено в RFC 7519, подписано или подпечатано от доставчика на портфейла чрез компактен подпис JAdES baseline B.

— FR_KA_1.1: Удостоверението за ключ трябва да е удостоверение за ключ, както е посочено в допълнение Г към OID4VCI, и разширено съгласно посоченото в C_KA-1 и C_KA-2 по-долу.

б) Изисквания относно транспорта

— TR-WIA-1: Портфейлът трябва да използва удостоверение за инстанция на портфейл при издаването на данни за идентификация на лица, квалифицирани или неквалифицирани електронни удостоверения за атрибути или електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от негово име.

— TR-WIA-2: Доставчикът на портфейл проверява целостта на инстанцията на портфейла и подписва или подпечатва удостоверението на инстанцията на портфейла.

— TR-WIA-2.1: Когато доставчик на портфейл издава удостоверение за инстанция на портфейл, разликата между часа, в който доставчикът на портфейл проверява целостта на инстанцията на портфейл, и часа, който той посочва в параметъра header „exp“ на издаденото удостоверение за инстанция на портфейл, трябва да бъде по-малка от 24 часа.

— TR-WIA-2.2: Доставчикът на портфейл гарантира, че портфейлният блок съдържа удостоверенията за инстанция на портфейл, които са необходими за издаване на данни за идентификация на лице и електронни удостоверения за атрибути.

— TR-WIA-3: По време на издаване портфейлният блок изпраща удостоверение за инстанция на портфейл до сървъра за упълномощаване в изпратената заявка за упълномощаване и в заявката за токен, както е посочено в OID4VCI.

— TR-WIA-3.1: портфейлният блок изпраща удостоверението за инстанция на портфейл заедно с доказателство за притежание („PoP“), както е посочено в допълнение Д към OID4VCI.

— TR-WIA-3.2: Портфейлният блок изпраща същото удостоверение за инстанция на портфейл само до един сървър за упълномощаване.

([1]) RFC 7519: JSON Web Token (JWT), май 2015 г.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Когато доставчикът на портфейл използва опцията „per-issuer reuse“, посочена в R_WIA_1 по-долу, портфейлният блок може многократно да изпрати дадено удостоверение за инстанция на портфейл до един и същ сървър за упълномощаване.

— TR-WIA-3.2.2: Когато доставчикът на портфейл не използва опцията „per-issuer reuse“, портфейлният блок трябва да използва дадено удостоверение за инстанция на портфейл в най-много един процес на издаване.

— TR-WIA-4: Когато сървър за упълномощаване получи удостоверение за инстанция на портфейл, той трябва да провери подписа на удостоверението за инстанция на портфейл, използвайки публичния ключ в удостоверението за подпис, включен в параметъра „x5c“ в заглавната част на JOSE на удостоверението за инстанция на портфейл.

— TR-WIA-4.1: Сървърът за упълномощаване също така проверява дали това удостоверение за подпис може да бъде проверено с котва на доверие в списъка на доставчиците на портфейли, посочен в член 5 от Регламент за изпълнение (ЕС) 2024/2980, като потенциално се използват междинни удостоверения, включени в параметъра x5c.

— TR-WIA-4.2: Сървърът за упълномощаване проверява дали валидността на удостоверението за инстанция на портфейл не е изтекла.

— TR-WIA-4.3: Сървърът за упълномощаване проверява подписа на PoP под публичния ключ, който е в твърдението „cnf“.

— TR_KA-1: Портфейлът трябва да използва удостоверение за ключ при издаването на данни за идентификация на лица и при издаването на обвързани с устройство квалифицирани или неквалифицирани електронни удостоверения за атрибути или електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от негово име.

— TR_KA-1.1: Портфейлът не трябва да използва удостоверение за ключ при издаването на необвързани с устройство квалифицирани или неквалифицирани електронни удостоверения за атрибути или електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от негово име.

— TR_KA-2: Доставчикът на портфейл трябва да предостави на портфейлния блок различни удостоверения за ключ за защитеното криптографско устройство на портфейла и за всеки от неговите хранилища на ключове.

— TR_KA-2.1: Доставчикът на портфейла подписва или подпечатва удостоверение за ключ, след като е проверил, че ключовете, удостоверени в удостоверението за ключ, се съхраняват в защитеното криптографско устройство на портфейлния блок или в хранилището на ключове, посочено в удостоверението за ключ.

— TR_KA-2.2: Удостоверението за ключ трябва да съдържа поне един удостоверен публичен ключ. Броят на ключовете в удостоверението на ключове, изпратено до издател на акредитиви, не трябва да надвишава максималния размер на пакета, посочен от този издател на акредитиви в неговите метаданни за издател на акредитиви; вж. ETSI TS 119 472-3 ([3]), параметър „credential_confidations_supported. credential_metadata.credential_reuse_policy.options.batch_size“.

— TR_KA-2.3: Доставчикът на портфейл включва публичен ключ (съответстващ на частен ключ, съхраняван в защитеното криптографско устройство на портфейла или в хранилището на ключове на портфейлния блок) в най-много едно удостоверение за ключ.

— TR_KA-2.4: Портфейлният блок трябва да използва удостоверение за ключ в най-много един процес на издаване или преиздаване на акредитиви.

— TR_KA-2.5: Доставчикът на портфейл гарантира, че портфейлният блок притежава удостоверенията за ключове, които са необходими за издаване на данни за идентификация на лица и на обвързани с устройство електронни удостоверения за атрибути.

([3]) ETSI, „Електронни подписи и инфраструктура (ESI); JAdES цифрови подписи; Част 3: JAdES нива и базови прифили“, ETSI TS 119 472-3, V1.1.1, март 2026 г.

— TR_KA-3: Когато е необходимо по време на издаването, портфейлният блок включва удостоверение за ключ в полето „proofs“ на искането за удостоверение на самоличност до издателя на удостоверение, както е посочено в OID4VCI, като доказателство е от типа „jwt“ или от типа „attestation“.

— TR_KA_3.1: Когато портфейлен блок включва удостоверение за ключ в елемент „jwt“, той подписва или подпечатва удостоверението за ключ, като използва частния ключ, съответстващ на публичния ключ в индекс 0 от масива „attested_key“ в рамките на обекта „key_attestation“.

— TR_KA-4: Когато издателят на удостоверения издава обвързани с устройства акредитиви, той посочва в параметъра „proof_types_supported“ в своите метаданни за издател на акредитиви, както е посочено в раздел 12.2.4 на OID4VCI, че поддържа доказателство от типа „jwt“ и от типа „attestation“ за удостоверения за ключ, които включват обекта „key_attestation_required“.

— TR_KA-4.1: Когато издател на удостоверения за самоличност издава необвързани с устройства удостоверения, той трябва да пропуска параметрите „provid_types_supported“ и „cryptographic_-binding_methods_supported“ в метаданните на издателя на удостоверения за самоличност.

— TR_KA-5: Когато издател на удостоверение за самоличност получи удостоверение за ключ от тип доказателство „jwt“ или „attestation“, той проверява подписа на удостоверението за ключ с публичния ключ в удостоверението за подпис, включено в параметъра „x5c“ в заглавната част на JOSE в удостоверението за ключ, както и дали това удостоверение за подпис с котва на доверие е в списъка за доставчиците на портфейли, посочен в член 5 от Регламент за изпълнение (ЕС) 2024/2980, като потенциално използва междинни удостоверения, включени в параметъра „x5c“.

— TR_KA-6: Когато издател на удостоверение за самоличност получи удостоверение за ключ от тип доказателство „jwt“, той проверява подписа на елемента „jwt“ под ключа в индекс 0 от масива „attested_key“ в рамките на обекта „key_attestation“, включен в елемента „jwt“.

— TR_KA-6.1: Издателят на удостоверение за самоличност проверява дали полето „nonce“ на елемента „jwt“ включва валиден c_nonce от тяхната nonce_endpoint, както е посочено в OID4VCI.

— TR_KA-7: Когато издател на удостоверение за самоличност получи удостоверение за ключа от типа доказателство „attestation“, той проверява дали обектът „key_attestation“ включва валидно c_nonce от тяхната nonce_endpoint.

— TR_KA-8: Доставчикът на данни за идентификация на лица гарантира, че данните за идентификация на лица са обвързани с публичен ключ, който произхожда от удостоверение за ключ, в което се посочва защитено криптографско устройство на портфейла.

в) изисквания за съдържанието

— C_WIA-1: Удостоверението за инстанция на портфейл трябва да съдържа следното:

— твърдението „wallet_name“, посочено в допълнение Д към OID4VCI, чиято стойност е идентификаторът на технологичното решение за портфейл от списъка на доставчиците на портфейли, посочен в член 5 от Регламент за изпълнение (ЕС) 2024/2980.

— твърдението „wallet_version“ ([4]), т.е. низ, чиято стойност е версията на технологичното решение за портфейл.

— твърдението „wallet_solution_certification_information“, което представлява обект от JSON, съдържащ информация за органа за оценяване на съответствието, който е сертифицирал технологичното решение за портфейл, сертификационния номер, според случая, и други съответни подробности по отношение на сертифицирането.

([4]) Това твърдение е определено в настоящия регламент за изпълнение на Комисията, тъй като не е част от спецификацията OID4VCI.

— твърдение „client_status“, съдържащо две подполета:

— 'status': отнася се за списъка със статуси, както е посочено в допълнение Д към OID4VCI, който представлява статуса на отмяна на инстанцията на портфейл. За повече подробности вж. раздел д) по-долу;

— 'exp': NumericDate, както е посочено в RFC 7519, определя времето, до което доставчикът на портфейл ще поддържа статуса на отмяна в индекса на списъка със статуси, посочен в „status“.

— твърдението „exp“, посочено в допълнение Д към OID4VCI.

— *БЕЛЕЖКА*: Твърдението „client_status.status“ в удостоверение за инстанция на портфейл представлява статусът на отмяна на инстанцията на портфейл, а не статусът на отмяна на самото удостоверение. Както е описано в R_WIA- -1 по-долу, доставчикът на портфейл може да реши да разшири обхвата на всяко удостоверение за инстанция на портфейл и да включи конкретен сървър за упълномощаване въз основа на факта, че всички удостоверения, изпратени до този сървър, съдържат една и съща стойност на индекса във вписването „client_status.status“.

— *БЕЛЕЖКА*: Стойността „idx“ в твърдението „status“ може да се използва като уникален идентификатор (по двойки) на инстанцията на портфейл и на портфейлния блок.

— C_WIA-2: Удостоверението за инстанция на портфейл следва да включва и твърдението „wallet_link“, посочено в допълнение Д към OID4VCI, като стойността на това твърдение е URI, където може се съдържа допълнителна информация за технологичното решение за портфейл.

— C_WIA-3: Сървърът за упълномощаване не трябва да тълкува параметъра „exp“ в най-високото ниво на удостоверението за инстанция на портфейл като край на периода на поддържане на отмяната на инстанцията на портфейл.

— *БЕЛЕЖКА*: Параметърът „exp“ в най-високото ниво на удостоверението за инстанция на портфейл означава, че срокът на валидност на самото удостоверение изтича.

— C_KA-1: Удостоверението за ключ трябва да включва:

— твърденията „key_storage“ и „user_authentication“, посочени в допълнение Г към OID4VCI.

— атрибутите „key_storage“ и „user_authentication“ имат стойност „iso_18045_high“, когато в удостоверението за ключ се споменава защитено криптографско устройство на портфейл,

— твърдението „certification“, посочено в допълнение Г към OID4VCI, съдържащо URL адрес с информация относно сертифицирането, постигнато от защитеното криптографско устройство на портфейла или хранилището на ключове, ориентировъчно схемата, като например Common Criteria или GlobalPlatform, оценените изисквания, като например приложимия защитен профил, и нивото на оценка.

— Въз основа на тази информация трябва да е възможно да се определи дали хранилището на ключа е защитено криптографско устройство на портфейл.

— твърдение „key_storage_status“, съдържащо две подполета:

— „status“: отнася се за списъка със статуси, както е посочено в допълнение Д.1 към OID4VCI. Стойността представлява статусът на отмяна на WSCD или типа хранилище на ключове, използвано за съхраняване на удостоверените ключове, или — в рамките на опцията за индекс per-key-attestation — статусът на отмяна на защитено криптографско устройство или хранилище на ключ на отделен портфейлен блок. Вж. R_KA_1 по-долу наличните варианти при задаване на индекси;

— 'exp': NumericDate, както е посочено в RFC 7519, определя времето, до което доставчикът на портфейл ще поддържа статуса на отмяна в индекса на списъка със статуси, посочен в „status“.

— твърдението „exp“, посочено в допълнение Г към OID4VCI.

— *БЕЛЕЖКА* относно стойността на „idx“ в твърдението „key_storage_status.status“ в удостоверение за ключ: Когато доставчикът на портфейл използва опцията „type-shared index“ (вж. R_KA_1 по-долу), всички удостоверения за ключ за един и същ вид защитено криптографско устройство или хранилище за ключове имат един и същ индекс на списъка със статуси. Следователно стойността „idx“ не е уникална за всеки портфейлен блок. Напротив, когато доставчикът на портфейл използва опцията „per-key-attestation index“, стойността „idx“ е уникална за портфейлния блок (или уникална по двойки за всеки издател на удостоверение). Във всички случаи обаче издателят на удостоверение за самоличност не използва стойността „idx“ в удостоверение за ключ като идентификатор на портфейлен блок, а вместо това използва стойността „idx“ в удостоверение на инстанция на портфейл.

— C_KA-2: Когато се изпраща удостоверение за ключ като доказателство от тип „attestation“, то трябва да включва и валидно c_nonce, както е посочено в допълнение E.3 към OID4VCI.

— C_KA-3: Издател на удостоверение за самоличност не трябва да тълкува параметъра „exp“ в най-високото ниво на удостоверението за ключ като край на периода на поддържане на отмяната на защитеното криптографско устройство на портфейл или хранилището на ключове.

— *БЕЛЕЖКА*: Параметърът „exp“ в най-високото ниво на удостоверението за ключ означава, че срокът на валидност на самото удостоверение за ключ изтича.

г) Изисквания за жизнения цикъл

— В настоящото приложение се определят следните параметри на метаданните за издателя на акредитиви:

— 'preferred_client_status_period': OPTIONAL. Цяло число, посочващо предпочитания оставащ период на поддържане на статуса на удостоверението за инстанция на портфейл, което трябва да се показва от модула на портфейла по време на издаването, в секунди. Оставащият период на поддържане на статуса се определя като стойността на „client_status.exp“ в удостоверението минус времето за получаване на удостоверението.

— 'preferred_key_storage_status_period': OPTIONAL. Цяло число, посочващо предпочитания оставащ период на поддържане на статуса на удостоверението за ключ, което трябва да се показва от модула на портфейла по време на издаването, в секунди. Оставащият период на поддържане на статуса се определя като стойността на „key_storage_status.exp“ в удостоверението минус времето за получаване на удостоверението.

— LC_WIA-1: Сървър за упълномощаване може да съобщи своите предпочитания за оставащия период на поддържане на статуса в удостоверенията за инстанция на портфейл, като включи параметъра на метаданните „preferred_client_status_period“ в своята крайна точка за метаданни на издателя на удостоверения за самоличност, както е посочено в раздел 12.2.2 от OID4VCI.

— LC_WIA-1.1: Това поле се поставя на най-високото ниво на метаданните на издателя на удостоверения за самоличност

— LC_WIA_2: Сървърът за упълномощаване не трябва да тълкува параметъра „exp“ в най-високото ниво на удостоверението за инстанция на портфейл като край на периода на поддържане на отмяната на инстанцията на портфейл.

— LC_WIA_3: Когато доставчик на портфейл подпише или подпечата удостоверение за инстанция на портфейла, той запазва статуса на отмяна на съответната инстанция на портфейл до изтичането на „wallet_instance_status.exp“, посочен в това удостоверение за инстанция на портфейл.

— LC_KA-1: Когато е необходимо удостоверение за ключ, издателят на удостоверение за самоличност може да съобщи своите предпочитания за оставащия период на поддържане на статуса в удостоверенията за ключ, като включи посочения по-горе параметър на метаданните „preferred_key_storage_status_period“ в своята крайна точка на издателя на удостоверения за самоличност, както е посочено в раздел 12.2.2 от OID4VCI.

— LC_KA-1.1: Полето трябва да се постави в обекта „key_attestations_required“, както е посочено в раздел 12.2.4 от OID4VCI.

— LC_KA-2: Доставчикът на портфейл трябва да избере периода на техническа валидност на удостоверенията за ключ, които издава.

— LC_KA-3: Когато доставчик на портфейл подпише или подпечата удостоверение за ключ, той запазва статуса на отмяна на съответното защитено криптографско устройство на портфейла или хранилище на ключове до изтичането на „key_storage_status.exp“, посочен в това удостоверение за ключ.

— LC_GEN-1: Доставчикът на портфейл гарантира, че портфейлният блок винаги може да представи удостоверения за портфейлен блок и удостоверения за ключ, чиито статуси „client_status.exp“ и „key_storage_status.exp“ (съответно) са най-малко 31 дни в бъдещето към момента на представяне на сървър за упълномощаване или на издател на удостоверения за самоличност.

— *БЕЛЕЖКА*: Това гарантира, че доставчиците на данни за идентификация на лица могат да разчитат на верижно отнемане, без да са принудени да издават кратковременни данни за идентификация на лица.

— LC_GEN-2: Доставчикът на портфейл трябва да гарантира, че портфейлният блок извличаметаданните на издателя на акредитиви при издаване.

  — LC_GEN_2.1: Ако в тези метаданни е включено поле „preferred_key_storage_status_duration“, портфейлният блок изпраща удостоверение за ключ с („key_storage_status.exp“ – текущо време) – „preferred_key_storage_status_period“ с възможно най-малка стойност, но не отрицателно. Ако портфейлният блок не разполага с такова удостоверение за ключ, той трябва да получи ново удостоверение за ключ от доставчика на портфейла, което отговаря на „key_storage_status.exp“ – текущо време ≥ „preferred_key_storage_status_period“.

  — LC_GEN_2.2: Ако в тези метаданни е включено поле „preferred_client_status_duration“, портфейлният блок изпраща удостоверение за инстанция на портфейл с („client_status.exp“ – текущо време) – „preferred_client_status_period“ с възможно най-малка стойност, но не отрицателно. Ако портфейлният блок не разполага с такова удостоверение за инстанция на портфейл, той трябва да подаде заявка за ново удостоверение за инстанция на портфейл от доставчика на портфейла, което отговаря на „client_status.exp“ – текущо време ≥ „preferred_client_-status_period“.

— LC_GEN-3: Срокът на техническа валидност на данните за идентификация на лица приключва преди „client_status.exp“ на удостоверението за инстанция на портфейл и „key_storage_status.exp“ на удостоверението за ключ, изпратени на доставчика на данни за идентификация на лица в процеса на издаване.

— LC_GEN-4: Доставчикът на данни за идентификация на лица със срок на техническа валидност над 24 часа проверява статуса на отмяна както на удостоверението за инстанция на портфейл, така и на удостоверението за ключ, получени в процеса на издаване, най-малко веднъж на всеки 24 часа по време на срока на техническа валидност на данните за идентификация на лица. Когато някое от двете бъде отменено, доставчикът отменя данните за идентификация на лица.

д) Изисквания за отмяна

— R_GEN-1: Доставчикът на портфейл използва списъци със статус на токените (посочени в списъка IETF Token Status List) като механизъм за отмяна както на удостоверенията за ключ, така и на удостоверенията за инстанция на портфейл, както е посочено съответно в допълнения Г и Д към OID4VCI.

— *БЕЛЕЖКА*: За да подобри мащабируемостта на своите списъци със статуси, доставчикът на портфейл може да използва следните оптимизации:

  — Списъкът със статуси да се раздели на множество части, когато доставчиците на портфейли имат значителен брой ползватели и издадени удостоверения. Големината на частите зависи от признаци като определен размер на списъка или период от време. Доставчикът на портфейл решава как да раздели списъка. Евентуалните съображения могат да включват размера на списъка със статуси при изтегляне и неприкосновеността на личните данни на потребителя.

  — Да се предлагат множество списъци със статуси.

  — Да се компресира списъкът със статуси, за да се намали размерът му.

— R_WIA-1: Доставчикът на портфейл може да зададе същата стойност на твърдението „idx“ в твърдението „client_status.status“ във всички удостоверения за инстанция на портфейл, които даден портфейлен блок представя на един и същ сървър за упълномощаване. Това се опцията „per-issuer reuse“. Ако се използва този вариант:

  — R_WIA-1.1: Портфейлният блок помни стойността на индекса, която е използвал за всеки сървър за упълномощаване, с който е взаимодействал преди това, и подава заявка за удостоверение за инстанция на портфейл със същата стойност на индекса, когато взаимодейства отново със същия сървър за упълномощаване.

  — R_WIA-1.2: Когато доставчик на портфейл получи заявка за удостоверение за инстанция на портфейл, съдържащо конкретна стойност на индекса, той проверява дали подалият заявката модул на портфейла е получавал тази стойност на индекс в миналото преди да издаде ново удостоверение за инстанция на портфейл с тази стойност на индекса.

  — R_WIA-1.3: Портфейлният блок не трябва да използва повторно един и същ индекс за взаимодействия с други сървъри за упълномощаване.

— *БЕЛЕЖКА*: Ако се използва опцията „per-issuer reuse“, доставчикът на портфейл ще може да определи с колко сървъра за упълномощаване е взаимодействал портфейлният блок и колко често взаимодейства с всеки от тях.

— R_WIA-2: В своята политика за поверителност доставчикът на портфейл документира дали използва опцията „per-issuer reuse“ за отмяна на инстанция на портфейл.

— R_WIA-3: Когато доставчик на портфейл не използва опцията „per-issuer reuse“, той задава нова, несвързана стойност на индекс за всяко удостоверение за инстанция на портфейл, което издава.

— R_WIA-4: Когато даден портфейлен блок трябва да бъде отменен, доставчикът на портфейл отменя стойностите на индексва в твърдението „client_status.status“ във всички удостоверения за инстанция на портфейл, свързани с този портфейлен блок.

— R_WIA-5: Доставчикът на портфейл взема предвид в какви мащаби внедрява и каква е основната архитектура, когато определя размера на своите списъци със статуси на удостоверенията за инстанция на портфейл, като гарантира, че те са достатъчно големи, за да се предотврати взаимовръзка и да се защити неприкосновеността на личния живот на потребителите. Когато е възможно, списъкът със статуси се отнася за най-малко 10 000 удостоверения.

— R_KA_1: Доставчикът на портфейл избира една от следните варианти за задаване на индекс за твърдението „key_storage_status.status“ в удостоверението за ключ:

  — Вариант 1, наречен „type-shared index“, при който всички удостоверения за ключ, удостоверяващи ключове и съхранявани в един и същ тип WSCD или хранилище на ключове, съдържат една и съща стойност за индекс в „key_storage_status.status“.

  — Вариант 2, наречен „per-key-attestion index“, при който дадено удостоверение за ключ, удостоверяващо ключове и съхранявано в индивидуално защитено криптографско устройство на портфейл или хранилище на ключове, съдържа уникална (по двойки) стойност за индекс в „key_storage_status.status“.

— *БЕЛЕЖКА*: Когато доставчик на портфейл използва вариант 1, едно действие за отмяна обезсилва всички удостоверения за ключ от засегнатия вид за всички портфейлни блокове. Освен това, тъй като всички удостоверения за ключ за един и същ вид защитено криптографско устройство на портфейл или хранилище за ключове споделят единен индекс на списъка със статуси, броят на вписванията в даден списък със статуси на удостоверения за ключове отразява броя на видовете защитени криптографски устройства на портфейл или хранилища на ключове, поддържани от доставчика на портфейл, а не броя на внедрени портфейлни блокове. Поради това съображенията, свързани с неприкосновеността на личния живот, които обосновават минималния размер на списъка със статуси за списъците със статуси на инстанции на портфейл, не се прилагат за списъците със статуси на удостоверенията за ключове при вариант 1, при условие че има достатъчно много портфейлни блокове, използващи един и същ вид защитено криптографско устройство на портфейл или хранилище на ключове.

— *БЕЛЕЖКА*: Когато доставчик на портфейл използва вариант 2, всеки индекс представлява статуса на отмяна на конкретното защитено криптографско устройство на портфейл или хранилище на ключове, удостоверен в това удостоверение за ключ.

— *БЕЛЕЖКА*: Когато доставчик на портфейл използва вариант 2, конкретно защитено криптографско устройство на портфейл или хранилище на ключове също може да бъде отменено по искане на потребителя.

— R_KA-2: Когато доставчик на портфейл използва вариант 2, той може по избор да използва опцията „per-issuer reuse“, описана в R_WIA-1. Ако доставчикът на портфейл използва този вариант, изискванията R_WIA-1 — R_WIA-3 се прилагат mutatis mutandis.

— R_KA-3: Когато доставчик на портфейл използва вариант 2, той взема предвид в какви мащаби внедрява и каква е основната архитектура, когато определя размера на своите списъци със статуси на удостоверенията за ключове, като гарантира, че те са достатъчно големи, за да се предотврати взаимовръзка и да се защити неприкосновеността на личния живот на потребителите. Когато е възможно, списъкът със статуси се отнася за най-малко 10 000 удостоверения за ключове.

— R_KA-4: Когато доставчик на портфейл използва вариант 1 (type-shared index), той отменя записа „key_storage_status.status“ само ако видът на защитеното криптографско устройство на портфейл или на хранилището на ключове е уязвимо по отношение на сигурността.

е) Изисквания по отношение на алгоритмите за електронни подписи

— SA-1: За подписване на удостоверенията за инстанция на портфейл, удостоверенията за ключ, свързаните с тях доказателства за собственост и списъци със статуси на токените се използва един от следните алгоритми:

  — ES256 (ECDSA с SHA-256 и P-256)

  — ES384 (ECDSA с SHA-384 и P-384)

  — ES512 (ECDSA с SHA-512 и P-521)

— SA-2: Доставчикът на портфейл избира кой от алгоритмите, посочени в SA-1, ще използва.

— SA-3: Сървър за упълномощаване или издател на акредитиви (както е посочено в OID4VCI) поддържа всички алгоритми, посочени в SA-1.“

ПРИЛОЖЕНИЕ IV

„ПРИЛОЖЕНИЕ II

Списък на стандартите, посочени в член 8

Прилагат се техническите спецификации, посочени в точки 2—6 от ETSI TS 119 472-1 V1.2.1 (2026-02). Те се четат със следните адаптации:

1) 2.1 Normative references (Нормативни препратки)

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): „Електронни подписи и инфраструктура (ESI); Профили на удостоверенията; Част 1: Преглед и общи структури на данните“.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): „Електронни подписи и доверителна инфраструктура за удостоверяване (ESI); Профили на удостоверенията; Част 6: Изисквания за профил на удостоверения за доставчици на PID (данни за идентификация на лица), портфейл, EAA (електронни удостоверения за атрибути), QEAA (квалифицирани електронни удостоверения за атрибути) и PSBEAA (специфична за доставчика бизнес логика за EAA)“.

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: „Token Status List“, 20 април 2026 г.

2) 4.2.11.1 Общи изисквания

— EAA-4.2.11.1-06: Когато елементът status се използва за данни за идентификация на лица, квалифицирани електронни удостоверения за атрибути или електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от негово име, в него трябва да е посочено единствено дали удостоверението е отменено или не е отменено и не се поддържат никакви други стойности за статуса, например временно спиране.

— EAA-4.2.11.1-06.1: Когато се отменя удостоверение, то се отменя завинаги.

3) 4.2.13 EAA short-lived (кратковременни EAA)

— EAA-4.2.13-03: Когато се издават кратковременни електронни удостоверения за атрибути със срок на валидност от 24 часа или по-малко, не се изисква отмяна.

4) 4.6.3 Изисквания за EAA от ЕС, издавани от публичен орган, отговарящ за автентичен източник, или от името на такъв орган (PuB-EAA)

— PuB-EAA-4.6.2-03: празно.

— Pub-EAA-4.6.2-04: празно.

— PuB-EAA-4.6.3-03: Цифровият подпис PuB-EAA следва да съдържа квалифицираното удостоверение, поддържащо цифровия подпис PuB-EAA.

— PuB-EAA-4.6.3-04: Квалифицираното удостоверение, поддържащо цифровия подпис PuB-EAA, трябва да отговаря на изискванията на точка 8 от ETSI TS 119 412-6 v1.1.1 и да съдържа QcType QcStatement, както е определено в ETSI EN 319 412-5 v2.5.1, със стойност id-etsi-qct-eidaspsbeaa, определена, както следва:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Сертификат, посочен в член 45е, параграф 1, буква б), поддържащ квалифицирания електронен подпис или квалифицирания електронен печат на органа от обществения сектор, посочен в член 3, точка 46 от Регламент (ЕС) № 910/2014.

5) 5.2.10.1 Общи изисквания

— EAA-5.2.10.1-04: празно.

— EAA-5.2.10.1-05: празно.

— EAA-5.2.10.1-06: Елементът status може да съдържа елемента status_list, както е посочено в точка 6.2 от IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: празно.

— EAA-5.2.10.1-08: празно.

— EAA-5.2.10.1-09: празно.

— EAA-5.2.10.1-10: празно.

— EAA-5.2.10.1-11: празно.

— EAA-5.2.10.1-12: празно.

6) 6.2.10.1 Общи изисквания

— EAA-6.2.10.1-01: Когато електронно удостоверение за атрибути, съответстващо на ISO/IEC mdoc, използва механизма на списъка със статуси на удостоверения, както е посочено в EAA-6.2.10.1-02.2, или механизма на списъка с отменени удостоверения, както е посочено в EAA-6.2.10.1-02.3, неговият мобилен елемент за сигурност (MSO) съдържа структурата на статуса, както е посочено в EAA-6.2.10.1-17, която съдържа информация за отмяната на MSO.

— EAA-6.2.10.1-01.1: При използване на механизма на списъка с идентификатори, елементът status трябва да съдържа елемента identifier_list, посочен в EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: При използване на механизма на списъка със статуси, елементът status трябва да съдържа елемента status_list, посочен в EAA-6.2.10.1-13.

— *БЕЛЕЖКА*:

  — Структурата на статуса съдържа препратка към списък на отменените MSO.

  — Списъкът на отменените MSO е със структура COSE_Sign1, която показва дали даден MSO е отменен или не.

  — Структурата на статуса съдържа цялата информация, необходима на доверяващата се на портфейл страна, за да определи дали списъкът на отменените MSO е автентичен.

— EAA-6.2.10.1-02: Доставчикът на данни за идентификация на лица, доставчикът на квалифицирани електронни удостоверения за атрибути или доставчикът на електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от името на такъв орган, използва един от следните методи за отмяна на данни за идентификация на лица, квалифицирани електронни удостоверения за атрибути или електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от името на такъв орган:

— EAA-6.2.10.1-02.1: Когато издават кратковременни електронни удостоверения за атрибути със срок на валидност от 24 часа или по-малко, отмяна не се изисква.

— EAA-6.2.10.1-02.2: Те използват механизма на списъка със статуси на удостоверения, за да кодират информацията за отмяната като списък със статуси.

— EAA-6.2.10.1-02.2.1: Механизмът на списъка със статуси отменя MSO въз основа на това дали битът на определената от издателя позиция на бита в MSO е зададен като „true“ в списъка със статуси.

— EAA-6.2.10.1-02.2.2: Механизмът на списъка със статуси е посочен в спецификацията на списъка със статуси на токените (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: Те използват механизма на списъка за отмяна на удостоверения, за да кодират информацията за отмяната като списък с идентификатори.

— EAA-6.2.10.1-02.3.1: Механизмът на списъка с идентификатори отменя MSO въз основа на това дали определеният от издателя идентификатор в MSO присъства в списъка с идентификатори.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 и EAA-6.2.10.1-11 определят механизма на списъка с идентификатори въз основа на изискванията от спецификацията за списъка със статуси на токените, включително на сходството между механизма на списъка със статуси и механизма на списъка с идентификатори.

— EAA-6.2.10.1-03: Когато се използва елемент status за данни за идентификация на лица, квалифицирани електронни удостоверения за атрибути или електронни удостоверения за атрибути, предоставяни от орган от публичния сектор, отговарящ за автентичен източник, или от негово име, трябва да се използва изключително статусът „revoked“.

— EAA-6.2.10.1-03.1: За списък със статуси това предполага, че се използват само стойности „valid“ и „invalid“, както е посочено в спецификацията на списъка със статуси на токени.

— EAA-6.2.10.1-03.2: За списъка с идентификатори — в него се включват само отменени MSO, а не временно спрени.

— EAA-6.2.10.1-04: Когато се отменя MSO, отмяната е завинаги.

— EAA-6.2.10.1-05: Проверката на списъка на отменените MSO не е задължителна за доверяващата се на портфейл страна и, когато е приложимо, проверката трябва да отговаря на изискванията за проверка, посочени в спецификацията за списъка със статуси на токени и в спецификацията за структура на статуса, съгласно посоченото в EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Когато доверяваща се на портфейл страна трябва да може да провери статуса на отмяна на данни за идентификация на лица или електронни удостоверения за атрибути, тя трябва да поддържа както механизма за списъка със статуси на удостоверения, така и механизма за списъка с отменени удостоверения, както е посочено в EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: identifier_list и status_list в MSO може да съдържат елемента certificate.

— EAA-6.2.10.1-06.1: Когато елементът certificate е налице, той трябва да съдържа удостоверението с публичния ключ, с който е било подписано или подпечатано удостоверението от най-високо ниво в елемента x5chain в структурата на списъка с отменени MSO.

— EAA-6.2.10.1-06.1.1: Доверяващата се на портфейл страна трябва да използва това удостоверение като котва на доверие за проверката на елемента x5chain в структурата на списъка с отменени MSO.

— EAA-6.2.10.1-06.2: Когато елементът certificate не е налице, удостоверението от най-високо ниво в елемента x5chain в структурата на списъка с отменени MSO трябва да бъде подписано или подпечатано с удостоверението, използвано за подписване на удостоверението в елемента x5chain на MSO.

— EAA-6.2.10.1-06.2.1: Доверяващата се на портфейл страна трябва да използва това удостоверение като котва на доверие за проверката на елемента x5chain в структурата на списъка с отменени MSO.

— EAA-6.2.10.1-07: Списъкът с отменени MSO трябва да се прилага в съответствие със спецификациите за списъка със статуси на токени като токен от списък със статуси във формат CWT.

— EAA-6.2.10.1-08: За списъка с отменени MSO при механизма на списъка с идентификатори и механизма на списъка със статуси се прилагат следните изисквания:

  — трябва да е налице твърдението exp.

  — може да е налице твърдението ttl.

  — твърдението aggregation_uri в твърдението IdentifierList или StatusList може да е налице и доставчикът на данни за идентификация на лица, доставчикът на квалифицирани електронни удостоверения за атрибути или доставчикът на електронни удостоверения за атрибути, предоставяни от орган от

публичния сектор, отговарящ за автентичен източник, или от негово име, може да използва твърдението aggregation_uri, за да укаже поддържане на механизма за агрегиране, както е посочено в спецификацията на списъка със статуси на токени.

— CWT трябва да бъде обект COSE_Sign1, като се използва един от следните алгоритми за подпис за изчисляване на подписа:

а) „ES256“ (ECDSA с крива NIST P-256 и SHA-256);

б) „ES384“ (ECDSA с крива NIST P-384 и SHA-384);

в) „ES512“ (ECDSA с крива NIST P-521 и SHA-512);

г) „ESB256“ (ECDSA с крива brainpoolP256r1 и SHA-256);

д) „ESB384“ (ECDSA с крива brainpoolP384r1 и SHA-384);

е) „ESB512“ (ECDSA с крива brainpoolP512r1 и SHA-512);

— CWT трябва да съдържа x5chain в защитената заглавна част, която съдържа удостоверението или веригата от удостоверения за проверка на подписа на списъка с отменени MSO.

— удължената употреба на ключа на идентификатора на обект, посочен в спецификацията на списъка със статуси на токени, може да се използва за удостоверението за подписване на списъка със статуси и списъка с идентификатори и инстанциите на доверяващата се на портфейл страна може да поддържат удължената употреба на ключа на идентификатори на обекти, посочени в спецификацията на списъка със статуси на токени, а за идентификатора на обект доставчикът на квалифицирани електронни удостоверения за атрибути или доставчикът на електронни удостоверения за атрибути, предоставяни от орган от публичния сектор или от името на такъв орган, не трябва да правят полето за удължена употреба на ключа от критично значение, когато прилагат удължената употреба на ключа OID, посочена в спецификацията на списъка със статуси на токени.

— EAA-6.2.10.1-09: За разлика от изискванията за спецификациите на списъка със статуси на токени за механизма на списъка с идентификатори се прилагат следните изисквания:

— стойността на вида твърдение трябва да бъде „application/identifierlist + cwt“;

— твърдението StatusList не трябва да присъства в набора от твърдения CWT;

— структурата на IdentifierList, определена в EAA-6.2.10.1-11, трябва да присъства като твърдение в набора от твърдения CWT, като се използва ключ 65530.

— EAA-6.2.10.1-10: Структурата IdentifierList е структура CBOR със следния CDDL:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Когато идентификаторът в IdentifierList е налице, MSO с идентификатора в елемента status се отменя.

— EAA-6.2.10.1-10.2: Твърдението aggregation_uri е уточнено в раздел 9.2 от спецификациите на списъка със статуси на токени.

— EAA-6.2.10.1-10.3: Списъкът с идентификатори за типа съдържание е „application/identifierlist + cwt“, посочен в изискванията в раздел 8.2 от спецификацията на списъка със статуси на токени.

— EAA-6.2.10.1-11: Следните изисквания се прилагат за елемента identifier_list в MSO (вж. EAA-6.2.10.1-17):

— EAA-6.2.10.1-11.1: Елементът identifier_list е структура CBOR със следния CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: За да се предотврати използването на идентификатора като взаимовръзка между представянията, той трябва да бъде уникален за всеки MSO.

— EAA-6.2.10.1-12: За списъка със статуси важат следните изисквания:

  — EAA-6.2.10.1-12.1: Елементът bits в структурата на StatusList трябва да е със стойност 1.

— EAA-6.2.10.1-13: Следните изисквания се прилагат за елемента status_list в MSO (вж. EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Елементът status_list следва изискванията за структурата на StatusListInfo, както е посочено в спецификацията за списъка със статуси на токени, и се добавя незадължителният елемент certificate, определен в EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: За да се предотврати индексът на статусите да бъде взаимовръзка между представянията, комбинацията от индекс на статусите и URI трябва да бъде уникална за всеки MSO.

— EAA-6.2.10.1-14: Доставчикът на портфейл използва втория (EAA-6.2.10.1-02.2) или третия (EAA-6.2.10.1-02.3) от методите, посочени в EAA-6.2.10.1-02, за отмяна на удостоверение за инстанция на портфейл (WIA) и на удостоверение за ключ (KA).

— EAA-6.2.10.1-15: Доставчикът на портфейл прилага в своето решение за портфейл механизмите за отмяна на удостоверение, посочени в EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: Доставчикът на данни за идентификация на лица и доставчикът на електронни удостоверения за атрибути поддържат както механизма за списък със статуси на удостоверения, така и механизма за списък на отменени удостоверения, посочени в EAA-6.2.10.1-02, за проверка на статуса на отмяна на удостоверение за инстанция на портфейл (WIA) и на удостоверение за ключ (KA).

— EAA-6.2.10.1-17: Структурата на статуса в MSO е структура CBOR със следния CDDL:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}“

ПРИЛОЖЕНИЕ V

„ПРИЛОЖЕНИЕ III

Технически спецификации, посочени в член 10

— Технически спецификации:

  — Точка 4.2.5 от ETSI TS 119 472-3 V1.1.1 (2026-03).“

ПРИЛОЖЕНИЕ VI

Приложение IV към Регламент за изпълнение (ЕС) 2024/2979 се изменя, както следва:

1) Точка 1 се заменя със следното:

„1. Задължителен формат на подпис или печат:

a) PAdES (Усъвършенствани електронни подписи във формат PDF), както е посочено в ETSI EN 319 142-1 V1.2.1 (2024-01); Електронни подписи и инфраструктура (ESI); PAdES цифрови подписи; Част 1: Градивни елементи и базови PAdES подписи.“

2) Точка 3 се заменя със следното:

„3. Приложно-програмен интерфейс:
ETSI TS 119 432 v1.3.1 (2026-03), точки 6.4.3, A.6, A.7 и A.8.“

ПРИЛОЖЕНИЕ VII

„ПРИЛОЖЕНИЕ VI

Цветна марка за доверие на ЕС за портфейл за цифрова самоличност



“

ПРИЛОЖЕНИЕ VIII

„ПРИЛОЖЕНИЕ VII

Чернобяла марка за доверие на ЕС за портфейл за цифрова самоличност



“

ПРИЛОЖЕНИЕ IX

„ПРИЛОЖЕНИЕ VIII

Данни за марка за доверие на ЕС за портфейл за цифрова самоличност

Данни	Описание	Кодиране	Статус
TrustMarkResourceURL	URL адрес на изображението на марката за доверие на ЕС за портфейл за цифрова самоличност и ресурси с информация за потребителите в потребителския интерфейс на портфейла.	URL адрес	задължително
ListOfCertifiedWalletsURL	URL адрес на публичния списък на сертифицираните технологични решения за портфейл в ЕС, както е посочено в Регламент за изпълнение (ЕС) 2025/849 на Комисията ([1]).	URL адрес	задължително
ListOfCertifiedWalletsQRCode	Код QR с информация за ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	незадължително
WalletSolutionInfoPageURL	URL адрес на информационната страница на сертифицираното технологично решение за портфейл в списъка на страницата за сертифицирани технологични решения за портфейл от URL адреса ListOfCertifiedWalletsURL с приложен знак „?“ и идентификатора WalletSolutionID на технологичното решение за портфейл.	URL адрес	задължително
WalletSolutionInfoPageQRCode	Код QR с информация за WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	незадължително
WalletVerifierToolURL*	URL адрес към инструмента за проверка на портфейл */.well-known/openid-credential-issuer* на крайната точка, използван за извличане на метаданните на доставчика на удостоверението.	URL	незадължително

([1]) Регламент за изпълнение (ЕС) 2025/849 на Комисията от 6 май 2025 г. за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на подаването на информация до Комисията и до групата за сътрудничество за списъка на сертифицираните европейски портфейли за цифрова самоличност (ОВ L, 2025/849, 7.5.2025 г., ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

ПРИЛОЖЕНИЕ X

Приложение II към Регламент за изпълнение (ЕС) 2024/2980 се изменя, както следва:

1) В приложение II, раздел 1 точка 1, буква и) се заменя със следното:

„i) едно или повече удостоверения, съобразени с ETSI EN 319 412-2 V2.4.1 (2025-06) или ETSI EN 319 412-3 V1.3.1 (2023-09), които може да се използват за проверка на подписа или печата, създаден от регистратора върху данните от регистъра и за които сертифицираните данни за самоличност включват името на регистратора и, когато е приложимо, регистрационния номер на регистратора, както е предвидено съответно в букви в) и г);“.

2) В приложение II, раздел 2 точка 1, буква з) се заменя със следното:

„з) едно или повече удостоверения, съобразени с ETSI EN 319 412-2 V2.4.1 (2025-06) или ETSI EN 319 412-3 V1.3.1 (2023-09), които може да се използват за удостоверяване на автентичността и валидността на удостоверения на портфейлен блок, издадени от доставчика на портфейл, и за които сертифицираните данни за самоличност включват наименованието и, когато е приложимо, регистрационния номер на доставчика на портфейла, както е предвидено съответно в буква а) и буква б);“.

3) В приложение II, раздел 3 точка 1, буква з) се заменя със следното:

„з) едно или повече удостоверения, съобразени с ETSI EN 319 412-2 V2.4.1 (2025-06) или ETSI EN 319 412-3 V1.3.1 (2023-09), които може да се използват за проверка на подписа или печата, създаден от доставчика на данни за идентификация на лица върху данните за идентификация на лица, които той предоставя, и за които сертифицираните данни за самоличност включват наименованието и, когато е приложимо, регистрационния номер на доставчика на данни за идентификация на лица, както е предвидено в буква а) и съответно в буква б).“

4) В приложение II, раздел 4 точка 1, буква ж) се заменя със следното:

„ж) едно или повече удостоверения, съобразени с ETSI EN 319 412-2 V2.4.1 (2025-06) или ETSI EN 319 412-3 V1.3.1 (2023-09), които може да се използват за проверка на подписа или печата, създадени от доставчика на удостоверенията за достъп на доверяваща се на портфейла страна относно удостоверението за достъп, което той предоставя на доверяващите се на портфейла страни, когато е приложимо, заедно с информацията, необходима за разграничаване на удостоверенията за достъп на доверяваща се на портфейла страна от други удостоверения.“

5) В приложение II се добавя раздел 5, както следва:

„5. Уведомления за информация относно доставчици на удостоверения за регистрация на доверяваща се на портфейл страна

1. Държавите членки предоставят на Комисията следната информация относно доставчиците на удостоверения за регистрация на доверяваща се на портфейл страна:

а) наименованието на доставчика на удостоверения за регистрация на доверяваща се на портфейл страна;

б) когато е приложимо, регистрационен номер на доставчика на удостоверения за регистрация на доверяваща се на портфейл страна;

в) държавата членка, в която е установен доставчикът на удостоверения за регистрация на доверяваща се на портфейл страна;

г) електронна поща и телефонен номер за контакт с доставчика на удостоверения за регистрация на доверяваща се на портфейл страна по въпроси, свързани с удостоверенията за регистрация, които той предоставя на доверяващите се на портфейл страни;

д) когато е приложимо, URL адрес на уебстраница на доставчика на удостоверения за регистрация на доверяваща се на портфейл страна, на която се съдържа допълнителна информация за доставчика и удостоверенията за регистрация, предоставяни от него на доверяващите се на портфейл страни;

е) URL адрес на уебстраница, на която се съдържат политиките, правилата и условията, които се прилагат по отношение на предоставянето и използването на удостоверения за регистрация, предоставяни на доверяващите се на портфейл страни;

ж) едно или повече удостоверения, съобразени с ETSI EN 319 412-2 V2.4.1 (2025-06) или ETSI EN 319 412-3 V1.3.1 (2023-09), които може да се използват за проверка на подписа или печата, създадени от доставчика на удостоверенията за регистрация на доверяваща се на портфейла страна относно удостоверението за регистрация, което той предоставя на доверяващите се на портфейл страни, когато е приложимо, заедно с информацията, необходима за разграничаване на удостоверенията за регистрация на доверяваща се на портфейл страна от други удостоверения.

2. Посочената в точка 1 информация се предоставя по доставчик на удостоверения за регистрация на доверяваща се на портфейл страна.“

ПРИЛОЖЕНИЕ XI

„ПРИЛОЖЕНИЕ I

Протоколи и интерфейси, посочени в член 4

Техническата спецификация ETSI TS 119 472-3 V1.1.1 (2026-03) се прилага със следните адаптации:

1) 4.1 Общи изисквания

— GEN-REQ-4.1-05: празно

— БЕЛЕЖКА: празно

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet (Предоставяне на удостоверения за регистрация на доставчик на PID/EAA до европейски портфейл за цифрова самоличност (EUDI Wallet)

— ISS-MDATA-REG_CERT-4.2.3-04: Един от елементите на параметъра на масив issuer_info трябва да съдържа удостоверението за регистрация на доставчика на PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: празно

— ISS-MDATA-REG_CERT-4.2.3-08: празно

— ISS-MDATA-REG_CERT-4.2.3-09: празно

— ISS-MDATA-REG_CERT-4.2.3-10: празно

— ISS-MDATA-REG_CERT-4.2.3-11: празно

— ISS-MDATA-REG_CERT-4.2.3-12: празно

— ISS-MDATA-REG_CERT-4.2.3-13: празно

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy (предварително определена политика за повторна употреба на PID/EAA в архитектурната и референтна рамка)

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Когато елементът id има стойност „arf_annex_ii“ и масивът, свързан с етикета „details“, съдържа стойност „once_only“ или „per-relying-party“, тогава обектът JSON, който съдържа този масив, свързан с етикета „details“, трябва да съдържа и номер JSON, свързан с етикета „reissue_trigger_unused“.

4) Приложение A не се прилага.“

ПРИЛОЖЕНИЕ XII

„ПРИЛОЖЕНИЕ II

Технически спецификации, посочени в член 5

Прилага се техническата спецификация от приложение B към ISO/IEC 18013-7:2025.

Техническите спецификации в точки 4.1, 4.2, 5 и 6 от ETSI TS 119 472-2 V1.2.1 (2026-03) се прилагат със следните адаптации, включително с вмъкването на нова точка 4.3:

1) 1 Scope (Обхват)

— В настоящия документ се определят два профила на протоколи, позволяващи на разчитащите на портфейл страни (по-нататък наричани „RP“) да пращат заявки за EAAP или данни за идентификация на лица (по-нататък наричани „PID“) до EUDI Wallet и той да изпраща заявките за EAAP/PID на RP. Всеки от профилите поддържа два механизма за предаване, а именно: с посредничеството на API и без посредничеството на API, както е показано по-долу:

а) Профилът е изграден на основата на:

— ISO/IEC 18013-5 [10] само за механизъм за предаване без посредничество на API, и

— Приложение B към ISO/IEC 18013-7 [16] — за механизъм за предаване с посредничеството на API.

Този профил е наречен профил ISO/IEC-mdoc и е определен в точка 5 от настоящия документ.

б) Профилът е изграден на основата на:

OpenID4VC-HAIP [11] за механизми за предаване с посредничеството на API и без посредничеството на API, както следва:

— Раздели 5, 5.1, 5.3, 7 и 8 от [11] за предаване чрез Redirects или чрез механизъм за предаване, без посредничеството на API, и

— Раздели 5, 5.2, 5.3, 7 и 8 от [11] за механизъм за предаване, с посредничеството на API.

Този профил е наречен профил OpenID4VC-HAIP и е определен в точка 6 от настоящия документ.

2) 2.1 Normative references (Нормативни препратки)

— [15] ISO 639: 'Language code'.

— [16] ISO/IEC 18013-7:2025 „Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions“.

3) 4.1 EAAP implementation based on SD-JWT VC (използване на EAAP въз основа на SD-JWT VC)

— EAAP-SD-JWT VC-04: празно.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc (използване на EAAP въз основа на ISO/IEC-mdoc)

— EAAP-ISO/IEC-mdoc-01: празно.

— *Note2*: празно.

— EAAP-ISO/IEC-mdoc-02: празно.

5) 4.3 EAAP implementation with mediating API (използване на EAAP с посредничеството на API)

— EAAP-API-GEN-01: EUDI Wallet поддържа посредничество на API, който поддържа и двата протокола, определени в точка 5.2 от [11] и в приложение B от [16].

— *БЕЛЕЖКА*: Когато устройството, на което е инсталиран EUDI Wallet, не поддържа и двата протокола, това изискване не може да бъде изпълнено и води до несъответствие поради това, че съответните операционни системи и браузъри не притежават необходимите характеристики за оперативна съвместимост.

— EAAP-API-GEN-02: EUDI Wallet поддържа посредничество на API най-малко за видовете PID и EAA, регистрирани в каталога на схемите, както е определено в Регламент за изпълнение (ЕС) 2025/1569, и най-малко за всички формати, определени в приложение II към Регламент за изпълнение (ЕС) 2024/2979.

— *БЕЛЕЖКА* 1: Когато базовата операционна система, браузърът, посредническите API или всеки друг технически пласт извън контрола на EUDI Wallet ограничават, филтрират, предварително избират или по друг начин ограничават форматите на удостоверенията, както и видовете PID и EAA, регистрирани в каталога на схемите, това изискване не може да бъде изпълнено. Когато такова ограничение възпрепятства EUDI Wallet да поддържа регистриран вид или формат на удостоверение, произтичащото от това несъответствие се дължи на неспособността на тези базови операционни системи, браузъри, посредничещи API или други съответни технически слоеве да осигурят необходимите характеристики за оперативна съвместимост.

6) 4.4 Валидиране на доверяваща се на портфейл страна и проверки за чрезмерни искания

— WRP-VALIDATION-01: EUDI Wallet валидира полученото в искането удостоверение за регистрация на доверяваща се на портфейл страна, преди да представи за одобрение на ползвателя на портфейла всеки поискан PID или електронно удостоверение за атрибути.

— WRP-VALIDATION-02: Когато валидирането на удостоверение за регистрация на доверяваща се на портфейл страна е неуспешно, включително когато удостоверението е изтекло, отменено, не е издадено от валиден доверен доставчик на удостоверения за регистрация на доверяваща се на портфейл страна, повредено е или не може да бъде проверено чрез криптографски средства, EUDI Wallet предупреждава ползвателя на портфейла, че доверяващата се на портфейл страна не може да бъде валидирана, и не представя искането като успешно валидирано. Ползвателят на портфейла изрично одобрява искането на доверяващата се страна. Липсата на отговор или предварително отбелязаните с отметка полета не са достатъчни за изрично одобрение.

— WRP-VALIDATION-03: Доставчикът на портфейла определя, въз основа на своя анализ на риска и политиката си за сигурност, дали и при какви условия конкретни неуспешни проверки за валидиране могат да бъдат заобиколени от ползвателя на портфейла.

— WRP-OVERASKING-01: EUDI Wallet сравнява удостоверенията и атрибутите, поискани от доверяващата се на портфейл страна, с регистрираните удостоверения и атрибути в удостоверението за регистрация на доверяваща се на портфейл страна.

— WRP-OVERASKING-02: Когато доверяващата се на портфейл страна поиска PID или електронни удостоверения за атрибути или твърдения, които не са обхванати от удостоверението за регистрация на доверяваща се на портфейл страна, EUDI Wallet предупреждава недвусмислено ползвателя на портфейла преди всяко разкриване. В предупреждението се посочва, че доверяващата се на портфейл страна иска повече информация, отколкото е регистрирала. Ползвателят на портфейла изрично одобрява искането на доверяващата се страна. Липсата на отговор или предварително отбелязаните с отметка полета не са достатъчни за изрично одобрение.

— WRP-OVERASKING-03: Доставчикът на портфейл определя, въз основа на своя анализ на риска, политиката за сигурност и приложимото право, дали ползвателят на портфейла може да продължи въпреки това предупреждение, дали може да бъде разкрита само подгрупата от искани данни, обхванати от удостоверението за регистрация, или искането се отхвърля.

7) 5.1 Introduction (Въведение)

— В точка 5 и нейните подточки се определя профил на протокол, който позволява на дадена RP да подава заявки за EAAP или PID до EUDI Wallet, а на EUDI Wallet — да изпраща заявките за EAAP/PID до RP, като се използва или механизъм за предаване, без посредничеството на API, проектиран по ISO/IEC 18013-5 [10], или механизъм за предаване, с посредничеството на API, проектиран по приложение B към ISO/IEC 18013-7 [16] за предаване на структурите от данни, определени в ISO/IEC 18013-5 [10], подходящо пакетирани.

— Останалата част от точка 5 е организирана, както следва:

  — В точка 5.2 се определят изискванията за поддържане на профила и механизмите за предаване от страна на RP и EUDI Wallet;

  — В точка 5.3 се определят изисквания, които са специфични за механизма за предаване без посредничеството на API;

  — В точка 5.4 и нейните подточки се определят изисквания, които са специфични за механизма за предаване с посредничеството на API.

8) 5.2 Requirements on EUDI Wallet and RP support (Изисквания относно поддръжката от EUDI Wallet и RP)

— ISO/IEC 18013-SUPPORT-01: Доставчиците на портфейли, доставчиците на PID, доставчиците на удостоверителни услуги, доставчиците на портфейли и доверяващите се страни не поддържат извличане от сървъра, както е посочено в ISO/IEC 18013-5 [10], за заявки и представяне на PID или атрибути на удостоверения.

— ISO/IEC 18013-SUPPORT-02: EUDI Wallet трябва да отговаря на изискванията, определени в точки 5.3 и 5.4 от настоящия документ.

— ISO/IEC 18013-SUPPORT-04: RP следва да прилага профила, определен в точка 5.4 от настоящия документ.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents (Съдържание на заявките за EAAP по ISO/IEC-mdoc)

— ISO/IEC 18013-5-REQ-04: Заявките от устройства, изпращани до EUDI Wallet, трябва да съдържат двойката стойности на ключ „requestInfo“, посочена в точка 8.3.2.1.2.1 от [10]. Стойността на тази двойка трябва да бъде от типа RequestInfo.

— ISO/IEC 18013-5-REQ-05: Типът RequestInfo трябва да бъде съгласно определеното на CDDL по-долу.

```
RequestInfo = {

    'euWrprc': bstr ; съдържа удостоверение за регистрация (вж. изискванията по-долу)

}
```

— ISO/IEC 18013-5-REQ-06: Посоченият елемент requestInfo съдържа елемент с етикет „euWrprc“.

— ISO/IEC 18013-5-REQ-07: Стойността на „euWrprc“ трябва да бъде удостоверение за регистрация, кодирано по CBOR.

— ISO/IEC 18013-5-REQ-08: празно.

— *БЕЛЕЖКА 3*: празно.

— ISO/IEC 18013-5-REQ-09: празно.

— ISO/IEC 18013-5-REQ-10: празно.

— ISO/IEC 18013-5-REQ-11: празно.

10) 5.3.3 Профил на отговор за EAAP по ISO/IEC-mdoc

— Настоящата точка определя изискванията за вида съобщение DeviceResponse, което е общо за двата вида механизми за предаване (с и без посредничеството на API).

— *БЕЛЕЖКА 1*: Когато се използва механизъм без API, проектиран по ISO/IEC 18013-5 [10], отговорът на EAAP е точно инстанция на DeviceResponse, както е описано в настоящата точка. Когато се използва механизъм посредством API, проектиран по приложение B към ISO/IEC 18013-7 [16], инстанцията на DeviceRequest е пакетирана, както е посочено в приложение B към [16].

— ISO/IEC 18013-5-RESP-02: Доставчикът на данни за идентификация на лица и електронни удостоверения за атрибути не включва никакви елементи от данни в KeyAuthorizations map в MSO на данните за идентификация на лица и електронните удостоверения за атрибути, които издава, с изключение на елементи от данни, които се предоставят от доверяващата се на портфейл страна в трансакционните данни в заявката mdoc за подпис или печат от портфейлния блок, като се използва частният ключ на данните за идентификация на лица или електронните удостоверения за атрибути.

— *БЕЛЕЖКА 2*: Съответно портфейлните блокове не могат да представят никакви елементи от данни, подписани от устройство, на доверяващите се на портфейл страни, освен за подписването на данни, които доверяващата се на портфейла страна е предоставила, например в случаи на употреба за сигурно удостоверяване на автентичността на потребителя.

— *БЕЛЕЖКА 3*: ISO/IEC 18013-5: 2021 не уточнява как доверяващите се на портфейл страни могат да включат трансакционни данни в заявка mdoc. Включването на трансакционни данни в заявка mdoc се извършва с добавяне на технически спецификации.

— ISO/IEC 18013-5-RESP-03: Доставчиците на данни за идентификация на лица не позволяват на частния ключ на данните за идентификация на лица да подписва елементи от данни, предоставени от доверяващата се на портфейл страна в трансакционните данни в заявката mdoc.

11) 5.4 Requirements for API mediated mechanism (Изисквания за механизъм с посредничеството на API)

5.4.1 ISO/IEC 18013-7-related requirements (Изисквания, свързани с ISO/IEC 18013-7)

Настоящата точка определя изискванията за механизма за предаване с посредничеството на API, във връзка с изискванията, определени в приложение B към [16].

— ISO/IEC 18013-7-API-01: Профилът, който поддържа представяния с посредничеството на API, трябва да отговаря на изискванията в приложение B към ISO/IEC 18013-7 [16], както е описано подробно в точки 5.3 и 5.4 от настоящия документ.

— ISO/IEC 18013-7-API-02: Всички задължителни изисквания в приложение B към [16] се прилагат, както е описано подробно в точки 5.3 и 5.4 от настоящия документ.

— ISO/IEC 18013-7-API-03: Всички незадължителни изисквания в приложение B към [16] остават незадължителни, освен ако е посочено друго в настоящия документ.

12) 5.4.2 Additional requirements (Допълнителни изисквания)

— В настоящата точка се определят допълнителни изисквания за механизма за предаване с посредничеството на API.

— ISO/IEC 18013-ADD-API-01: EUDI Wallet по подразбиране разкрива наличието на всички видове съхранявани електронни удостоверения за атрибути на междинния API, който функционира в съответствие с приложение B към [16], но не разкрива атрибутите и техните стойности в тези електронни удостоверения за атрибути.

— *БЕЛЕЖКА 1*: Ограничението за стойността на атрибутите се прилага дори ако оповестяването ѝ би подобрило услугите, предоставяни от операционната система на EUDI Wallet, например при подбора на удостоверения в контекста на случаите с посредничещ API.

— Съществуват съображения, свързани с операционните системи и браузърите извън контрола на внедрителите, които могат да бъдат взети предвид, както е посочено в бележки 2-4 по-долу:

— *БЕЛЕЖКА 2*: Заявка за представяне от доверяваща се страна, поддържаща приложение B към [16], може да се обработва от браузъра и/или операционната система за търсене на налични EAA, за предотвратяване на измами на потребителя или за целите на отстраняване на неизправности.

— *БЕЛЕЖКА 3*: Заявка за представяне от доверяваща се страна, поддържаща приложение B към [16], се очаква да се обработва от браузъра и/или операционната система за целите на сигурността на потребителите.

— *БЕЛЕЖКА 4*: Заявка за представяне от доверяваща се страна, поддържаща приложение B към [16], се очаква да не се обработва от браузъра и/или операционната система за целите на пазарния анализ (включително като вторична цел) или за вътрешни цели на браузъра и/или операционната система.

— ISO/IEC 18013-ADD-API-02: Когато EUDI Wallet изтрие по искане на потребител PID или EAA, споделени преди това с посредничещия API, който функционира в съответствие с приложение B към [16], EUDI Wallet споделя с посредничещия API, че вече не съхранява този PID или EAA.

— ISO/IEC 18013-ADD-API-03: Ако потребителят деинсталира своя EUDI Wallet, въпросният портфейл оповестява, че вече не съхранява никакви PID или EAA, споделени по-рано с посредничещия API, който функционира в съответствие с приложение B към [16].

— ISO/IEC 18013-ADD-API-04: EUDI Wallet предоставя глобална потребителска настройка за блокиране на споделянето на съхранявани EAA чрез посредничещ API, който функционира, както е посочено в ISO/IEC 18013-ADD-API-01. Когато тази настройка е деактивирана, EUDI Wallet не се обявява, нито отговаря на заявките за представяне или издаване с посредничеството на API.

— ISO/IEC 18013-ADD-API-05: EUDI Wallets проверяват при потоците между устройства, като използват посредничещ API, дали взаимодействащото устройство е в непосредствена физическа близост до EUDI Wallet, като използват сигурен, пряк и изискващ действие от ползвателя локален канал за обмен, като например безжична комуникационна технология с малък обсег на действие, за да извършат проверката за физическа близост.

— *БЕЛЕЖКА*: CTAP 2.3 позволява използването на BLE за извършване на проверка за непосредствена физическа близост и когато се прилага и от двете устройства, също така позволява пренос на данни между устройствата чрез технологии за предаване на данни с малък обсег на действие. Както проверката за физическа близост, така и прехвърлянето на данни между двете устройства се извършва по локален канал за обмен, както позволява CTAP 2.3, и следва да се предпочита от съответните операционни системи, браузъри, посредничещи API или всеки друг технически слой извън контрола на EUDI Wallet, пред използването на услугите на хибриден тунел за CTAP.

13) 6.2 Requirements on EUDI Wallet and RP support (Изисквания относно поддръжката от EUDI Wallet и RP)

— OIDFVP-HAIP-SUPPORT-02: EUDI Wallet трябва да отговаря на изискванията, посочени в точка 6.5 от настоящото приложение.

— OIDFVP-HAIP-SUPPORT-03: EUDI Wallet не следва да поддържа посочения в точка 6.4 механизъм, основан на пренасочване, за потоци за представяне на информация между устройства.

— *БЕЛЕЖКА 3*: Използването на този механизъм е уязвимо на атаки, като например фиксиране на сесията. Ограничаването на последствията от подобни атаки зависи от доверяващите се страни. Прилагането на този механизъм не следва да води до несъответствие.

— OIDFVP-HAIP-SUPPORT-05: РПС трябва да отговаря на изискванията, посочени в точка 6.5 от настоящото приложение.

— *БЕЛЕЖКА 5*: празно.

14) 6.3.1. Общи изисквания

— OIDFVP-HAIP-GEN-01: Прилагат се всички задължителни изисквания, посочени в точки 5, 5.3, 7 и 8 от HAIP [11].

— *БЕЛЕЖКА 1*: „HAIP [11] Раздел 5“ се отнася само до изискванията, посочени директно под заглавието на раздел 5. Това не включва раздели 5.1, 5.2 и 5.3.

— OIDFVP-HAIP-GEN-03: Ако настоящото приложение изменя изискване в OpenID4VC-HAIP [11], измененото изискване, посочено в настоящото приложение, има предимство.

— *БЕЛЕЖКА 2*: Това ще позволи например да се преобразува в задължително незадължително изискване от OpenID4VC-HAIP [11] или да се разширят задължителните изисквания.

— OIDFVP-HAIP-GEN-04: Когато форматът на исканото удостоверение отговаря на [10], РПС и EUDI Wallets трябва да отговарят на профила „ISO mdocs“ в [11], раздел 6.

— *БЕЛЕЖКА 3*: За яснота: Профилът „ISO mdocs“ в HAIP предполага, че РПС и EUDI Wallets трябва да отговарят на приложимите изисквания в [7], приложение Б.2.

— OIDFVP-HAIP-GEN-05: Когато форматът на исканото удостоверение отговаря на [2] РПС и EUDI Wallets трябва да отговарят на профила „IETF SD-JWT VCs“ в [11], раздел 6.

— *БЕЛЕЖКА 4*: За яснота: Профилът „IETF SD-JWT VCs“ предполага, че РПС и EUDI Wallets трябва да отговарят на изискванията в [7], приложение Б.3, както и на изискванията в [11], раздел 6.1.

15) 6.3.2.1 General requirements (Общи изисквания)

— OIDFVP-HAIP-COMMON-REQ-01: празно.

16) 6.3.2.2 Requirements for the Request Object (Изисквания за обекта на искането)

— OIDFVP-HAIP-COMMON-REQ-RO-02: празно

— OIDFVP-HAIP-COMMON-REQ-RO-03: празно

— OIDFVP-HAIP-COMMON-REQ-RO-04: празно

— OIDFVP-HAIP-COMMON-REQ-RO-05: празно

— OIDFVP-HAIP-COMMON-REQ-RO-06: празно.

— OIDFVP-HAIP-COMMON-REQ-RO-07: празно

— OIDFVP-HAIP-COMMON-REQ-RO-08: празно

— OIDFVP-HAIP-COMMON-REQ-RO-09: празно

— OIDFVP-HAIP-COMMON-REQ-RO-10: празно

— OIDFVP-HAIP-COMMON-REQ-RO-11: празно

— OIDFVP-HAIP-COMMON-REQ-RO-12: празно

— *Бележка 2*: празно

— OIDFVP-HAIP-COMMON-REQ-RO-13: Един от елементите на параметъра verifier_info трябва да включва удостоверението за регистрация.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Сертификатът на лист, посочен в OpenID4VP, раздел 5.9.3, който се използва с x509_hash Client Identifier Prefix, е сертификат за достъп на RP, както е посочено в ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile (профил на отговора на заявка за упълномощаване (отговор EAAP)

— OIDFVP-HAIP-COMMON-RESP-01: празно.

18) 6.4.1 General requirements (Общи изисквания)

— OIDFVP-HAIP-REDIRECTS-04: празно.

— *БЕЛЕЖКА*: празно.

19) 6.5.2 Additional requirements (Допълнителни изисквания)

— OIDFVP-HAIP-ADD-API-01: EUDI Wallet по подразбиране разкрива наличието на всички съхранявани видове EAA на междинния API, който функционира в съответствие с точка 5.2 от [11], но не разкрива атрибутите и техните стойности в тези EAA.

— OIDFVP-HAIP-ADD-API-04: Ако EUDI Wallet поддържа посредничещ API, който функционира, както е посочено в OIDFVP-HAIP-ADD-API-01, той трябва да осигури глобална потребителска настройка за блокиране на споделянето на съхранявани EAA чрез посредничещия API. Когато тази настройка е деактивирала споделянето, EUDI Wallet следва впоследствие да позволява на потребителя да избере отделни удостоверения, които да бъдат споделяни с посредничещия API.

— OIDFVP-HAIP-ADD-API-05: EUDI Wallets проверяват при потоците между устройства, като използват посредничещ API, дали взаимодействащото устройство е в непосредствена физическа близост до EUDI Wallet, като използват сигурен, пряк и опосредстван от ползвателя локален канал за обмен, като например безжична комуникационна технология с малък обсег на действие, за да извършат проверката за физическа близост.

— *БЕЛЕЖКА 5*: CTAP 2.3 позволява използването на BLE за извършване на проверка за непосредствена физическа близост и когато се прилага и от двете устройства, също така позволява пренос на данни между устройствата чрез технологии за предаване на данни с малък обсег на действие. Както проверката за физическа близост, така и прехвърлянето на данни между двете устройства се извършва по локален канал за обмен, както позволява CTAP 2.3, и следва да се предпочита от съответните операционни системи, браузъри, посредничещи API или всеки друг технически слой извън контрола на EUDI Wallet, пред използването на услугите на хибриден тунел за CTAP.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP (Специфични изисквания при поискване на EAAP по ISO/IEC 18013-5)

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Всички изисквания, посочени в настоящия документ, приложими към структури за заявки на устройства и отговори на устройства, посочени в ISO/IEC 18013-5, се прилагат и когато EUDI Wallet получи заявка за представяне по ISO/IEC mdoc чрез механизъм за предаване, подпомогнат от API, посочен в точка B.1 от [16].“