2024/2979

4.12.2024 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2024/2979 НА КОМИСИЯТА

от 28 ноември 2024 година

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

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) Европейската рамка за цифрова самоличност, създадена с Регламент (ЕС) № 910/2014, е ключов компонент в изграждането на сигурна и оперативно съвместима екосистема на цифровата самоличност в Съюза. Тъй като европейските портфейли за цифрова самоличност („портфейли“) са крайъгълният камък на рамката, нейната цел е да се улесни достъпът до услуги в държавите членки за физически и юридически лица, като същевременно се гарантира защитата на личните данни и неприкосновеността на личния живот.

(2) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([2]) и, когато е целесъобразно, Директива 2002/58/ЕО на Европейския парламент и на Съвета ([3]) се прилагат по отношение на всички дейности по обработване на лични данни съгласно настоящия регламент.

(3) С член 5а, параграф 23 от Регламент (ЕС) № 910/2014 на Комисията се възлага, когато е необходимо, да установи съответните спецификации и процедури. Това се постига чрез четири регламента за изпълнение, отнасящи се до протоколите и интерфейсите: Регламент за изпълнение (ЕС) 2024/2982 на Комисията ([4]), целостта и основните функции: Регламент за изпълнение (ЕС) 2024/2979 на Комисията ([5]), данните за идентификация на лица и електронното удостоверение за атрибути: Регламент за изпълнение (ЕС) 2024/2977 на Комисията ([6]), както и уведомленията до Комисията: Регламент за изпълнение (ЕС) 2024/2980 на Комисията ([7]). С настоящия регламент се определят съответните изисквания за целостта и основните функции на европейските портфейли за цифрова самоличност.

([1]) ОВ L 257, 28.8.2014 г., стр. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj.)

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

(4) Комисията редовно оценява нови технологии, практики, стандарти или технически спецификации. С цел да се осигури най-високо равнище на хармонизация между държавите членки за разработването и сертифицирането на портфейлите, определените в настоящия регламент технически спецификации се основават на работата, извършена въз основа на Препоръка (ЕС) 2021/946 на Комисията от 3 юни 2021 г. относно общ инструментариум на Съюза за координиран подход към европейска рамка за цифрова самоличност ([8]), и по-специално рамката за техническа архитектура и технически справки. В съответствие със съображение 75 от Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета ([9]) Комисията следва да преразглежда и при необходимост да актуализира настоящия регламент за изпълнение, за да бъде в съответствие с глобалното развитие, рамката за техническа архитектура и технически справки и да следва най-добрите практики на вътрешния пазар.

(5) За да се гарантира точна комуникация, техническа диференциация и ясно разпределение на отговорностите, е необходимо да се направи разграничение между различните компоненти и конфигурации на портфейлите. Технологично решение за портфейл следва да се разбира като пълната система, предоставена от доставчик на портфейл, която е необходима за експлоатацията на портфейл. Това следва да включва софтуерните и хардуерните компоненти, както и услугите, настройките и конфигурациите, необходими за осигуряване на правилното функциониране на портфейла. Технологичното решение за портфейла може да бъде разположено на устройствата и средата на ползвателите и на бекенд структурата на доставчика. Портфейлен блок следва да се разбира като специфична конфигурация на технологичното решение за портфейла за отделен ползвател. Той следва да включва приложението, инсталирано на устройството или средата на ползвателя на портфейла, с които той взаимодейства пряко („инстанцията на портфейла“), и необходимите защитни елементи за защитата на данните и трансакциите на ползвателя. Тези защитни елементи следва да включват специален софтуер или хардуер за криптиране и защита на чувствителна информация. Инстанцията на портфейла следва да бъде част от портфейлния блок и да позволява на ползвателя на портфейла да получи достъп до функциите на своя портфейл.

(6) В качеството си на отделни специализирани компоненти в рамките на портфейлен блок защитените криптографски приложения на портфейла са необходими не само за защита на стратегически активи, като криптографски частни ключове, но също така и за предоставяне на съществени функции, като представяне на електронни удостоверения за атрибути. Използването на общи технически спецификации може да улесни достъпа на доставчиците на портфейли до вградени защитени елементи. Защитените криптографски приложения на портфейла могат да бъдат предоставени по различни начини и за различни видове защитени криптографски устройства на портфейла. Когато доставчиците на портфейли предоставят персонализирани защитени криптографски приложения като аплети на Java Card за вградени защитени елементи, доставчиците на портфейли следва да спазват стандартите, изброени в приложение I, или еквивалентни технически спецификации.

(7) Портфейлните блокове трябва да предоставят възможност на доставчиците на данни за идентификация на лица или електронни удостоверения за атрибути да потвърдят, че издават тези данни или удостоверения по отношение на действителни портфейлни блокове на ползвателя на портфейла.

(8) С цел да се осигури защита на данните на етапа на проектирането и по подразбиране, портфейлите следва да разполагат с най-съвременните налични техники за подобряване на неприкосновеността на личния живот. Тези функции следва да предоставят възможност портфейлите да се използват, без ползвателят на портфейла да може да бъде проследен между различни доверяващи се на портфейла страни, ако това е приложимо при сценария на използване. Например доставчиците на портфейли следва да вземат предвид най-съвременните мерки за смекчаване относно неприкосновеността на личния живот във връзка с удостоверенията за портфейлни блокове, като например използване на временни удостоверения за портфейлни блокове или издаване по партиди. Освен това включените политики за оповестяване следва да предупреждават ползвателите на портфейла за неподходящо или незаконно оповестяване на атрибути от електронни удостоверения за атрибути.

(9) Удостоверенията за портфейлни блокове следва да предоставят възможност на доверяващите се на портфейла страни, които изискват атрибути от портфейлни блокове, да проверят състоянието на валидност на портфейлния блок, с който се свързват, тъй като удостоверенията за портфейлни блокове трябва да бъдат отменени, когато даден портфейлен блок вече не се счита за валиден. Информацията относно състоянието на валидност на портфейлните блокове следва да бъде предоставена по оперативно съвместим начин, за да се гарантира, че може да се използва от всички доверяващи се на портфейла страни. Освен това в случаите, когато ползвателите на портфейла са загубили своите портфейлни блокове или вече не могат да ги управляват, доставчиците на портфейли следва да позволят на ползвателите на портфейла да поискат отмяната на техния портфейлен блок. За да се гарантира неприкосновеността на личния живот и липсата на свързаност, държавите членки следва да използват техники за запазване на неприкосновеността на личния живот и за удостоверението за портфейлен блок. Това може да включва използването на множество удостоверения за портфейлен блок за различни цели, като се разкрива само минималната относима информация за портфейла, необходима за дадена трансакция, или за ограничаване на жизнения цикъл на удостоверението за портфейлен блок като алтернатива на използването на идентификатори за отмяна.

([8]) OB L 210, 14.6.2021 г., стр. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност (OB L, 2024/1183, 30.4.2024 г., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) За да се гарантира, че при всички портфейли е налице техническа възможност за получаване и представяне на данни за идентификация на лица и електронни удостоверения за атрибути при трансгранични сценарии, без да се нарушава оперативната съвместимост, портфейлите следва да поддържат предварително определени видове формати на данни и избирателно разкриване. Както е посочено в Регламент (ЕС) № 910/2014, избирателното разкриване е понятие, съгласно което собственика на данни има право да разкрива само определени части от по-голям набор от данни, за да може получаващият субект да получи само информацията, която е необходима за предоставянето на услуга, поискана от ползвател. Тъй като портфейлите трябва да позволяват на ползвателя избирателно да разкрива атрибути, стандартите, изброени в приложение II, следва да се прилагат по начин, който позволява тази характеристика на портфейлите. Освен това с цел да се улеснят специфични случаи на употреба портфейлите може да поддържат други формати и функции.

(11) Регистрирането на трансакции е важен инструмент за осигуряване на прозрачност под формата на предоставяне на преглед на трансакциите на ползвателя на портфейла. Освен това в случай на подозрително поведение от страна на доверяващи се на портфейла страни следва да се използват регистрационни файлове с цел да се даде възможност за бързо и лесно споделяне, по искане на ползвателя на портфейла, на определена информация с компетентните надзорни органи, създадени съгласно член 51 от Регламент (ЕС) 2016/679.

(12) За да може ползвателят на портфейла да се подписва електронно, следва да му бъде издадено квалифицирано удостоверение, което е обвързано с устройство за създаване на квалифициран електронен подпис. Ползвателят на портфейла следва да има достъп до приложение за създаване на подпис. Докато издаването на квалифицирани удостоверения е услуга на доставчици на квалифицирани доверителни услуги, то доставчиците на портфейли или други субекти следва да могат да предоставят останалите компоненти. Например устройствата за създаване на квалифициран електронен подпис може да се управляват от доставчици на квалифицирани доверителни услуги като услуга или могат да бъдат налични локално на устройството на ползвателя на портфейла, например като карта с чип. По подобен начин приложенията за създаване на подпис може да бъдат интегрирани в инстанцията на портфейла, да бъдат отделно приложение на устройството на ползвателя на портфейла или да се предоставят от разстояние.

(13) С обектите за експортиране на данни и преносимост може да се регистрират данните за идентификация на лица и електронните удостоверения за атрибути, които са били издадени за определен портфейлен блок. Тези обекти позволяват на ползвателите на портфейла да извличат съответните данни от своя портфейл, за да утвърдят правото си на преносимост на данните. Доставчиците на портфейли се насърчават да използват едни и същи технически решения, за да прилагат процеси за архивиране и възстановяване на портфейли, което прави възможно възстановяването на изгубени портфейли или прехвърляне на информация от един доставчик на портфейл към друг, когато е подходящо и доколкото това може да се извърши, без да се нарушава правото на защита на данните и сигурността на екосистемата на цифровата самоличност.

(14) Генерирането на специфични псевдоними за доверяващата се на портфейла страна следва да позволи на ползвателите на портфейла да удостоверят автентичността си, без да предоставят ненужна информация на доверяващите се на портфейла страни. Както е посочено в Регламент (ЕС) № 910/2014, ползвателите на портфейли не трябва да бъдат възпрепятствани да имат достъп до услуги под псевдоним, когато няма правно изискване за юридическа самоличност за удостоверяване на автентичността. Поради това портфейлите трябва да включват функционалност за генериране на избрани от ползвателите и управлявани псевдоними за удостоверяване на автентичността при достъп до онлайн услуги. Прилагането на спецификациите, посочени в приложение V, следва съответно да позволи тези функции. Освен това доверяващите се на портфейла страни не трябва да изискват от ползвателите да предоставят каквито и да било данни, различни от посочените за предвидената употреба на портфейлите в регистъра на доверяващата се страна. Ползвателите на портфейла следва да имат възможност да проверяват по всяко време данните за регистрация на доверяващите се страни.

(15) Както е посочено в Регламент (ЕС) 2024/1183 държавите членки не трябва пряко или косвено да ограничават достъпа до публични или частни услуги за физически или юридически лица, които не избират да използват портфейли, и следва да предоставят подходящи алтернативни решения.

(16) 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 ([10]) и той прие своето становище на 30 септември 2024 г.

([10]) 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).

(17) Предвидените в настоящия регламент мерки са в съответствие със становището на комитета, посочен в член 48 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и приложно поле

С настоящия регламент се установяват правилата за целостта и основните функции на портфейлите, които трябва редовното да се актуализират, за да бъдат в съответствие с развитието на технологиите и стандартите и с работата, извършена въз основа на Препоръка (ЕС) 2021/946 на Комисията, и по-специално рамката за техническа архитектура и технически справки.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „защитено криптографско приложение на портфейла“ означава приложение, с което се управляват стратегически активи чрез свързване с и използване на криптографските и некриптографските функции, предоставяни от защитеното криптографско устройство на портфейла;

2) „портфейлен блок“ означава уникална конфигурация за технологично решение за портфейл, включваща инстанции на портфейла, защитени криптографски приложения на портфейла и защитени криптографски устройства на портфейла, предоставени от доставчик на портфейла на индивидуален ползвател на портфейла;

3) „стратегически активи“ означава активи в рамките на или във връзка с портфейлен блок от такова изключително значение, че тяхното извеждане от строя или унищожаване би имало много сериозен, отслабващ ефект върху способността да се разчита на портфейлния блок;

4) „доставчик на данни за идентификация на лица“ означава физическо или юридическо лице, отговорно за издаването и отмяната на данните за идентификация на лица и гарантирането, че данните за идентификация на лице на ползвателя са свързани криптографски с портфейла;

5) „ползвател на портфейла“ означава ползвател, който управлява портфейлния блок;

6) „доверяваща се на портфейла страна“ означава доверяваща се страна, която възнамерява да разчита на портфейлни блокове за предоставянето на публични или частни услуги чрез цифрово взаимодействие;

7) „доставчик на портфейл“ означава физическо или юридическо лице, което предоставя технологични решения за портфейла;

8) „удостоверение за портфейлен блок“ означава обект на данни, който описва компонентите на портфейла или позволява удостоверяване на автентичността и валидиране на тези компоненти;

9) „включени политики за оповестяване“ означава набор от правила, включени в електронно удостоверение за атрибути от неговия доставчик, посочващи условията, които доверяващата се на портфейла страна трябва да изпълни, за да получи достъп до електронното удостоверение за атрибути;

10) „инстанция на портфейла“ означава приложението, инсталирано и конфигурирано на устройството или средата на ползвателя на портфейла, което е част от портфейлния блок и което ползвателят на портфейла използва за взаимодействие с портфейлния блок;

11) „технологично решение за портфейл“ означава съчетание от софтуер, хардуер, услуги, настройки и конфигурации, включително инстанции на портфейла, едно или повече защитени криптографски приложения на портфейла и едно или повече защитени криптографски устройства на портфейла;

12) „защитено криптографско устройство на портфейла“ означава устойчиво на опити за подправяне устройство, осигуряващо среда, която е свързана с и използвана от защитеното криптографско приложение на портфейла за защита на стратегически активи и предоставяне на криптографски функции за сигурно изпълнение на операции от критично значение;

13) „криптографска операция с портфейла“ означава криптографски механизъм, необходим в контекста на удостоверяването на автентичността на ползвателя на портфейла и издаването или представянето на данни за идентификация на лица или електронни удостоверения за атрибути;

14) „удостоверение за достъп на доверяваща се на портфейла страна“ означава удостоверение за електронни печати или подписи за удостоверяване на автентичността и валидиране на доверяваща се на портфейла страна, издадено от доставчик на удостоверения за достъп на доверяваща се на портфейла страна;

15) „доставчик на удостоверения за достъп на доверяваща се на портфейла страна“ означава физическо или юридическо лице, на което е възложено от държава членка да издава удостоверения за достъп на доверяваща се страна на регистрирани във въпросната държава членка доверяващи се на портфейла страни.

ГЛАВА II

ЦЯЛОСТ НА ЕВРОПЕЙСКИТЕ ПОРТФЕЙЛИ ЗА ЦИФРОВА САМОЛИЧНОСТ

Член 3

Цялост на портфейлния блок

1. Докато с портфейлния блок не се удостовери успешно автентичността на ползвателя на портфейла, портфейлните блокове не изпълняват функциите, изброени в член 5а, параграф 4 от Регламент (ЕС) № 910/2014, с изключение на удостоверяването на автентичността на ползвателя на портфейла за достъп до портфейлния блок.

2. Доставчиците на портфейли подписват или подпечатват за всеки портфейлен блок поне едно удостоверение за портфейлен блок, което отговаря на посочените в член 6 изисквания. Удостоверението, използвано за подписване или подпечатване на удостоверението за портфейлния блок, се издава под формата на удостоверение, посочено в доверителния списък, изложен в Регламент за изпълнение (ЕС) 2024/2980.

Член 4

Инстанции на портфейла

1. Инстанциите на портфейла използват поне едно защитено криптографско устройство на портфейла, за да управляват стратегически активи.

2. Доставчиците на портфейли гарантират целостта, автентичността и поверителността на комуникацията между инстанциите на портфейла и защитените криптографски приложения на портфейла.

3. Когато стратегическите активи са свързани с извършване на електронна идентификация на ниво на осигуреност „високо“, криптографските операции с портфейла или други операции, при които се обработват стратегически активи, се извършват в съответствие с изискванията за характеристиките и проекта на средствата за електронна идентификация на ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502 на Комисията ([11]).

Член 5

Защитени криптографски приложения на портфейла

1. Доставчиците на портфейли гарантират, че защитените криптографски приложения на портфейла:

а) извършват криптографски операции по портфейла, включващи критични активи, различни от необходимите за удостоверяване на автентичността на ползвателя на портфейла, само в случаите, когато тези приложения са удостоверили успешно автентичността на ползвателите на портфейла;

([11]) Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 г. за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (ОВ L 235, 9.9.2015 г., стр. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

б) когато удостоверяват автентичността на ползвателите на портфейла в контекста на извършване на електронна идентификация на ниво на осигуреност „високо“, извършват удостоверяване на автентичността на ползвателите на портфейла в съответствие с изискванията за характеристиките и проекта на средствата за електронна идентификация на ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502;

в) са в състояние да генерират сигурно нови криптографски ключове;

г) са в състояние да изтриват сигурно стратегически активи;

д) са в състояние да генерират доказателство за притежание на частни ключове;

е) защитават личните ключове, генерирани от тези защитени криптографски приложения на портфейла, по време на съществуването на ключовете;

ж) са в съответствие с изискванията за характеристиките и проекта на средствата за електронна идентификация на ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502;

з) са единствените компоненти, способни да изпълняват криптографски операции с портфейла и всякакви други операции със стратегически активи в контекста на извършване на електронна идентификация на ниво на осигуреност „високо“.

2. Когато доставчиците на портфейли решат да предоставят защитено криптографско приложение на портфейл на вграден защитен елемент, тези доставчици на портфейли основават техническото си решение на техническите спецификации, изброени в приложение I, или на други еквивалентни технически спецификации.

Член 6

Автентичност и валидност на портфейлния блок

1. Доставчиците на портфейли гарантират, че всеки портфейлен блок съдържа удостоверения за портфейлен блок.

2. Доставчиците на портфейли гарантират, че посочените в параграф 1 удостоверения за портфейлен блок съдържат публични ключове и че съответните частни ключове са защитени чрез защитено криптографско устройство на портфейла.

3. Доставчиците на портфейли:

а) информират ползвателите на портфейла за техните права и задължения във връзка с техния портфейл;

б) предоставят механизми, независими от портфейлните блокове, за сигурна идентификация и удостоверяване на автентичността на ползвателите на портфейла;

в) гарантират, че ползвателите на портфейла имат право да поискат отмяна на техните удостоверения за портфейлен блок, като използват посочените в буква б) механизми за удостоверяване на автентичността.

Член 7

Отмяна на удостоверения за портфейлен блок

1. Доставчиците на портфейли са единствените субекти, способни да отменят удостоверенията за портфейлен блок, които те са предоставили.

2. Доставчиците на портфейли установяват публично достъпна политика, с която се определят условията и времевата рамка за отмяна на удостоверенията за портфейлен блок.

3. Когато доставчиците на портфейл са отменили удостоверенията за портфейлен блок, те информират засегнатите ползватели на портфейла в срок от 24 часа след отмяната на портфейла, включително причината за отмяната и последиците за ползвателя на портфейла. Тази информация се предоставя по кратък и лесно достъпен начина, като се използва ясен и понятен език.

4. Когато доставчиците на портфейли са отменили удостоверенията за портфейлен блок, те правят статуса на валидност на удостоверението за портфейлен блок публично достъпен, като запазват поверителността и описват местоположението на тази информация в удостоверението за портфейлен блок.

ГЛАВА III

ОСНОВНИ ФУНКЦИИ И ХАРАКТЕРИСТИКИ НА ЕВРОПЕЙСКИТЕ ПОРТФЕЙЛИ ЗА ЦИФРОВА САМОЛИЧНОСТ

Член 8

Формати за данните за идентификация на лица и електронните удостоверения за атрибути

Доставчиците на портфейли гарантират, че технологичните решения за портфейл поддържат използването на данни за идентификация на лица и електронни удостоверения за атрибути, издадени в съответствие със списъка от стандарти, посочен в приложение II.

Член 9

Регистрационни файлове за трансакциите

1. Независимо от това дали дадена трансакция е изпълнена успешно или не, инстанциите на портфейла ще регистрират всички трансакции с доверяващи се на портфейла страни и други портфейлни блокове, включително електронно подписване и подпечатване.

2. Записаната информация съдържа най-малко:

а) времето и датата на трансакцията;

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, или в случай на други портфейлни блокове — подходяща информация от удостоверението за портфейлен блок;

в) вида или видовете данни, поискани и представени при изпълнение на трансакцията;

г) в случай на неизпълнени трансакции — причината за въпросното неизпълнение.

3. Доставчиците на портфейли гарантират целостта, автентичността и поверителността на регистрираната информация.

4. Инстанциите на портфейла регистрират отчети, изпратени от ползвателя на портфейла до органите за защита на данните чрез неговия портфейлен блок.

5. Посочените в параграфи 1 и 2 регистрационни файлове са достъпни за доставчика на портфейла, когато това е необходимо за предоставянето на услуги за портфейла, въз основа на изрично предварително съгласие от ползвателя на портфейла.

6. Посочените в параграфи 1 и 2 регистрационни файлове остават достъпни, докато се изискват от правото на Съюза или националното право.

7. Доставчиците на портфейли предоставят възможност на ползвателите на портфейла да експортират регистрираната информация, посочена в параграф 2.

Член 10

Включено оповестяване

1. Доставчиците на портфейли гарантират, че електронните удостоверения за атрибути с общи включени политики за оповестяване, посочени в приложение III, могат да бъдат обработени от портфейлните блокове, които предоставят.

2. Инстанциите на портфейла трябва да могат да обработват и представят такива включени политики за оповестяване, посочени в параграф 1, във връзка с данните, получени от доверяващата се на портфейла страна, която е отправила искането.

3. Инстанциите на портфейла проверят дали доверяващата се на портфейла страна спазва изискванията на включената политика за оповестяване на информация и информира ползвателя на портфейла за резултата.

Член 11

Квалифицирани електронни подписи и печати

1. Доставчиците на портфейли гарантират, че ползвателите на портфейла могат да получават квалифицирани удостоверения за квалифицирани електронни подписи или печати, свързани с устройства за създаване на квалифициран подпис или печат, които са локални, външни или дистанционно управлявани по отношение на инстанциите на портфейла.

2. Доставчиците на портфейли гарантират, че технологичните решения за портфейл са в състояние да взаимодействат сигурно с един от следните типове устройства за създаване на квалифициран подпис или печат: локални, външни или дистанционно управлявани устройства за създаване на квалифициран подпис или печат за целите на използването на квалифицираните удостоверения, посочени в параграф 1.

3. Доставчиците на портфейли гарантират, че ползвателите на портфейла, които са физически лица, притежават, поне за непрофесионални цели, безплатен достъп до приложения за създаване на подписи, позволяващи създаването на безплатни квалифицирани електронни подписи с помощта на посочените в параграф 1 удостоверения.

Член 12

Приложения за създаване на подпис

1. Използваните от портфейлните блокове приложения за създаване на подпис могат да бъдат предоставени от доставчици на портфейли, от доставчици на доверителни услуги или от доверяващи се на портфейла страни.

2. Приложенията за създаване на подпис имат следните функции:

а) подписване или подпечатване на предоставени от ползвателя данни за портфейла;

б) подписване или подпечатване на данни, предоставени от доверяваща се страна;

в) създаване на подписи или печати в съответствие най-малко със задължителните формати, посочени в приложение IV;

г) информиране на ползвателите на портфейла за резултата от процеса на създаване на подпис и печат.

3. Приложенията за създаване на подписи могат или да бъдат интегрирани в инстанции на портфейла, или да бъдат външни за тях. Когато приложенията за създаване на подписи разчитат на дистанционно управлявани устройства за създаване на квалифицирани подписи и когато са интегрирани в инстанции на портфейла, те поддържат програмния интерфейс на приложението, посочен в приложение IV.

Член 13

Експорт и преносимост на данни

Портфейлните блокове, когато е технически осъществимо и с изключение на случаи на стратегически активи, поддържат сигурно експортиране и преносимост на личните данни на ползвателя на портфейла с цел да му позволят да премине към портфейлен блок на различно технологично решение за портфейла, така че да се гарантира ниво на осигуреност „високо“, както е предвидено в Регламент за изпълнение (ЕС) 2015/1502.

Член 14

Псевдоними

1. Портфейлните блокове поддържат генерирането на псевдоними за ползвателите на портфейла в съответствие с техническите спецификации, посочени в приложение V.

2. Портфейлните блокове поддържат генерирането, по искане на доверяваща се на портфейла страна, на псевдоним, който е специфичен и уникален за тази доверяваща се на портфейла страна, и предоставят този псевдоним на доверяващата се на портфейла страна било то самостоятелно, или в комбинация с всякакви данни за идентификация на лица или електронно удостоверение за атрибут, поискани от въпросната доверяваща се на портфейла страна.

ГЛАВА IV

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 15

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 28 ноември 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

СПИСЪК НА СТАНДАРТИТЕ, ПОСОЧЕНИ В ЧЛЕН 5

— SAM.01 Secured Applications for Mobile - Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;

— GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;

— GPD_SPE_ 0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

ПРИЛОЖЕНИЕ II

СПИСЪК НА СТАНДАРТИТЕ, ПОСОЧЕНИ В ЧЛЕН 8

— ISO/IEC.18013-5:2021;

— „Модел на данни за проверими свидетелства 1.1“, Препоръка на W3C, 3 март 2022 г.

ПРИЛОЖЕНИЕ III

СПИСЪК НА ОБЩИТЕ ВКЛЮЧЕНИ ПОЛИТИКИ ЗА ОПОВЕСТЯВАНЕ, ПОСОЧЕНИ В ЧЛЕН 10

1. „Няма политика“, което показва, че не се прилага политика за електронните удостоверения на атрибути.
2. „Политика за оповестяване само на оправомощени доверяващи се страни“, указваща, че ползвателите на портфейли могат да оповестяват електронни удостоверения за атрибути само на доверяващи се страни с удостоверена автентичност, които са изрично изброени в политиките за оповестяване.
3. „Специфичен корен на доверието“, указващ, че ползвателите на портфейла следва да оповестяват специфичното електронно удостоверение за атрибути само на доверяващи се на портфейла страни с удостоверена автентичност с удостоверения за достъп на доверяващи се на портфейла страни, изведени от конкретен корен (или списък от конкретни корени) или междинно(и) удостоверение(я).

ПРИЛОЖЕНИЕ IV

ФОРМАТИ ЗА ПОДПИС И ПЕЧАТ, ПОСОЧЕНИ В ЧЛЕН 12

1. Задължителен формат на подпис или печат:

   а) PAdES (Усъвършенствани електронни подписи във формат PDF), както е посочено в ETSI EN 319 142-1 V1.1.1 (2016-04); Електронни подписи и инфраструктура (ESI); PAdES цифрови подписи; Част 1: Градивни елементи и базови PAdES подписи.

2. Списък на незадължителни формати за подпис или печат:

   а) XAdES, както е посочено в „ETSI EN 319 132-1 V1.2.1 (2022-02) Електронни подписи и инфраструктура (ESI); XAdES цифрови подписи; Част 1: Градивни елементи и базови XAdES подписи (XAdES)“ за подписване на XML формат;

   б) JAdES, както е посочено в „ETSI TS 119 182-1 V1.2.1 (2024-07) Електронни подписи и инфраструктура (ESI); JAdES цифрови подписи; Част 1: Градивни елементи и базови JAdES подписи“ за подписване на JSON формат;

   в) CAdES (Усъвършенствани електронни подписи във формат CMS), както е посочено в „ETSI EN 319 122-1 V1.3.1 (2023-06) Електронни подписи и инфраструктура (ESI); CAdES цифрови подписи; Част 1: Градивни елементи и базови CAdES подписи“ за подписване на CMS формат;

   г) ASiC (Свързан с подписа носител), както е посочено в „ETSI EN 319 162-1 V1.1.1 (2016-04) Електронни подписи и инфраструктура (ESI); Свързани с подписа носители (ASiC); Част 1: Градивни елементи и базови ASiC носители и ETSI EN 319 162-2 V1.1.1 (2016-04) Електронни подписи и инфраструктура (ESI); Свързани с подписа носители (ASiC); Част 2: Допълнителни ASiC носители за подписване на носители“.

3. Приложно-програмен интерфейс:

   — Спецификация на консорциум за подпис в облак (CSC) версия 2.0 (20 април 2023 г.).

ПРИЛОЖЕНИЕ V

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ГЕНЕРИРАНЕ НА ПСЕВДОНИМИ, ПОСОЧЕНИ В ЧЛЕН 14

Технически спецификации:

— WebAuthn — Препоръка на W3C, 8 април 2021 г., Ниво 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.