2024/2981

4.12.2024 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2024/2981 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 сертифицирането 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 5в, параграф 6 от него,

като има предвид, че:

(1) Съгласно член 5в от Регламент (ЕС) № 910/2014, сертифицирането на европейските портфейли за цифрова самоличност („портфейли“) трябва да се извършва в съответствие с изискванията за функционалност, киберсигурност и защита на данните, за да се гарантира високо ниво на сигурност и доверие в портфейлите. Тези изисквания за сертифициране трябва да бъдат хармонизирани във всички държави членки с оглед на предотвратяване на разпокъсаността на пазара и изграждането на надеждна рамка.

(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 дейностите по обработване на лични данни съгласно настоящия регламент.

(3) 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 ([4]), 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 ([5]) 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.

(4) За да се удостовери съответствие с включените в рамката за сертифициране изисквания за киберсигурност, сертифицирането на технологични решения за портфейл следва, когато е налично и значимо, да се отнася до европейските схеми за сертифициране на киберсигурността, създадени съгласно Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета ([6]). При липса на такива схеми или когато те частично покриват изискванията за киберсигурност, с настоящия регламент се определят общите изисквания, приложими по отношение на националните схеми за сертифициране, обхващащи функционалните изисквания, изискванията за киберсигурност и за защита на данните.

([1]) ОВ L 257, 28.8.2014 г., стр. 73, ELI: https://eur-lex.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]) ОВ L 210, 14.6.2021 г., стр. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

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

([6]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Съгласно член 5а, параграф 11 от Регламент (ЕС) № 910/2014 портфейлите трябва да бъдат сертифицирани за ниво на осигуреност „високо“, както е посочено в Регламент (ЕС) № 910/2014 и в Регламент за изпълнение (ЕС) 2015/1502 на Комисията ([7]). Това ниво на осигуреност трябва да бъде постигнато от цялостното технологично решение за портфейла. Съгласно посочения регламент някои компоненти на технологичното решение за портфейла може да бъдат сертифицирани на по-ниско ниво на осигуреност, при условие че това е надлежно обосновано и без да се засяга достигнато от цялостното решение ниво на осигуреност „високо“.

(6) Във всички национални схеми за сертифициране трябва да се определя собственик на схемата, който ще отговаря за разработването и поддържането на схемата за сертифициране. Собственикът на схемата може да бъде орган за оценка на съответствието, правителствен орган или структура, търговска асоциация, група органи за оценка на съответствието или всеки подходящ орган, като той може да бъде различен от органа, управляващ националната схема за сертифициране.

(7) Обектът на сертифициране следва да включва софтуерните компоненти на технологичното решение за портфейла, като например инстанцията на портфейла. Макар че защитеното криптографско устройство на портфейла (ЗКПП), защитеното криптографско устройство на портфейла (ЗКУП) и платформите, на които се прилагат тези софтуерни компоненти, са част от операционната среда, те следва да бъдат включени в обекта на сертифициране само когато се предоставят от технологичното решение за портфейла. В други случаи, и по-специално когато тези устройства и платформи се предоставят от крайни ползватели, доставчиците следва да установят допускания за операционната среда на технологичното решение за портфейла, включително на тези устройства и платформи, и да приложат мерки с цел да потвърдят, че тези допускания са проверени на практика. За да се осигури защита на стратегическите активи чрез хардуер и системен софтуер, използвани за управление и защита на криптографски ключове, създадени, съхранени или обработени от ЗКУП, ЗКУП трябва да отговаря на високи стандарти за сертифициране, както е отразено в международните стандарти, като например общите критерии (ЕССК), установени в Регламент за изпълнение (ЕС) 2024/482 на Комисията ([8]), оценката съгласно EAL4 и усъвършенствания методичен анализ на уязвимостта, равностоен на AVA_VAN.5. Тези стандарти за сертифициране следва да се използват най-късно, когато сертифицирането на съответствието на портфейлите се извършва съгласно приета в съответствие с Регламент (ЕС) 2019/881 европейска схема за сертифициране на киберсигурността.

(8) Напълно мобилните, сигурни и лесни за употреба портфейли се поддържат чрез наличието на стандартизирани и сертифицирани решения, устойчиви на опити за подправяне, като вградени защитени елементи, външни устройства, като например смарткарти, или вградени SIM платформи в мобилни устройства. Важно е да се осигури своевременен достъп до вградени защитени елементи за националните средства за електронна идентификация и портфейли и да се координират усилията на държавите членки в тази област. Поради това Европейската група за сътрудничество в областта на цифровата самоличност, създадена съгласно член 46д, параграф 1 от Регламент (ЕС) № 910/2014 („групата за сътрудничество“), следва да създаде специална подгрупа за тази цел. Като се консултира със съответните заинтересовани страни, тази подгрупа следва да постигне съгласие по съвместна пътна карта за достъп до вградени защитени елементи, която да бъде разгледана от Комисията във връзка с доклада за преглед на Регламент (ЕС) № 910/2014. За да се улесни използването на портфейла на национално равнище, Комисията следва освен това, в сътрудничество с държавите членки, да разработи и непрекъснато да актуализира наръчник за случаите на употреба като част от рамката за техническа архитектура и технически справки.

(9) Обектът на сертифициране на националните схеми за сертифициране следва също така да включва процесите, които се използват за предоставяне и управление на технологичното решение за портфейла, дори когато определянето или изпълнението на тези процеси е възложено на подизпълнители — трети лица. За да се докаже, че процесите отговарят на изискванията на схемите, е разрешено като доказателство да се използва информация във връзка с осигуреността, при условие че, за да се определи дали информацията във връзка с осигуреността е достатъчна, се използва анализ на зависимостта. Информацията във връзка с осигуреността се получава в много различни форми, включително доклади и сертификати за съответствие, които могат да бъдат частни, национални, европейски или международни, на основата на стандарти или технически спецификации. Целта на анализа на зависимостта е да се оцени качеството на наличната информация във връзка с осигуреността относно компонентите на портфейла.

([7]) 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).

([8]) Регламент за изпълнение (ЕС) 2024/482 на Комисията от 31 януари 2024 г. за определяне на правила за прилагането на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета по отношение на приемането на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) (ОВ L, 2024/482, 7.2.2024 г., ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Като следва установените за тази цел процедури, групата за сътрудничество следва да може да предоставя становища и препоръки относно представените ѝ проекти за национални схеми за сертифициране. Тези национални схеми за сертифициране следва да са специфични за архитектурата на портфейла и следва да имат специфични профили за всяка конкретна поддържана архитектура.

(11) За да се осигури общо разбиране и хармонизиран подход към оценката на най-големите рискове, които биха могли да повлияят върху предоставянето и работата на портфейлите, следва да се изготви регистър на рисковете и заплахите, които следва да бъдат взети под внимание при проектирането на технологични решения за портфейл, независимо от тяхната конкретна архитектура. Описаните в Регламент (ЕС) № 910/2014 цели на киберсигурността, като поверителността, целостта и наличността на технологично решение за портфейла, както и поверителността на ползвателите и данните, следва да се вземат предвид, когато се определят рискове, които следва да бъдат включени в регистъра. Надлежното отчитане на рисковете и заплахите, включените в посочения регистър на рисковете, следва да бъде част от изискванията на националните схеми за сертифициране. За да се бъде в съответствие с постоянно променящия се контекст на заплахите, регистърът на рисковете следва да се поддържа и редовно да се актуализира в сътрудничество с групата за сътрудничество.

(12) Когато създават своите схеми за сертифициране, собствениците на схеми следва да извършат оценка на риска, за да прецизират и допълнят посочените в регистър рискове и заплахи с такива, които са специфични за архитектурата или изпълнението на технологичното решение за портфейла. При оценката на риска следва да се обмисли как приложимите рискове и заплахи могат да бъдат разгледани по подходящ начин. Доставчиците на портфейли следва да допълнят оценката на риска на схемата, за да установят всички рискове и заплахи, специфични за тяхното прилагане, и да предложат подходящи мерки за обработка във връзка с оценката от страна на сертифициращия орган.

(13) За да се демонстрира, че архитектурата на технологично решение за портфейла отговаря на приложимите изисквания за сигурност, всяка специфична за архитектурата схема или профил следва да съдържа най-малко описание на архитектурата на технологичното решение за портфейла, списък на изискванията за сигурност, приложими по отношение на архитектурата на технологичното решение за портфейла, план за оценка, с който да се потвърди, че основано на тази архитектура технологично решение за портфейла отговаря на тези изисквания и оценка на риска. Националните схеми за сертифициране следва да изискват от доставчиците на портфейли да демонстрират начина, по който предоставяния от тях проект на технологичното решение за портфейла съответства на референтната архитектура и представя подробно проверките за сигурност и плановете за валидиране за конкретното технологично решение за портфейла. В националните схеми за сертифициране следва също така да се определи дейност по оценка на съответствието, за да се провери дали проектът на портфейла отразява правилно референтната архитектура на избрания профил. Националните схеми за сертифициране следва да отговарят на изискванията, посочени в член 51 от Регламент (ЕС) 2019/881, с изключение на букви д) и е), свързани с регистрирането.

(14) По отношение на сертифицирането на продукти следва да бъде разрешено използването на сертификати за съответствие, издадени съгласно схемата на ЕС за сертифициране на киберсигурността, основана на ЕССК, и сертификати за съответствие, издадени съгласно национални схеми за сертифициране в контекста на Споразумението за взаимно признаване на Групата на висшите служители по сигурността на информационните системи (SOG-IS). Освен това следва да се разреши използването на други национални схеми за сертифициране за по-малко чувствителни продуктови компоненти, като тези, установени съгласно стандарта CEN EN 17640 за методиката за оценка на киберсигурността с фиксирано време.

(15) Марката за доверие на портфейла за цифрова самоличност на ЕС („марка за доверие“) следва да се използва, за да се посочи по ясен, прост и разпознаваем начин, че портфейлът е предоставен в съответствие с Регламент (ЕС) № 910/2014. Поради това тя следва да се счита за знак за съответствие за технологично решение за портфейл, сертифицирано съгласно национални схеми за сертифициране. В националните схеми за сертифициране не следва да определят никакви други марки за съответствие.

(16) За да се обезсърчат измамите, националните схеми за сертифициране следва да определят действията, които трябва да се предприемат, когато сертифицирането съгласно схемата се претендира чрез измама.

(17) За да осигурят ефективно управление на уведомленията за уязвимости, доставчиците на технологични решения за портфейл и схемата за електронна идентификация, по която те се предоставят, следва да определят и да прилагат процеси за оценка на сериозността и потенциалното въздействие на уязвимостите. Националните схеми за сертифициране следва да определят праг, над който сертифициращият орган трябва да бъде уведомен. Такова изискване за уведомяване не следва да засяга критериите, установени от законодателството за защита на данните и органите за защита на данните на държавите членки за уведомяване за нарушения на сигурността на личните данни. Могат да бъдат установени възможни полезни взаимодействия между задължителното уведомяване за нарушение или компрометиране на технологичните решения за портфейл и уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679. Оценката на сертифициращия орган на доклада за анализ на въздействието на уязвимостта не следва да засяга оценката на органа за защита на данните на оценка на въздействието върху защитата на данните съгласно членове 35 и 36 от Регламент (ЕС) 2016/679.

(18) Доставчиците на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, следва да уведомят собственика на схемата за всички основания за изключения от оценката на уязвимостта, необходима за оценката на ЗКУП и ЗКПП, както е посочено в приложение IV.

(19) Отмяната на сертификат за съответствие може да има тежки последици, като например отмяна на всички внедрени портфейлни блокове. Поради това сертифициращите органи следва да обмислят отмяна само ако е налице вероятност неотстранена уязвимост да повлияе значително върху надеждността на технологичното решение за портфейла или надеждността на друго технологично решение за портфейла.

(20) Следва да се въведе специфичен процес за актуализиране на националните схеми за сертифициране с цел да се управлява преходът между последователните версии на схемите, по-специално във връзка с действията, които трябва да бъдат предприети от притежателя на сертификата по отношение на предстоящи оценки, поддръжка, повторно сертифициране и специални оценки.

(21) За да се улесни прозрачността, доставчиците на портфейли следва публично да споделят информация за сигурността относно своето технологично решение за портфейла.

(22) Когато националните схеми за сертифициране разчитат на информация във връзка с осигуреността от други схеми или източници за сертифициране, следва да се извърши анализ на зависимостта, за да се провери дали документацията във връзка с осигуреността, например доклади във връзка с осигуреността и сертификати за съответствие, е налична и подходяща за технологичните решения за портфейла и схемата за електронна идентификация, съгласно която те се предоставят. Този анализ на зависимостта следва да се основава на оценката на риска на технологичните решения за портфейла и схемата за електронна идентификация, съгласно която те се предоставят. При оценката следва да се определи дали наличната документация във връзка с осигуреността за дадено технологично решение за портфейла и схемата за електронна идентификация, съгласно която то се предоставя, е подходяща за предоставяне на осигуреност, съответстваща на целевото равнище на оценка. При оценката следва да се актуализира и анализът на зависимостта или той да се преоцени изцяло, когато това е необходимо.

(23) Сертифициращите органи следва да издават сертификати за съответствие в рамките на националните схеми за сертифициране, заедно с публично достъпен доклад за сертифициране, както е посочено в член 5г, параграф 2, буква а) от Регламент (ЕС) № 910/2014. Свързаният доклад за оценка на сертифицирането следва да бъде предоставен на групата за сътрудничество.

(24) В националните схеми за сертифициране следва да се представя годишна оценка на надзора, за да се гарантира ефективната работа на процесите, свързани с управлението и поддръжката на портфейлите, което означава, че те работят, както е предвидено в политиките, определящи процесите. Изискването за оценка на уязвимостта на всеки две години произтича от Регламент (ЕС) № 910/2014, за да се гарантира, че технологичното решение за портфейла продължава да покрива по подходящ начин рисковете и заплахите за киберсигурността, установени в регистъра на рисковете, включително всяка промяна в контекста на заплахите. Понятията оценки на надзора, оценки за повторно сертифициране и специални оценки следва да са в съответствие с EN ISO/IEC 17021-1:2015.

(25) Цикълът на сертифициране завършва с изтичане на срока на действие на сертификата за съответствие или с издаването на нов сертификат за съответствие след успешна оценка на повторното сертифициране. Оценката на повторното сертифициране следва да включва оценка на всички компоненти на обекта на сертифициране, включително оценка на ефективността и, когато е приложимо, оценка на уязвимостта. По време на повторното сертифициране следва да е възможно повторното използване на резултатите от предишни оценки на компоненти, които не са променени.

(26) Когато бъде приета европейска схема за сертифициране на киберсигурността, националните схеми за сертифициране със същия обхват следва да спрат да издават сертификати след определен преходен период, както е посочено в член 57, параграф 1 от Регламент (ЕС) 2019/881.

(27) Националните схеми за сертифициране следва да разчитат на съществуващи рамки и да използват повторно доказателства, когато е подходящо, за да осигурят хармонизация и оперативна съвместимост. Държавите членки могат да сключват споразумения за трансгранично повторно използване на схеми за сертифициране или части от тях. Европейската комисия и ENISA следва, в сътрудничество с групата за сътрудничество, да подкрепят държавите членки при разработването и поддържането на техните национални схеми за сертифициране, като гарантират обмен на знания и най-добри практики.

(28) 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 ([9]) и той прие своето становище на 30 септември 2024 г.

(29) Предвидените в настоящия регламент мерки са в съответствие със становището на Комитета, посочен в член 48, параграф 1 от Регламент (ЕС) № 910/2014,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и приложно поле

С настоящия регламент се определят референтни стандарти и се установяват спецификации и процедури за изграждане на стабилна рамка за сертифициране на портфейли, която трябва редовно да се актуализира, за да бъде в съответствие с развитието на технологиите и стандартите и с работата, извършена въз основа на Препоръка (ЕС) 2021/946 относно общ инструментариум на Съюза за координиран подход към европейска рамка за цифрова самоличност, и по-специално рамката за техническа архитектура и технически справки.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „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;

2) „собственик на схема“ означава организация, която отговаря за разработването и поддържането на схема за сертифициране;

3) „обект на сертифициране“ означава продукти, процеси и услуги или комбинация от тях, по отношение на които се прилагат определени изисквания;

4) „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;

5) „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;

([9]) 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).

6) „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;

7) „регистър на рисковете“ означава запис на информация, свързана с процеса на сертифициране относно установените рискове;

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

9) „сертифициращ орган“ означава орган за оценка на съответствието — трето лице, работещ със схеми за сертифициране;

10) „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;

11) „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;

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

(13) „инцидент“ означава инцидент съгласно определението в член 6, точка 6 от Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([10]);

(14) „включени политики за оповестяване“ означава набор от правила, включени при електронно удостоверение за атрибути от техния доставчик, посочващи условията, които доверяващата се на портфейла страна трябва да изпълни, за да получи достъп до електронното удостоверение за атрибути.

ГЛАВА II

НАЦИОНАЛНИ СХЕМИ ЗА СЕРТИФИЦИРАНЕ

Член 3

Установяване на национални схеми за сертифициране

1. Държавите членки определят собственик на схемата за всяка национална схема за сертифициране.

2. Обектът на сертифициране, определен в националните схеми за сертифициране, е предоставянето и функционирането на технологични решения за портфейл и на схемите за електронна идентификация, съгласно които те се предоставят.

3. В съответствие с Регламент за изпълнение (ЕС) 2015/1502 обектът на сертифициране в националните схеми за сертифициране включва следните елементи:

а) компонентите на софтуер, включително настройки и конфигурации на технологично решение за портфейла и на схемата за електронна идентификация, съгласно която технологичните решения за портфейла се предоставят;

б) хардуерните компоненти и платформи, на които посочените в точка б) софтуерни компоненти работят или разчитат във връзка с операции от критично значение, в случаите, когато те се предоставят пряко или непряко от технологичното решение за портфейла и схемата за електронна идентификация, съгласно която то се предоставя, и когато се изискват, за да отговарят на желаното ниво на осигуреност за тези софтуерни компоненти. Когато хардуерните компоненти и платформи не се предоставят от доставчика на портфейла, в националните схеми за сертифициране се формулират допускания за оценката на хардуерните компоненти и платформи, съгласно които може да се осигури съпротива срещу атакуващи с висок потенциал за атака в съответствие с Регламент за изпълнение (ЕС) 2015/1502, и да се уточнят дейностите по оценка за потвърждаване на тези допускания, както е посочено в приложение IV;

([10]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

в) процесите, с които се поддържат предоставянето и функционирането на технологичното решение за портфейла, включително процеса на включване на ползвателя, както е посочено в член 5а от Регламент (ЕС) № 910/2014, които обхващат най-малко записване, управление на електронни средства и организация съгласно раздели 2.1, 2.2 и 2.4 от приложение I към Регламент за изпълнение (ЕС) 2015/1502.

4. Националните схеми за сертифициране включват описание на конкретната архитектура на технологичните решения за портфейла и на схемата за електронна идентификация, съгласно която те се предоставят. Когато националните схеми за сертифициране обхващат повече от една конкретна архитектура, те включват профил за всяка конкретна архитектура.

5. За всеки профил в националните схеми за сертифициране се определя най-малко следното:

а) конкретната архитектура на технологично решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя;

б) проверките за сигурност, свързани с нивата на осигуреност, определени в член 8 от Регламент (ЕС) № 910/2014;

в) план за оценка, изготвен в съответствие с раздел 7.4.1 от EN ISO/IEC 17065:2012;

г) изискванията за сигурност, необходими за справяне с рисковете и заплахите за киберсигурността, изброени в посочения в приложение I към настоящия регламент регистър на рисковете, до изискваното ниво на осигуреност и за постигане, когато е приложимо, на целите, определени в член 51 от Регламент (ЕС) 2019/881;

д) обозначаване на посочените в буква б) от настоящия параграф проверки на компонентите на архитектурата;

е) описание на начина, по който проверките на сигурността, обозначаването, изискванията за сигурност и планът за оценка, посочени в букви б) и в), позволяват на доставчиците на технологичните решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, да се справят по подходящ начин с рисковете и заплахите за киберсигурността, установени в посочения в буква г) регистър на рисковете, до изискваното ниво на осигуреност въз основа на оценката на риска, за да прецизират и допълнят посочените в регистъра рискове и заплахи с такива, които са специфични за конкретната архитектура.

6. В плана за оценка, посочен в параграф 5, буква в), се изброяват дейностите по оценка, които трябва да бъдат включени в оценката на технологичните решения за портфейл и на схемата за електронна идентификация, съгласно която те се предоставят.

7. При посочената в параграф 6 дейност за оценка от доставчиците на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, се изисква да предоставят информация, отговаряща на изискванията, посочени в приложение II.

Член 4

Общи изисквания

1. Националните схеми за сертифициране покриват изискванията за функционалност, киберсигурност и защита на данните, като използват, когато са налични и приложими, следните схеми за сертифициране:

а) европейските схеми за сертифициране на киберсигурността, създадени съгласно Регламент (ЕС) 2019/881, включително европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК);

б) национални схеми за сертифициране на киберсигурност, обхванати от ЕССК, в съответствие с член 49 от Регламент за изпълнение (ЕС) 2024/482.

2. Националните схеми за сертифициране могат в допълнение, когато са налични и приложими, да се отнасят до:

а) други съответни национални схеми за сертифициране;

б) международни, европейски и национални стандарти;

в) технически спецификации, които отговарят на изискванията, определени в приложение II към Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета ([11]).

3. Националните схеми за сертифициране:

а) уточняват елементите, посочени в раздел 6.5 от EN ISO/IEC 17067:2013;

б) се изпълняват като схема тип 6, в съответствие с раздел 5.3.8 от EN ISO/IEC 17067:2013.

4. Националните схеми за сертифициране отговарят на следните изисквания:

а) на условията за издаване на сертификати съгласно националните схеми за сертифициране отговарят само доставчиците, посочени в член 5а, параграф 2 от Регламент (ЕС) № 910/2014;

б) като марка за съответствие се използва само марката на доверие;

в) когато се позовават на схемата, доставчиците на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, включват препратки към Регламент (ЕС) № 910/2014 и настоящия регламент;

г) доставчиците на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, допълват оценката на риска на схемата, както е посочено в член 3, параграф 5, буква е), за да идентифицират рисковете и заплахите, специфични за тяхното прилагане, и предлагат подходящи мерки за справяне с всички съответни рискове и заплахи;

д) отговорностите и правните действия са установени и включват препратки към приложимото национално законодателство, в което се определят отговорностите и възможните правни действия, в случай че сертифицирането по схемата се използва по измамен начин.

5. Оценката, посочена в параграф 4, буква г), се споделя със сертифициращия орган, извършващ оценката.

Член 5

Управление на инциденти и уязвимостта

1. Националните схеми за сертифициране съдържат изисквания за управление на инциденти и уязвимостта в съответствие с параграфи 2—9.

2. Притежателят на сертификат за съответствие на технологично решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя, уведомява своя сертифициращ орган без неоснователно забавяне за всяко нарушение или компрометиране на технологичното решение за портфейла или на схемата за електронна идентификация, съгласно която то се предоставя, при условие че е вероятно да повлияе на съответствието му с изискванията на националните схеми за сертифициране.

3. Притежателят на сертификат за съответствие установява, поддържа и прилага политика и процедури за управление на уязвимостите, като взема предвид процедурите, посочени в съществуващите европейски и международни стандарти, включително EN ISO/IEC 30111:2019.

4. Притежателят на сертификата за съответствие уведомява издаващия сертифициращ орган за уязвимостите и промените, засягащи технологичното решение за портфейла, въз основа на определени критерии за въздействието на тези уязвимости и промени.

5. Притежателят на сертификата за съответствие изготвя доклад за анализ на въздействието на уязвимостта за всяка уязвимост, която засяга софтуерните компоненти на технологичното решение за портфейла. Докладът включва следната информация:

а) въздействието на уязвимостта върху сертифицираното технологично решение за портфейла;

б) възможни рискове, свързани с близостта или вероятността от атака;

([11]) Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (текст от значение за ЕИП) (ОВ L 316, 14.11.2012 г., стр. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

в) дали уязвимостта може да бъде отстранена с наличните средства;

г) когато уязвимостта може да бъде отстранена с наличните средства — възможните налични за отстраняване на уязвимостта.

6. Когато в параграф 4 се изисква уведомяване, притежателят на сертификата за съответствие предава на сертифициращия орган без неоснователно забавяне доклада за анализ на въздействието на уязвимостта, посочен в параграф 5.

7. Притежателят на сертификат за съответствие установява, поддържа и управлява политика за управление на уязвимостите, отговаряща на изискванията, посочени в приложение I към Акта за киберустойчивостта ([12]).

8. Националните схеми за сертифициране установяват изисквания за оповестяване на уязвимости, приложими по отношение на сертифициращите органи.

9. Притежателят на сертификат за съответствие оповестява и регистрира всяка публично известна и отстранена уязвимост в технологичното решение за портфейла или в някое от онлайн хранилищата, посочени в приложение V.

Член 6

Поддръжка на националните схеми за сертифициране

1. Националните схеми за сертифициране включват процес за периодичен преглед на функционирането им. Целта на този процес е да се потвърди тяхната адекватност и да се установят аспекти, които изискват подобрение, като се вземе предвид получената от заинтересованите страни обратна информация.

2. Националните схеми за сертифициране включват разпоредби относно тяхната поддръжка. Този процес включва най-малко следните изисквания:

а) правила за управление на определението и изискванията на националните схеми за сертифициране;

б) установяване на срокове за издаване на сертификати след приемането на актуализирани версии на националните схеми за сертифициране — както за нови сертификати за съответствие, така и за вече издадени такива;

в) периодичен преглед на националните схеми за сертифициране, за да се гарантира, че изискванията на националните схеми за сертифициране се прилагат по последователен начин, като се вземат предвид най-малко следните аспекти:

— искания за разяснения, отправени към собственика на схемата, свързани с изискванията на националната схема за сертифициране;

— обратна информация от действащите лица и други заинтересовани страни;

— способност на собственика на националната схема за сертифициране да реагира на искания за информация;

г) правила за наблюдение на референтни документи и процедури за развитие на референтните версии на националните схеми за сертифициране, включително най-малко преходни периоди;

д) процес, необходим за да се гарантира, че са обхванати най-новите рискове и заплахи за киберсигурността, изброени в регистъра на рисковете, посочен в приложение I към настоящия регламент;

е) процес за управление на други промени в националните схеми за сертифициране.

([12]) Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ L, 2024/2847, 20.11.2024 г., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Националните схеми за сертифициране съдържат изисквания за извършване на оценки на сертифицираните понастоящем продукти в рамките на определен период след прегледа на схемата или след пускането на нови спецификации или стандарти или нови техни версии, които се спазват от технологичните решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят.

ГЛАВА III

ИЗИСКВАНИЯ, СВЪРЗАНИ СЪС СОБСТВЕНИЦИТЕ НА СХЕМИТЕ

Член 7

Общи изисквания

1. Собствениците на схеми разработват и поддържат национални схеми за сертифициране и управляват техните операции.

2. Собствениците на схеми могат да възлагат всички или част от задачите си на подизпълнители — трети лица. Когато възлагат на подизпълнител — частно лице, собствениците на схемата определят задълженията и отговорностите на всички страни в договор. Собствениците на схемата остават отговорни за всички възложени на подизпълнители дейности, извършвани от техните подизпълнители.

3. Собствениците на схеми извършват своите дейности по наблюдение, ако е приложимо, най-малко въз основа на следната информация:

а) информация, получена от сертифициращи органи, национални органи по акредитация и съответните органи за надзор на пазара;

б) информация, получена в резултат на собствени одити и разследвания или одити и разследвания на други органи;

в) възражения и обжалвания в съответствие с член 15.

4. Собствениците на схеми уведомяват групата за сътрудничество за преразглеждания на националните схеми за сертифициране. Това уведомление предоставя подходяща информация за групата за сътрудничество за издаване на препоръки към собствениците на схеми и становища относно актуализираните национални схеми за сертифициране.

ГЛАВА IV

ИЗИСКВАНИЯ, СВЪРЗАНИ С ДОСТАВЧИЦИТЕ НА ТЕХНОЛОГИЧНИ РЕШЕНИЯ ЗА ПОРТФЕЙЛ И СХЕМАТА ЗА ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ, СЪГЛАСНО КОЯТО ТЕ СЕ ПРЕДОСТАВЯТ

Член 8

Общи изисквания

1. Националните схеми за сертифициране съдържат изисквания за киберсигурност въз основа на оценка на риска за всяка конкретна поддържана архитектура. Целта на тези изисквания за киберсигурност е да се разглеждат установените рискове и заплахи за киберсигурността, определени в посочения в приложение I регистър на рисковете.

2. В съответствие с член 5а, параграф 23 от Регламент (ЕС) № 910/2014 националните схеми за сертифициране изискват технологичните решения за портфейл и схемите за електронна идентификация, съгласно които те се предоставят, да бъдат устойчиви срещу атакуващи с висок потенциал за атака за ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502.

3. Националните схеми за сертифициране установяват критерии за сигурност, които включват следните изисквания:

а) Акта за киберустойчивостта, когато е приложимо, или изисквания, отговарящи на целите на сигурността, посочени в член 51 от Регламент (ЕС) 2019/881;

б) установяването и прилагането на политики и процедури относно управлението на рисковете, свързани с работата на технологично решение за портфейла, включително установяването и оценката на рисковете и смекчаването на установените рискове;

в) установяването и прилагането на политики и процедури, свързани с управлението на промените и с управлението на уязвимостите в съответствие с член 5 от настоящия регламент;

г) установяването и прилагането на политики и процедури за управление на човешките ресурси, включително изисквания за експертен опит, надеждност, опит, обучение за сигурност и квалификация на персонала, участващ в разработването или управлението на технологичното решение за портфейла;

д) изискванията, свързани с операционната среда на технологичното решение за портфейла, включително под формата на допускания за сигурността на устройствата и платформите, на които работят софтуерните компоненти на технологичното решение за портфейла, включително ЗКУП и, когато е приложимо и относимо, изисквания за оценка на съответствието, за да се потвърди, че тези допускания са преминали проверка на съответните устройства и платформи;

е) за всяко допускане, което не е подкрепено от сертификат за съответствие или друга приемлива информация за осигуреност — описание на механизма, който доставчикът на портфейла използва, за да наложи допускането, както и обосновка, че механизмът е достатъчен, за да се гарантира, че допускането е преминало проверка;

ж) установяването и прилагането на мерки за гарантиране на използването на настоящата сертифицирана версия на технологичното решение за портфейла.

4. Националните схеми за сертифициране съдържат функционални изисквания, свързани с механизмите за актуализиране за всеки софтуерен компонент на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, за изброените в приложение III операции.

5. Националните схеми за сертифициране изискват следната информация и документация да бъдат представени или предоставени по друг начин на сертифициращия орган от заявителя за сертифициране:

а) доказателства, свързани с посочената в приложение IV, точка 1 информация, включително, когато е необходимо, подробности относно технологичното решение за портфейла и неговия изходен код, включително:

— *информация за архитектурата*: за всеки компонент на технологичното решение за портфейла (включително компоненти за продукт, процес и услуга) — описание на неговите основни свойства, свързани със сигурността, включително неговите външни зависимости;

— *нива на контрол и осигуреност*: за всяка проверка на сигурността на технологичното решение за портфейла — описание на проверката и необходимото ниво на осигуреност, въз основа на приложението към Регламент за изпълнение (ЕС) 2015/1502, определящо редица технически спецификации и процедури, които се прилагат за различните проверки, реализирани чрез средствата за електронна идентификация;

— *обозначаване на проверките на компонентите на архитектурата*: описание на начина, по който проверките на портфейла се прилагат с помощта на различните компоненти на технологичното решение за портфейла, въз основа на обосновка, в която се пояснява причината за изискването на дадено ниво на осигуреност и начина на извършване на проверката, заедно с всички необходими аспекти на сигурността на подходящото ниво;

— *обосновка и аргументация на покритието на риска*: обосновка на:

— обозначаването на проверките на компонентите;

— пригодността на предложения план за оценка да обхваща по подходящ начин всички проверки;

— покритието от проверките на рисковете и заплахите за киберсигурността, установени в регистъра на рисковете, допълнени от проверките на рисковете и заплахите, специфични за изпълнението, при подходящо ниво на осигуреност.

б) информацията, посочена в приложение V;

в) пълен списък на сертификатите за съответствие и друга информация за осигуреността, използвана като доказателство по време на дейностите по оценка;

г) всяка друга информация от значение за дейностите по оценка.

ГЛАВА V

ИЗИСКВАНИЯ, СВЪРЗАНИ СЪС СЕРТИФИЦИРАЩИТЕ ОРГАНИ

Член 9

Общи изисквания

1. Сертифициращите органи се акредитират от национални органи по акредитация, назначени съгласно Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета ([13]) в съответствие с EN ISO/IEC 17065:2012, при условие че отговарят на изискванията, определени в националните схеми за сертифициране в съответствие с параграф 2.

2. За целите на акредитацията сертифициращите органи отговарят на всички изброени по-долу изисквания за компетентност:

а) подробни и технически познания за съответните архитектури на технологично решение за портфейла и за схемата за електронна идентификация, съгласно която то се предоставя, както и за заплахите и рисковете, свързани с тези архитектури;

б) познаване на наличните решения, свързани със сигурността, и техните свойства съгласно приложението към Регламент за изпълнение (ЕС) 2015/1502;

в) познаване на дейностите, извършвани по силата на сертификати за съответствие, прилагани по отношение на компонентите на технологичното решение за портфейла и схемата за електронна идентификация, съгласно която то се предоставя, като обект на сертифициране;

г) задълбочено познаване на приложимата национална схема за сертифициране, създадена в съответствие с глава II.

3. Сертифициращите органи извършват дейностите си по надзор, по-специално въз основа на следната информация:

а) информация, получена от националните органи по акредитация и съответните органи за надзор на пазара;

б) информация, получена в резултат на собствени одити и разследвания или одити и разследвания на други органи;

в) възражения и обжалвания в съответствие с член 15.

Член 10

Възлагане на подизпълнители

Сертифициращите органи могат да възлагат дейностите по оценка на подизпълнители — трети лица, както е посочено в член 13. Когато дейностите по оценка са възложени на подизпълнители, националните схеми за сертифициране установяват следното:

1) всички подизпълнители на сертифициращия орган, извършващи дейности по оценка, отговарят, както е приложимо и целесъобразно за дейностите, които ще се извършват, на изискванията на хармонизирани стандарти като EN ISO/IEC 17025:2017 за изпитване, EN ISO/IEC 17020:2012 за проверка, EN ISO/IEC 17021-1:2015 за одит и EN ISO/IEC 17029:2019 за валидиране и проверка;

2) сертифициращите органи поемат отговорност за всички дейности по оценка, възложени на други органи, и демонстрират, че са предприели подходящи мерки по време на своята акредитация, включително като разчитат на собствената акредитация на своите подизпълнители, когато това е приложимо;

3) степента, до която предварително съгласие за нуждите от възлагане на дейности на външни изпълнители трябва да се получи от собствениците на схемата или от клиента, чието технологично решение за портфейла се сертифицира съгласно схемата за сертифициране.

([13]) Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Член 11

Уведомяване на надзорния орган

Сертифициращите органи уведомяват надзорния орган, посочен в член 46а, параграф 1 от Регламент (ЕС) № 910/2014, за издаването, спирането и отмяната на сертификати за съответствие на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят.

Член 12

Управление на инциденти и уязвимостта

1. Сертифициращите органи спират, без неоснователно забавяне, действието на сертификата за съответствие на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, след като потвърдят, че пробивът или компрометирането на сигурността, за които е съобщено, влияе върху съответствието с изискванията на националните схеми за сертифициране, на технологичното решение за портфейла или на схемата за електронна идентификация, съгласно която то се предоставя.

2. Сертифициращите органи отменят сертификата за съответствие, спрян поради нарушение на сигурността или компрометиране, което не е отстранено своевременно.

3. Сертифициращите органи отменят сертификати за съответствие, когато установената уязвимост не е била отстранена своевременно, пропорционално на нейната тежест и потенциално въздействие, в съответствие с член 5в, параграф 4 и член 5д, параграф 2 от Регламент (ЕС) № 910/2014.

ГЛАВА VI

ДЕЙНОСТИ ПО ОЦЕНКА НА СЪОТВЕТСТВИЕТО

Член 13

Дейности по оценка

1. Националните схеми за сертифициране съдържат методи и процедури, които да се използват от органите за оценка на съответствието, когато извършват своите дейности по оценка в съответствие с EN ISO/IEC 17065:2012, които обхващат най-малко следните аспекти:

а) методите и процедурите за извършване на дейности по оценка, включително тези, свързани със ЗКУП, както е посочено в приложение IV;

б) одитът на прилагането на технологичното решение за портфейла и схемата за електронна идентификация, съгласно която то се предоставя, въз основа на посочения в приложение I регистър на рисковете, допълнен, когато е необходимо, от специфични за изпълнението рискове;

в) дейности по функционално изпитване, които се основават, когато са налични и подходящи, на набори от изпитвания, определени съгласно технически спецификации или стандарти;

г) оценка на наличието и пригодността на процесите на поддръжка, включително най-малко управление на версиите, управление на актуализацията и управление на уязвимостите;

д) оценка на оперативната ефективност на процесите на поддръжка, включително най-малко управление на версиите, управление на актуализацията и управление на уязвимостите;

е) анализ на зависимостта, предоставен от доставчика на портфейла, включително методика за оценка на приемливостта на информацията във връзка с осигуреността, която включва посочените в приложение VI елементи;

ж) оценка на уязвимостта на подходящо ниво, включително:

— преглед на проекта на технологичното решение за портфейла и, когато е приложимо, на изходния му код;

— изпитване на устойчивостта на технологичното решение за портфейла срещу атакуващи с висок потенциал за атака за ниво на осигуреност „високо“ съгласно раздел 2.2.1 от приложението към Регламент за изпълнение (ЕС) 2015/1502;

з) оценка на развитието на средата на заплахата и нейното въздействие върху покритието на рисковете от технологичното решение за портфейла, за да се определи кои дейности по оценка са необходими за различните компоненти на технологичното решение за портфейла.

2. Националните схеми за сертифициране включват оценка, за да се определи дали прилагането на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, съответстват на архитектурата, посочена в член 3, параграф 5, буква а), както и оценка за определяне на това дали предложеният заедно с изпълнението план за оценка съответства на плана за оценка, посочен в член 3, параграф 5, буква в).

3. Националните схеми за сертифициране определят правила за изготвяне на извадки с цел да се избегне повторението на идентични дейности по оценка и да се постави акцент върху дейности, които са специфични за даден вариант. Тези правила за изготвяне на извадки предоставят възможност за извършването на функционални изпитвания и изпитвания за сигурност само върху извадка от варианти на целеви компонент на технологично решение за портфейла и схемата за електронна идентификация, съгласно която то се предоставя, както и върху извадка от целеви устройства. Националните схеми за сертифициране изискват от всички сертифициращи органи да обосноват използването на изготвянето на извадки.

4. Националните схеми за сертифициране изискват оценка от сертифициращия орган на ЗКПП въз основа на методите и процедурите, посочени в приложение IV.

Член 14

Дейности по сертифициране

1. Националните схеми за сертифициране определят дейността по удостоверяване с цел издаване на сертификат за съответствие съгласно раздел V, буква а) от EN ISO/IEC 17067:2013, таблица 1, включително следните аспекти:

а) съдържанието на сертификата за съответствие, както е посочено в приложение VII;

б) начина, по който резултатите от оценката трябва да бъдат докладвани в публичния доклад за сертифициране, включително най-малко резюме на предварителния одит и план за валидиране, както е посочено в приложение VIII;

в) съдържанието на резултатите от оценката, докладвани в доклада за оценка на сертифицирането, включително елементите, посочени в приложение VIII.

2. Докладът за оценка на сертифицирането може да бъде предоставен на групата за сътрудничество и на Комисията.

Член 15

Възражения и жалби

Националните схеми за сертифициране съдържат процедури или препратки към приложимото национално законодателство, които определят механизма за ефективно подаване и разглеждане на възражения и жалби във връзка с прилагането на схемата за сертифициране или издадения сертификат за съответствие. Тези процедури включват предоставяне на информация на жалбоподателя за хода на производството и за взетото решение, както и информация на жалбоподателя относно правото на ефективно средство за правна защита. Националните схеми за сертифициране изискват всички възражения и жалби, които не са били или не могат да бъдат разрешени от сертифициращия орган, да се изпращат на собственика на схемата за оценка и решаване.

Член 16

Дейности по надзор

1. Националните схеми за сертифициране изискват от сертифициращите органи да прилагат дейности по надзор, състоящи се от надзорна оценка на процесите, комбинирана с произволни изпитвания или проверки.

2. Националните схеми за сертифициране съдържат изисквания към собствениците на схеми да наблюдават спазването от сертифициращите органи на задълженията им съгласно Регламент (ЕС) № 910/2014 и съгласно националните схеми за сертифициране, ако е приложимо.

3. Националните схеми за сертифициране съдържат изисквания към сертифициращите органи да наблюдават за следното:

а) спазване от страна на притежателите на сертификат за съответствие, издаден съгласно национални схеми за сертифициране, на задълженията им по отношение на сертифицирането съгласно Регламент (ЕС) № 910/2014 и съгласно националните схеми за сертифициране;

б) съответствие на сертифицираното технологично решение за портфейла с изискванията, определени в националните схеми за сертифициране.

Член 17

Последици от несъответствието

В националните схеми за сертифициране се определят последиците от несъответствието на сертифицирано технологично решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя, заедно с посочените в настоящия регламент изисквания. Тези последици включват следните аспекти:

1) задължението на сертифициращия орган да информира притежателя на сертификата за съответствие и да изиска от притежателя на сертификата за съответствие да прилага коригиращи действия;

2) задължението на сертифициращия орган да информира други съответни органи за надзор на пазара, когато несъответствието засяга съответното законодателство на Съюза;

3) условията за извършване на коригиращи действия от притежателя на сертификата за съответствие;

4) условията за спиране на действието на сертификата за съответствие от сертифициращия орган и за възстановяване на сертификата за съответствие след отстраняване на несъответствието;

5) условията за отмяна на сертификат за съответствие от сертифициращия орган;

6) последиците от неспазване от страна на сертифициращия орган на изискванията на националната схема за сертифициране.

ГЛАВА VII

ЖИЗНЕН ЦИКЪЛ НА СЕРТИФИЦИРАНЕТО

Член 18

Жизнен цикъл на сертифицирането

1. Валидността на сертификатите за съответствие, издадени съгласно национални схеми за сертифициране, подлежи на редовни дейности по оценка от страна на сертифициращия орган, извършвани в съответствие с посочените в приложение IX изисквания.

2. Националните схеми за сертифициране съдържат процес за повторно сертифициране на технологични решения за портфейл и схемата за електронна идентификация, съгласно която те се предоставят, по искане на притежателя на сертификата за съответствие преди изтичането на първоначалния сертификат за съответствие. Този процес на повторно сертифициране включва пълна оценка на технологичното решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя, включително оценка на уязвимостта, като се следват принципите, посочени в приложение IX.

3. Националните схеми за сертифициране съдържат процес за управление на промени в сертифицирано технологично решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя. Този процес включва правила, с които се определя дали дадена промяна трябва да бъде обхваната от специална оценка, както е посочено в параграф 4, или от проверка на оперативната ефективност на процесите на поддръжка, както е посочено в приложение IV.

4. Националните схеми за сертифициране съдържат процес за специални оценки в съответствие с EN ISO/IEC 17065:2012. Този процес за специални оценки включва подбор на дейности, които да бъдат извършени за справяне със конкретния проблем в резултат на специалната оценка.

5. Националните схеми за сертифициране определят правила, свързани с отмяната на сертификат за съответствие.

ГЛАВА VIII

ВОДЕНЕ НА ДОКУМЕНТАЦИЯ И ЗАЩИТА НА ИНФОРМАЦИЯТА

Член 19

Съхраняване на документация

1. Националните схеми за сертифициране съдържат изисквания към сертифициращите органи по отношение на система за запис на цялата съответна информация, създадена във връзка с дейностите по оценка на съответствието, които те извършват, включително данни, издадени и получени от доставчиците на технологични решения за портфейл и схемите за електронна идентификация, съгласно които те се предоставят. Записите на такава информация се съхраняват по сигурен начин. Записите могат да се съхраняват по електронен път и остават достъпни толкова дълго, колкото се изисква съгласно правото на Съюза или националното право, и най-малко пет години след отмяната или изтичането на срока на действие на съответния сертификат за съответствие.

2. Националните схеми за сертифициране определят изисквания към притежателя на сертификата за съответствие да съхранява по сигурен начин следната информация за целите на настоящия регламент и най-малко пет години след отмяната или изтичането на срока на действие на съответния сертификат за съответствие:

а) записи на информацията, предоставена на сертифициращия орган или на някой от неговите подизпълнители по време на процеса на сертифициране;

б) образци на хардуерни компоненти, които са включени в обхвата на сертифициране за технологично решение за портфейла.

3. Националните схеми за сертифициране изискват от притежателя на сертификата за съответствие да предоставя при поискване посочената в параграф 1 информация на сертифициращия орган или на надзорния орган, посочен в член 46а, параграф 1 от Регламент (ЕС) № 910/2014.

Член 20

Защита на информацията

Съгласно националните схеми за сертифициране, всички лица или организации, на които е предоставен достъп до информация при изпълнение на дейности по националната схема за сертифициране, са задължени да гарантират сигурността и защитата на търговската тайна и друга поверителна информация, както и да зачитат правата на интелектуална собственост и да вземат необходимите и подходящи технически и организационни мерки, за да гарантират тази поверителност.

ГЛАВА IX

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 21

Преход към европейска схема за сертифициране на киберсигурността

Настоящият регламент подлежи на преразглеждане при приемането на първата европейска схема за сертифициране на киберсигурността за технологични решения за портфейл и схемите за електронна идентификация, съгласно които те се предоставят, с цел да се вземе предвид приносът на такава европейска схема за сертифициране на киберсигурността към цялостното сертифициране на технологични решения за портфейл и схемите за електронна идентификация, съгласно които те се предоставят.

Член 22

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

РЕГИСТЪР НА РИСКОВЕТЕ ЗА ЕВРОПЕЙСКИТЕ ПОРТФЕЙЛИ ЗА ЦИФРОВА САМОЛИЧНОСТ

Въведение

В регистъра на рисковете се описват основните рискове и заплахи за сигурността и неприкосновеността на личния живот, които засягат портфейлите и които трябва да бъдат проверени по подходящ начин във всяка архитектура и изпълнение на портфейли. **Рисковете на високо ниво** (раздел I) са свързани с използването на портфейли от ползватели и доверяващи се страни и с преки заплахи, насочени към активите на портфейлите. Освен това са установени няколко **риска на системно ниво** (раздел II) за портфейлите, които обикновено са резултат от комбинация от заплахи, приложими по отношение на цялата система на портфейла.

Вид риск	Идентификационен номер на риска	Наименования на свързани рискове
Рискове на високо ниво за портфейлите	R1	Създаване или използване на съществуваща електронна самоличност
	R2	Създаване или използване на фалшива електронна самоличност
	R3	Създаване или използване на фалшиви атрибути
	R4	Кражба на самоличност
	R5	Кражба на данни
	R6	Разкриване на данни
	R7	Манипулиране на данни
	R8	Загуба на данни
	R9	Неразрешена трансакция
	R10	Манипулиране на трансакции
	R11	Отказ
	R12	Разкриване на данни за трансакцията
	R13	Прекъсване на услугата
	R14	Следене
Свързани със системата рискове	SR1	Мащабно следене
	SR2	Накърняване на репутацията
	SR3	Неспазване на законовите изисквания

В регистъра се установяват и **технически заплахи** (раздел III), насочени към изпълнението на технологичното решение за портфейла. Тези заплахи са свързани с рисковете от високо ниво, което означава, че всяка една от тях може да се използва за предизвикване на много рискове на високо ниво.

Вид на заплахата	Идентификационен номер на заплахата	Наименования на свързани заплахи	Подкатегории заплахи
Техническа заплаха	TT1	Физически атаки	1.1. *Кражба*
			1.2. *Изтичане на информация*
			1.3 *Подправяне*
	TT2	Грешки и неправилни конфигурации	2.1. *Грешки, допуснати при управление на ИТ система*
			2.2. *Грешки на равнище приложения и грешки при използване*
			2.3. *Грешки по време на разработка и неправилно конфигуриране на системата*

Вид на заплахата	Идентификационен номер на заплахата	Наименования на свързани заплахи	Подкатегории заплахи
	ТТ3	Използване на ненадеждни ресурси	3.1. *Неправилно използване или конфигуриране на компоненти на портфейла*
	ТТ4	Срив и прекъсвания	4.1. *Срив или затруднения във функционирането на оборудване, устройства или системи*
			4.2. *Загуба на ресурси*
			4.3 *Загуба на помощни услуги*
	ТТ5	Злонамерени действия	5.1 *Прихващане на информация*
			5.2 *Фишинг и спуфинг*
			5.3 *Повторно възпроизвеждане на съобщения*
			5.4 *Атака с груба сила*
			5.5 *Уязвимости на софтуера*
			5.6 *Атаки по веригата на доставки*
			5.7 *Зловреден софтуер*
			5.8 *Прогнозиране на произволни числа*

Накрая в регистъра са **изброени преките заплахи за портфейлите**, като всяка от тях е свързана с (неизчерпателен) подбор от рискове (раздел IV).

РАЗДЕЛ I

Рискове на високо ниво за портфейлите

R1. Създаване или използване на съществуваща електронна самоличност

Създаването или използването на съществуваща електронна самоличност се определя като създаване на електронна самоличност в портфейл, който съществува в реалния свят и се предоставя на друг ползвател. По същество този риск води до рисковете „Кражба на самоличност (R4)“ и „Неразрешена трансакции (R9)“.

R2. Създаване или използване на фалшива електронна самоличност

Създаването или използването на фалшива електронна самоличност се определя като създаване на електронна самоличност в портфейл, който не съществува в реалния свят.

R3. Създаване или използване на фалшиви атрибути

Създаването или използването на фалшиви атрибути се определя като създаване или използване на атрибути, които не могат да бъдат валидирани като издадени от твърдяния доставчик и на които не може да се вярва.

R4. Кражба на самоличност

Кражбата на самоличност се определя като неразрешено придобиване на портфейлен блок или загуба на фактори за удостоверяване на самоличността, които дават възможност на дадено лице да се представи за друго лице.

R5. Кражба на данни

Кражбата на данни се определя като неразрешено извличане на данни. Кражбата на данни също е свързана със заплахи, като прихващане на данни (неразрешено събиране на данни при пренос) и декриптиране на данни (неразрешено декриптиране на криптирани данни), които вероятно ще доведат в някои случаи до „Разкриване на данни (R6)“.

R6. Разкриване на данни

Разкриването на данни се определя като неразрешено разкриване на лични данни, включително специални категории лични данни. Рискът от нарушаване на неприкосновеността на личния живот е много подобен, когато се разглежда от гледна точка на неприкосновеността на личния живот, а не от гледна точка на сигурността.

R7. Манипулиране на данни

Манипулирането на данни се определя като неразрешена промяна на данни.

R8. Загуба на данни

Загубата на данни се определя като ситуация, при която съхранените в портфейла данни се губят поради злоупотреба или злонамерено действие. Този риск често е вторичен риск от „Манипулиране на данни (R7)“ или „Прекъсване на услугата (R13)“, при което всички данни или части от тях не могат да бъдат възстановени.

R9. Неразрешена трансакция

Неразрешените трансакции се определят като оперативни дейности, извършвани без разрешението или знанието на ползвателя на портфейла. В много случаи неразрешена трансакция може да доведе до „Кражба на самоличност (R4)“ или „Разкриване на данни (R6)“. Това също така е свързано с неразрешени трансакции, като злоупотреба с криптографски ключове.

R10. Манипулиране на трансакции

Манипулирането на трансакции се определя като неразрешена промяна на операциите в портфейла. Манипулирането на трансакции представлява атака върху целостта и е свързано с нарушаване на целостта на данните.

R11. Отказ

Отказът се определя като ситуация, при която заинтересована страна може да откаже да извърши действие или да участва в трансакция, а други заинтересовани страни нямат подходящи доказателства, за да ѝ противоречат.

R12. Разкриване на данни за трансакцията

Разкриването на данни за трансакция се определя като разкриване на информация, свързана с трансакция между заинтересовани страни.

R13. Прекъсване на услугата

Прекъсването на услугата се определя като прекъсване или влошаване на нормалната работа на портфейла. Специфичен вид прекъсване на услугата е блокирането на ползвателя, определено като невъзможност на ползвателя да получи достъп до профила или до портфейла си.

R14. Следене

Следенето или наблюдението се определя като неразрешено проследяване или наблюдение на дейностите, комуникацията или данните на ползвателя на портфейла. Следенето често е свързано с правене на изводи, което се определя като извличане на чувствителна или лична информация от привидно безобидни данни.

РАЗДЕЛ II

Свързани със системата рискове

Тези рискове не се използват в списъка със заплахи, тъй като обикновено са следствие от множество заплахи, повтарящи се по начин, който застрашава цялата система.

SR1. Мащабно следене

Мащабното следене се определя като проследяване или наблюдение на дейностите на много ползватели чрез комуникацията или данните на портфейла им. Мащабното следене често се свързва със Следене (R14) и правене на изводи в глобален мащаб, където се комбинира информацията за много ползватели, за да се изведат чувствителни или лични данни за ползвателите или да се идентифицират статистически тенденции, които могат да се използват за проектиране на допълнителни атаки.

SR2. Накърняване на репутацията

Накърняването на репутацията се определя като вреда, нанесена на репутацията на организация или правителствен орган. Накърняването на репутацията ще произтича и от други рискове, когато нарушение или инцидент се отразява от медиите и представя организацията в неблагоприятна светлина. Накърняването на репутацията може да доведе до допълнителни рискове, като загуба на доверие, произтичаща от основателни съмнения на ползвателя, и загуба на екосистема, когато цялата екосистема се срине.

SR3. Неспазване на законовите изисквания

Неспазването на законовите изисквания се определя като ситуация, при която съответните законови и подзаконови, разпоредби или стандарти не могат да бъдат спазени. В контекста на портфейла, тъй като сигурността и неприкосновеността на личния живот за решението са законови изисквания, всички заплахи вероятно ще доведат до някакъв вид неспазване на законовите изисквания.

РАЗДЕЛ III

Технически заплахи

Не всички технически заплахи са свързани с конкретни рискове за портфейлите, тъй като много от тях са средства, които могат да се използват за осъществяване на атаки, съответстващи на много различни рискове.

TT1. Физически атаки

1.1. *Кражба*

Кражбата се определя като кражба на устройства, които могат да променят правилното функциониране на портфейла (в случай че устройството е откраднато и портфейлният блок не е защитен по подходящ начин). Това може да допринесе за много рискове, включително Кражба на самоличност (R4), Кражба на данни (R5) и Неразрешени трансакции (R9).

1.2. *Изтичане на информация*

Изтичането на информация се определя като неразрешен достъп, излагане на информация или споделяне след физически достъп до портфейла. Това може да допринесе по-специално за Разкриване на данни (R6) и Кражба на данни (R5).

1.3. *Подправяне*

Подправянето се определя като нарушаване на целостта на един или множество компоненти на портфейлния блок или на компонентите, на които разчита портфейлният блок, например потребителското устройство или неговата операционна система. Това може да допринесе по-специално за Манипулиране на данни (R7), Загуба на данни (R8) и Манипулиране на трансакции (R10). Когато подправянето е насочено към софтуерни компоненти, то може да допринесе за много рискове.

TT2. Грешки и неправилни конфигурации

2.1 *Грешки, допуснати при управление на ИТ система*

Грешките, допуснати при управлението на ИТ система, се определят като изтичане или споделяне на информация или вреди, причинени от злоупотреба с ИТ активи от ползвателите (непознаване на функциите на приложението) или от неправилна конфигурация или управление на ИТ активи.

2.2 *Грешки на равнище приложения и грешки при използване*

Грешките на равнище приложения или грешките при използване се определят като нарушения на приложението поради грешка в самото приложение или грешка на някой от ползвателите (ползватели на портфейла и доверяващи се страни).

2.3. *Грешки по време на разработка и неправилно конфигуриране на системата*

Грешките по време на разработката и неправилните конфигурации на системата се определят като нарушение или уязвимости, причинени от неправилно разработени или конфигурирани ИТ активи или бизнес процеси (неподходящи спецификации на ИТ продукти, неадекватна използваемост, несигурни интерфейси, неправилни политики и потоци от процедури, грешки при проектирането).

TT3. Използване на ненадеждни ресурси

Използването на ненадеждни ресурси се определя като дейност, която води до непреднамерени щети, дължащи се на неправилно определени доверителни отношения, като например доверие в доставчик — трето лице без достатъчна осигуреност.

3.1 *Неправилно използване или конфигуриране на компоненти на портфейла*

Неправилното използване или конфигуриране на компонентите на портфейла се определя като неволно увреждане на компонентите на портфейла поради неправилно използване или неправилно конфигуриране от ползватели на портфейла или от недостатъчно обучени разработчици, или поради липса на приспособяване към промените в контекста на заплахите — обикновено използването на уязвими компоненти на трети страни или платформи за изпълнение.

ТТ4. Срив и прекъсвания

4.1 *Срив или затруднения във функционирането на оборудване, устройства или системи*

Повреда или нарушение на оборудване се определя като непреднамерена повреда на ИТ активи поради повреда или нарушение на оборудване, включително инфраструктурата на доставчика и потребителските устройства.

4.2 *Загуба на ресурси*

Загубата на ресурси се определя като прекъсване или нарушение поради липса на такива ресурси, например като части за поддръжка.

4.3. *Загуба на помощни услуги*

Загубата на помощни услуги се определя като прекъсване или нарушение поради липса на помощни услуги, необходими за правилното функциониране на системата, включително мрежова свързаност на инфраструктурата на доставчика и на потребителското устройство.

ТТ5. Злонамерени действия

5.1 *Прихващане на информация*

Прихващането на информация се определя като събиране на информация, защитена по неподходящ начин при предаването, включително атаки „човек по средата“.

5.2 *Фишинг и спуфинг*

Фишингът се определя като събиране на информация, предоставена от ползвателя след измамно взаимодействие, често свързано с подправяне на законни средства за комуникация и уебсайтове. Тези заплахи са насочени към ползвателя и обикновено допринасят за Кражба на самоличност (R4) и Неразрешени трансакции (R9), често пъти чрез Кражба на данни (R5) или Разкриване на данни (R6).

5.3 *Повторно възпроизвеждане на съобщения*

Повторното възпроизвеждане на съобщения се определя като повторно използване на прихванати преди това съобщения за извършване на неразрешени трансакции, често на равнище протокол. Тази техническа заплаха основно допринася за неразрешени трансакции, които след това могат да доведат до други рискове, в зависимост от трансакцията.

5.4 *Атака с груба сила*

Атаката с груба сила се определя като нарушение на сигурността, често на поверителността, чрез извършване на голям брой взаимодействия до тогава, докато отговорите предоставят ценна информация.

5.5 *Уязвимости на софтуера*

Заплахата, свързана с уязвимостите на софтуера, е нарушение на сигурността чрез използване на уязвимост на софтуера в компонентите на портфейла или в софтуерните и хардуерните компоненти, използвани при изпълнението на портфейла, включително публикувани уязвимости и непубликувани (от същия ден) уязвимости.

5.6 *Атаки по веригата на доставки*

Атаката по веригата на доставки се определя като нарушение на сигурността чрез атаки, извършени срещу доставчика на доставчика на портфейла или на неговите ползватели с цел да се предостави възможност за по-нататъшни атаки срещу самия портфейл.

5.7 *Зловреден софтуер*

Зловредният софтуер се определя като нарушение на сигурността чрез зловредни приложения, извършващи нежелани и незаконосъобразни действия върху портфейла.

5.8 *Прогнозиране на произволни числа*

Прогнозиране на произволни числа се определя като разрешаване на груби атаки чрез частично или пълно прогнозиране на генерирани произволни числа.

РАЗДЕЛ IV

Заплахи за портфейлите

В този последен раздел се представя набор от типични сценарии на заплаха, специфични за портфейлите, които са съпоставени с основни свързани рискове на високо ниво, посочени по-горе. В този списък се посочват заплахи, които трябва да бъдат обхванати, но той не представлява изчерпателен списък от заплахи, а това зависи до голяма степен от архитектурата на избраното технологично решение за портфейла и от развитието на средата на заплахите. Освен това в оценката на риска и предложените мерки доставчикът на портфейла може да носи отговорност само за тези компоненти, които попадат в обхвата на сертифицирането (*).

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR1	Атакуващият може да отмени псевдоними без основателна причина.	Създаване или използване на фалшива електронна самоличност (R2)
TR2	Атакуващият може да издаде изфабрикувани електронни самоличности, които не съществуват.	Създаване или използване на фалшива електронна самоличност (R2)
TR3	Атакуващият може да започне да издава неразрешени ДИЛ (данни за идентификация на лица).	Създаване или използване на фалшива електронна самоличност (R2)
TR4	Атакуващият може да накара администратор да въведе грешен доставчик на ДИЛ в списъка с надеждни доставчици на ДИЛ.	Създаване или използване на фалшива електронна самоличност (R2)
TR5	Атакуващият може да заобиколи услугата за проверка на самоличност от разстояние.	Създаване или използване на съществуваща електронна самоличност (R1)/ Създаване или използване на фалшива електронна самоличност (R2)
TR6	Атакуващият може да заобиколи услугата за проверка на физическата самоличност.	Създаване или използване на съществуваща електронна самоличност (R1)/ Създаване или използване на фалшива електронна самоличност (R2)
TR7	Атакуващият може да заобиколи услугите за проверка на самоличността, свързани с използването на (квалифицирано) удостоверение от разстояние.	Създаване или използване на съществуваща електронна самоличност (R1)/ Създаване или използване на фалшива електронна самоличност (R2)
TR8	Атакуващият може да получи достъп до портфейл, който не е обвързан с дадено лице.	Създаване или използване на съществуваща електронна самоличност (R1)/ Създаване или използване на фалшива електронна самоличност (R2)
TR9	Атакуващият може да справи с технически и процедурни проверки, за да създаде погрешни ДИЛ.	Създаване или използване на съществуваща електронна самоличност (R1)/ Създаване или използване на фалшива електронна самоличност (R2)
TR10	Атакуващият може да активира нов портфейл на невалидно ЗКУП.	Създаване или използване на съществуваща електронна самоличност (R1)/ Създаване или използване на фалшива електронна самоличност (R2)
TR11	Атакуващият може да използва няколко услуги за проверка на самоличността, свързани с използването на съществуващи средства за електронна идентификация.	Създаване или използване на съществуваща електронна самоличност (R1)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)
TR12	Атакуващият може да заобиколи проверката от страна на доставчика на ДИЛ дали портфейлът се контролира от ползвателя и дали в компрометиран портфейл под контрола на атакуващия има издадени ДИЛ.	Създаване или използване на съществуваща електронна самоличност (R1)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR13	Атакуващият може да въведе валидни ДИЛ в невалиден портфейлен блок.	Създаване или използване на съществуваща електронна самоличност (R1)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)
TR14	Доставчик на ДИЛ може да издава изфабрикувани самоличности, когато самоличността е свързана със съществуващо лице.	Създаване или използване на съществуваща електронна самоличност (R1)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)
TR15	Атакуващият може да свърже ДИЛ с грешен портфейл, защото доставчикът на ДИЛ не може да свърже ДИЛ с правилния портфейл.	Създаване или използване на съществуваща електронна самоличност (R1)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)
TR16	Атакуващият може да накара ползвателя да одобри активирането на нов портфейлен блок/нова инстанция на портфейла под контрола на атакуващия — с последващ контрол и върху удостоверенията.	Създаване или използване на съществуваща електронна самоличност (R1)/Създаване или използване на фалшива електронна самоличност (R2)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)
TR17	Атакуващият може да издаде ДИЛ на друга държава за достъп до данни/цифрови активи на целеви граждани.	Създаване или използване на съществуваща електронна самоличност (R1)/Кражба на самоличност (R4)/Неразрешена трансакция (R9)
TR18	Атакуващият може да справи с технически и процедурни проверки, за да създаде фалшиви (К)ЕУА ((квалифицирани) електронни удостоверения за атрибути).	Създаване или използване на фалшиви атрибути (R3)
TR19	Атакуващият може да представи (К)ЕУА, които не са валидно издадени на него.	Създаване или използване на фалшиви атрибути (R3)
TR20	Атакуващият може да атакува механизма на портфейла за криптографско свързване между ДИЛ и (К)ЕУА, което не е следвало да му се издава.	Създаване или използване на фалшиви атрибути (R3)
TR21	Атакуващият може да използва (К)ЕУА в портфейл, въпреки че физическият аналог на (К)ЕУА е изтекъл или е невалиден.	Създаване или използване на фалшиви атрибути (R3)
TR22	Атакуващият може да заобиколи проверката от страна на доставчика на (К)ЕУА дали портфейлът се контролира от ползвателя и да получи издадени (К)ЕУА в компрометиран портфейл под контрола на атакуващия.	Създаване или използване на фалшиви атрибути (R3)
TR23	Атакуващият може да фалшифицира електронни удостоверения за атрибути.	Създаване или използване на фалшиви атрибути (R3)
TR24	Атакуващият може да въведе в портфейла фалшифицирани електронни удостоверения за атрибути.	Създаване или използване на фалшиви атрибути (R3)
TR25	Портфейл може да представи атрибути на доверяваща се страна, без одобрението на ползвател.	Разкриване на данни (R6)
TR26	ДИЛ, (К)ЕУА или псевдоними може да бъдат представени на погрешна доверяваща се страна.	Разкриване на данни (R6)
TR27	Атакуващият може да инициира зловредно подновяване на ЕУА.	Разкриване на данни (R6)
TR28	Атакуващият може да накара ползвател да одобри неправомерно искане за електронни удостоверения за атрибути (фишинг или други).	Разкриване на данни (R6)

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR29	Атакуващият може да разкрие атрибути от портфейла и да идентифицира ползвателя на портфейла, когато идентификацията не е необходима/разрешена.	Разкриване на данни (R6)
TR30	Атакуващият може да се справи с технически и процедурни проверки, за да извлече данни.	Разкриване на данни (R6)
TR31	Искане може да бъде разкрито на атакуващ.	Разкриване на данни (R6)
TR32	Атакуващият може да получи информация за включената политика за оповестяване за атрибути и да представя атрибути, съдържащи се в текущото искане от портфейлни блокове.	Разкриване на данни (R6)
TR33	Атакуващият може да извлича регистрационни файлове или части от тях.	Разкриване на данни (R6)
TR34	Атакуващият може да знае дали портфейлът е инсталиран на същото устройство, което използва, или на друго, и да получи информация за него.	Разкриване на данни (R6)
TR35	Атакуващият може да получи елемент на знанието, използван за удостоверяване на автентичността на ползвателя към ЗКПП.	Разкриване на данни (R6)
TR36	Електронното удостоверение за атрибути за лице, което е представено в множество трансакции с доверяваща се страна или между различни доверяващи се страни, неволно позволява свързването на множество трансакции със съответното лице.	Разкриване на данни (R6)
TR37	Списъкът за отмяна на публично удостоверение/доверяваща се страна може да съдържа информация относно използването на удостоверенията от ползвателя (например местоположение, IP адрес…).	Разкриване на данни (R6)
TR38	Тъй като не могат да докажат съгласието на ползвателя за споделени атрибути, доверяващите се страни могат да повлияят на целостта на регистрационните файлове.	Разкриване на данни (R6)
TR39	Атакуващият може незаконно да проследи ползвателите на портфейла, като използва уникални/проследими идентификационни кодове.	Разкриване на данни (R6)/Следене (R14)
TR40	Доверяваща се страна, състояща се от множество модули/субекти, всеки от които има различен обхват във връзка с това, което им е разрешено да изискват/обработват, може да изисква и обработва данни, за които не притежава законово основание.	Разкриване на данни (R6)/Неразрешена трансакция (R9)
TR41	Атакуващият може да изопачи проверките за целостта и автентичността от портфейла на ДИЛ, за да бъдат те винаги успешни.	Манипулиране на данни (R7)
TR42	Атакуващият може да заобиколи или изопачи изпълнението на проверките от портфейла, с които се проверява целостта и автентичността на поисканите атрибути, за да бъдат те винаги успешни.	Манипулиране на данни (R7)
TR43	Атакуващият може да заобиколи или изопачи изпълнението на проверките от портфейла, с които се проверяват всички поискани атрибути, принадлежащи на същия ползвател, за да бъдат те винаги успешни.	Манипулиране на данни (R7)
TR44	Атакуващият може да заобиколи или изопачи изпълнението на проверките от портфейла, с които се проверява дали ДИЛ са валидни и издадени от доверен доставчик на ДИЛ, за да бъдат те винаги успешни.	Манипулиране на данни (R7)

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR45	Атакуващият може да заобиколи или изопачи изпълнението на проверките от портфейла, с които се проверява дали КЕУА е валидно и издадено от квалифициран доставчик на удостоверителни услуги, регистриран да издава КЕУА, за да бъдат те винаги успешни.	Манипулиране на данни (R7)
TR46	Атакуващият може да заобиколи или изопачи изпълнението на проверките от портфейла, с които се проверява дали ДИЛ може да бъдат отменени от страна на доставчика на ДИЛ, за да бъдат те винаги успешни.	Манипулиране на данни (R7)
TR47	Атакуващият може да заобиколи или изопачи изпълнението на проверките от портфейла, с които се проверява дали (К)ЕУА е било отменено от страна на доставчика на (К)ЕУА, за да бъдат те винаги успешни.	Манипулиране на данни (R7)
TR48	Атакуващият може да измени съдържанието на данните за архивиране и възстановяване, които трябва да бъдат изключително под контрола на ползвателя.	Манипулиране на данни (R7)/Загуба на данни (R8)
TR49	Атакуващият може да промени историята на трансакциите за дадена инстанция на портфейла от регистрационните файлове на дейността.	Манипулиране на данни (R7)/Загуба на данни (R8)
TR50	Атакуващият може да подслушва по време на връзката от портфейла към доверяващите се страни.	Кражба на данни (R5)/Разкриване на данни (R6)
TR51	Атакуващият може да убеди ползвател да сподели лични данни (например ДИЛ, ЕУА, псевдоними, електронни подписи, регистрационни файлове и други данни) с атакуващия или с трета страна, които ползвателят не е възнамерявал да споделя.	Кражба на данни (R5)/Разкриване на данни (R6)
TR52	Атакуващият може да прочете историята на трансакциите за дадена инстанция на портфейла от регистрационните файлове на дейността.	Кражба на данни (R5)/Разкриване на данни (R6)
TR53	Атакуващият може да експортира или извлича материал за криптографски ключове извън ЗКУП.	Кражба на данни (R5)/Разкриване на данни (R6)/Неразрешена трансакция (R9)
TR54	Атакуващият може да прочете съдържанието на данните за архивиране и възстановяване, които трябва да бъдат изключително под контрола на ползвателя.	Кражба на данни (R5)/Разкриване на данни (R6)
TR55	Атакуващият може да заобиколи метода за удостоверяване на автентичността на ползвателя, за да използва псевдоним, генериран от портфейлен блок.	Кражба на самоличност (R4)
TR56	Атакуващият може да предложи на ползвателите приложение, което имитира конкретен легитимен портфейл.	Кражба на самоличност (R4)
TR57	Атакуващият може да експортира данни от портфейла, включително ДИЛ, (К)УЕА или регистрационни файлове.	Кражба на самоличност (R4)
TR58	Атакуващият може да експортира криптографски обвързващ материал.	Кражба на самоличност (R4)
TR59	Атакуващият може да придобие самоличност чрез криптографските ключове на портфейла.	Кражба на самоличност (R4)
TR60	Атакуващият може да направи дубликат на портфейлния блок на личен портфейл на друг ползвател на личното му устройство и да го използва.	Кражба на самоличност(R4)/ Създаване или използване на съществуваща електронна самоличност (R1)

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR61	Органите на друга държава могат да поискат от ползвателя да покаже и/или сподели всички данни от портфейла в ситуация на близост, като например при пресичане на границата на тази държава.	Кражба на самоличност (R4)/Следене (R14)
TR62	Ползвателите не могат да прехвърлят своите регистрационни файлове за трансакции след срив на потребителско устройство, което води до загуба на проследимост на предишни трансакции в новия портфейл.	Отказ (R11)
TR63	Ползвателите не могат да възстановят своите регистрационни файлове за трансакции след срив на потребителско устройство, което води до загуба на проследимост на новия портфейл.	Отказ (R11)
TR64	Доверяващите се страни могат да срещнат трудности при доказване на съгласие за електронни подписи от разстояние.	Отказ (R11)
TR65	Атакуващият може да „наводни“ връзката(ите) с искания по време на свързването с доверяващите се страни.	Прекъсване на услугата (R13)
TR66	Атакуващият може да „наводни“ услуга за предоставяне на статус с връзки към доверяващите се страни.	Прекъсване на услугата (R13)
TR67	Атакуващият може да направи така, че представянето на атрибута да се показва като оспорено/отказано, макар че при представянето на атрибута се посочва неговата валидност.	Прекъсване на услугата (R13)
TR68	Атакуващият може да отмени ДИЛ без основателна причина.	Прекъсване на услугата (R13)
TR69	Атакуващият може да отмени ДИЛ без съгласието на ползвателя.	Прекъсване на услугата (R13)
TR70	Атакуващият може да отмени (К)ЕУА без основателна причина.	Прекъсване на услугата (R13)
TR71	Атакуващият може да отмени (К)ЕУА без съгласието на ползвателя.	Прекъсване на услугата (R13)
TR72	Атакуващият може да задейства множество искания за идентификация, без те да бъдат разпознати като умишлено осиротели искания.	Прекъсване на услугата (R13)
TR73	Атакуващият може да изпрати множество искания без последваща трансакция.	Прекъсване на услугата (R13)
TR74	Атакуващият може да предостави възможност на доверяващата се страна да поиска идентификация без съответстваща идентификация (отговор) и пълен контрол.	Прекъсване на услугата (R13)
TR75	Атакуващият може да изпрати отговор на искане след ситуация на изчакване или подобни ситуации, водещи до прекъсване на услугата.	Прекъсване на услугата (R13)
TR76	Доверяваща се страна може да изпрати множество невалидни искания.	Прекъсване на услугата (R13)
TR77	Атакуващият може да изпрати множество невалидни искания на доставчик на портфейл.	Прекъсване на услугата (R13)
TR78	Атакуващият може да отнеме способността на държава членка да отхвърли ненадежден доставчик на ДИЛ от доверения списък на доверените доставчици на ДИЛ.	Прекъсване на услугата (R13)
TR79	Атакуващият може да предотврати спирането или отнемането на портфейл.	Прекъсване на услугата (R13)

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR80	Атакуващият може да блокира трансакции на доверяващите се страни, ползватели и/или доставчик на ДИЛ.	Прекъсване на услугата (R13)
TR81	Атакуващият може да деактивира или да направи недостъпно ЗКУП.	Прекъсване на услугата (R13)
TR82	Атакуващият може да отнеме възможността на доставчика на ДИЛ да отмени или спре ДИЛ.	Прекъсване на услугата (R13)/Неразрешена трансакция (R9)
TR83	Доверяваща се страна може да извлече данни за самоличността на ползвателя от данни, различни от споделените с тях.	Следене (R14)
TR84	Група от заговорничещи доверяващи се страни или доставчици на ДИЛ може да извлече данни за самоличността на ползвателя от данни, различни от тези, които са им известни.	Следене (R14)
TR85	Атакуващият може да проследи и открие ползвател, като използва данните за идентификация на лице на ползвателя, когато не се изисква идентифициране на ползвателя.	Следене (R14)
TR86	Атакуващият може да комбинира „подправено“ представяне на комбинации от (K)EYA.	Манипулиране на трансакции (R10)
TR87	Атакуващият може да активира/превземе портфейла от разстояние (например банково приложение с включено искане за удостоверяване на автентичността или за удостоверение) без изричното съгласие или самостоятелния контрол от страна на ползвателя, в ситуации, в които ползвателят не знае (например се намира в спящ режим) или не може да вижда доверяващата се страна.	Манипулиране на трансакции (R10)
TR88	Атакуващите могат да правят промени в метаданните на искането (име на услугата, употреби и др.).	Манипулиране на трансакции (R10)
TR89	Атакуващите могат да правят промени в информацията за отговор (състояние на услугата, еднократен код и др.).	Манипулиране на трансакции (R10)
TR90	Атакуващите могат да правят промени в информацията за атрибутите на искането (прекомерно запитване и др.).	Манипулиране на трансакции (R10)
TR91	Доверяваща се страна може да възпроизвежда елементи от предишна сесия в друга сесия.	Манипулиране на трансакции (R10)
TR92	Атакуващият може да замени или измени ДИЛ по време на прехвърлянето им от доставчика на ДИЛ до портфейлния блок.	Манипулиране на трансакции (R10)
TR93	Атакуващият може да замени или измени ДИЛ по време на прехвърлянето им от портфейлния блок към онлайн доверяващата се страна.	Манипулиране на трансакции (R10)
TR94	Атакуващият може да замени или измени ДИЛ по време на прехвърлянето им от портфейлния блок към офлайн доверяващата се страна.	Манипулиране на трансакции (R10)
TR95	Атакуващият може да издаде ДИЛ без съгласието на ползвателя.	Неразрешена трансакция (R9)
TR96	Атакуващият може да използва отменени или невалидни включени политики за оповестяване, вероятно без знанието на доверяващите се страни.	Неразрешена трансакция (R9)
TR97	Атакуващият може да заблуди портфейла да провери грешни електронни подписи.	Неразрешена трансакция (R9)
TR98	Атакуващият може да използва портфейла извън контрола на ползвателя.	Неразрешена трансакция (R9)

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR99	Атакуващият може да убеди ползвателя да удостовери автентичността и одобри трансакции с атакуващ или неупълномощена трета страна.	Неразрешена трансакция (R9)
TR100	Атакуващият може да накара ползвателя да подпише по електронен път, без да представя съдържанието на ползвателя или след като е представил грешно съдържание.	Неразрешена трансакция (R9)
TR101	Атакуващият може да заобиколи контрола на достъпа до профила на ползвателя при доставчика на портфейла.	Неразрешена трансакция (R9)
TR102	Атакуващият може да се представи за доверяващи се страни по време на осъществяване на връзката с доверяващи се страни.	Неразрешена трансакция (R9)/Разкриване на данни (R6)
TR103	Ползвателят зад връзката между доверяващата се страна и браузъра може да е различен от ползвателя зад връзката между доверяващата се страна и портфейла.	Неразрешена трансакция (R9)/Разкриване на данни (R6)/Кражба на самоличност (R4)
TR104	Атакуващият може да убеди ползвателя да отмени портфейла на ползвателя без причина.	Неразрешена трансакция (R9)/Прекъсване на услугата (R13)
TR105	Атакуващият може да извърши атаки „човек в средата“.	Неразрешена трансакция (R9)/Разкриване на данни (R6)/Следене (R14)
TR106	Атакуващият може да представи невалидни или отменени атрибути от портфейл, който не се свързва редовно с мрежата.	Ефект върху различни рискове
TR107	Атакуващият може да открадне информация от ползвателя чрез спуфинг на портфейл.	Ефект върху различни рискове
TR108	Атакуващият може да се представя за ползвателя, като повтори/имитира искане за данни (например удостоверяване на автентичността), която ще изглежда като валидна.	Ефект върху различни рискове
TR109	Атакуващият може да възпроизведе включена политика за оповестяване спрямо ползвател, за да имитира одобрено искане.	Ефект върху различни рискове
TR110	Атакуващият може да използва липсата на информация за ползвателите на портфейла или неоправдани забавяния след пробив или компрометиране на сигурността.	Ефект върху различни рискове
TR111	Атакуващият може да измени предварително инсталирана легитимна инстанция на портфейла, за да добави зловредни функции.	Ефект върху различни рискове
TR112	Атакуващият може да измени легитимна инстанция на портфейла и да я предложи на ползвателите като легитимна.	Ефект върху различни рискове
TR113	Атакуващият може да се справи със самия механизъм за удостоверяване на автентичността на ползвателя, за да заобиколи удостоверяването на автентичността на ползвателя на портфейла.	Ефект върху различни рискове
TR114	Атакуващият може да въведе зловреден код или задни вратички в кода на портфейла по време на внедряването му на потребителското устройство.	Ефект върху различни рискове
TR115	Атакуващият може да въведе зловреден код или задни вратички в кода на портфейла по време на разработването му.	Ефект върху различни рискове
TR116	Атакуващият може да подмени генерирането на произволни числа, за да намали достатъчно тяхната ентропия с цел да позволи атаки.	Ефект върху различни рискове

Идентификационен номер *Идентификационен код*	Описание на заплахата *Описание на установената заплаха(*)*	Наименование на риска *Свързани рискове*
TR117	Атакуващият може да подмени потребителските устройства във веригата за доставки, за да включи код или конфигурации, които не отговарят на условията за използване на портфейла.	Ефект върху различни рискове
TR118	Атакуващият може да активира устройство за портфейл, докато използва подправено ЗКУП, контролирано от атакуващите.	Ефект върху различни рискове
TR119	Атакуващият може да прочете информацията, изпратена на ЗКПП и/или на ЗКУП.	Ефект върху различни рискове
TR120	Атакуващият може да изпрати произволна информация на ЗКПП.	Ефект върху различни рискове
TR121	Атакуващият може да открадне информация чрез прихващане на обмен между ЗКПП и ЗКУП.	Ефект върху различни рискове
TR122	Атакуващият може да изпрати произволна информация на ЗКУП.	Ефект върху различни рискове
TR123	Атакуващият може да изпрати информация до ЗКУП, като заобикаля ЗКПП.	Ефект върху различни рискове
TR124	Атакуващият може да използва фишинг, за да накара ползвателите да стигнат до фалшив портфейл и уеб приложение за управление на ДИЛ.	Ефект върху различни рискове
TR125	Атакуващият може да замени ключовете на портфейла с други ключове, за да създаде съобщения, които да бъдат използвани в друга атака.	Ефект върху различни рискове
TR126	Атакуващият може да измени или унищожи ключовете на портфейла, правейки някои функции на портфейла неизползваеми.	Ефект върху различни рискове
TR127	Атакуващият може да контролира зловреден софтуер за достъп до данни, съхранявани в портфейла.	Ефект върху различни рискове
TR128	Атакуващият може да получи достъп до събраните в портфейла доказателства.	Ефект върху различни рискове
TR129	Доставчици на портфейли могат да получат достъп до обекти в портфейла.	Ефект върху различни рискове
TR130	Доставчици на портфейли могат да получат достъп до събраните в портфейла доказателства.	Ефект върху различни рискове
TR131	Атакуващият може да открадне незаключено устройство на портфейл.	Ефект върху различни рискове
TR132	Атакуващият може да манипулира система, за да предотврати регистрирането на определени събития.	Ефект върху различни рискове
TR133	Атакуващият може да прихване комуникацията между инстанцията на портфейла и ЗКПП или да възпроизведе/имитира ползвател (например чрез отвличане на механизъм за удостоверяване на автентичността).	Ефект върху различни рискове

ПРИЛОЖЕНИЕ II

КРИТЕРИИ ЗА ОЦЕНКА НА ПРИЕМЛИВОСТТА НА ИНФОРМАЦИЯТА ВЪВ ВРЪЗКА С ОСИГУРЕНОСТТА

Наименование	Предмет	Въпроси, на които следва да се обръща внимание
ЕССК	ИКТ продукти	Информация за издателя: няма (акредитирани сертифициращи органи) Информация за обхвата: — Проверете защитния профил и целевото ниво на сигурност — Проверете оценката на нивото на осигуреност и разширения Информация за осигуреността: — Проверете ограниченията в документацията на ползвателя — За композиция може да се изисква достъп до технически доклад за оценка
Европейска схема за сертифициране на киберсигурността за облачни услуги (EUCS) (когато е налична)	Услуги в облак	Информация за издателя: няма (акредитирани сертифициращи органи) Информация за обхвата: — Проверете описанието на услуги в облак — Проверете нивото на оценка и профилите на разширение Информация за осигуреността: — Проверете информацията относно прозрачността и, ако е необходимо, състава на информацията
Основани на общи критерии схеми, управлявани в ЕС, включително схеми на Групата на висшите служители по сигурността на информационните системи (SOG-IS)	ИКТ продукти	Информация за издателя: няма (държави членки) Информация за обхвата: — Проверете защитния профил и целевото ниво на сигурност — Проверете оценката на нивото на осигуреност и разширения Информация за осигуреността: — Проверете ограниченията в документацията на ползвателя — За композиция може да се изисква достъп до технически доклад за оценка
EN 17640:2018 (FITCEM, включително CSPN, BSZ, LINCE, BSZA)	ИКТ продукти	Информация за издателя: — Проверете схемата и изискванията за сертифициращите органи Информация за обхвата: — Проверете описанието на продукта — Проверете исканията във връзка със сигурността — Проверете нивото на осигуреност Информация за осигуреността: — Проверете извършените дейности и констатациите в доклада
Схеми за сертифициране на устройства за създаване на квалифицирани подписи съгласно член 30 от Регламент (ЕС) № 910/2014	УСКП	Информация за издателя: — Проверете схемата и изискванията за сертифициращите органи Информация за обхвата: — Проверете описанието на продукта — Проверете исканията във връзка със сигурността — Проверете нивото на осигуреност Информация за осигуреността: — Проверете извършените дейности

Наименование	Предмет	Въпроси, на които следва да се обръща внимание
EN ISO/IEC 27001:2022 Оценяване на съответствието	ISMS	Информация за издателя: няма (акредитирани сертифициращи органи) Информация за обхвата: — Проверете описанието на системата за управление — Проверете декларацията за приложимост Информация за осигуреността: — Проверете извършените дейности
SOC2	Организации	Информация за издателя: — Проверете техния статус на публичен счетоводител Информация за обхвата: — Проверете декларацията за управление и описанието на проверките — Проверете декларацията за приложимост Информация за осигуреността: — Проверете констатациите в доклада — Проверете свързващите писма, ако е необходимо
MDSCert (GSMA) (когато е налично)	Мобилни устройства	Информация за издателя: — Проверете изискванията за сертифициращите органи Информация за обхвата: — Проверете нивото на осигуреност във връзка със сигурността — Проверете изискванията на схемата Информация за осигуреността: — Проверете дейностите и констатациите в доклада
Други схеми	Всеки компонент	Информация за схемата: — Проверете уместността и разпоредбите на схемата Информация за издателя: — Проверете изискванията за сертифициращите органи Информация за обхвата: — Проверете изискванията на схемата — Проверете целевото ниво на сигурност или подобен документ, описващ функционалните изисквани за сигурност и изискванията за осигуреност — Проверете описанието на продуктите и избраните функционални изисквания за сигурност Информация за осигуреността: — Проверете дейностите и констатациите в доклада

ПРИЛОЖЕНИЕ III

ФУНКЦИОНАЛНИ ИЗИСКВАНИЯ ЗА ТЕХНОЛОГИЧНИТЕ РЕШЕНИЯ ЗА ПОРТФЕЙЛ

Съгласно член 5a, параграфи 4, 5, 8 и 14 от Регламент (ЕС) № 910/2014 функционалните критерии, на които трябва да отговаря сертифицирано технологично решение за портфейл, и схемата за електронна идентификация, съгласно която то се предоставя, включват функционалните изисквания за операциите, изброени в посочените по-долу:

1) Регламент за изпълнение (ЕС) 2024/2979 на Комисията ([1]) за определяне на правила за прилагането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета по отношение на целостта и основните функции;

2) Регламент за изпълнение (ЕС) 2024/2982 на Комисията ([2]) 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;

3) Регламент за изпълнение (ЕС) 2024/2977 на Комисията ([3]) 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.

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

([2]) 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: https://eur-lex.europa.eu/eli/reg_impl/2024/2982/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: https://eur-lex.europa.eu/eli/reg_impl/2024/2977/oj).

ПРИЛОЖЕНИЕ IV

МЕТОДИ И ПРОЦЕДУРИ ЗА ДЕЙНОСТИ ПО ОЦЕНКА

1. **Одит на изпълнението на технологично решение за портфейл**

Дейността по оценка на съответствието се състои в избор на специфични дейности по оценка.

В националните схеми за сертифициране се определя дейност по оценка за оценка на предоставената информация, която обхваща най-малко следното:

а) анализ на предоставената информация, за да се потвърди, че е подходяща за една от архитектурите, посочени в националните схеми за сертифициране;

б) анализ на обхвата на рисковете и заплахите за киберсигурността, установени в регистъра на рисковете от приложение I, чрез описаните проверки на сигурността.

Посоченият в букви а) и б) анализ се основава на обосновката и аргументацията, предоставени от доставчика на портфейла.

2. **Оценка на дейностите, свързани със защитеното криптографско устройство на портфейла**

1) Не се изисква цялостно изпълнение в ЗКУП на операциите от критично значение, включително криптографските изчисления. Тази част обаче, която се изпълнява в ЗКУП, когато функционира като част от технологичното решение за портфейла, гарантира защитата на операциите от критично значение, които извършва, срещу атаки от атакуващи с голям потенциал за атаки в съответствие с Регламент за изпълнение (ЕС) 2015/1502 на Комисията ([1]).

2) ЗКУП или част от него може да бъде в рамките на обекта на сертифициране, когато е предоставен от притежателя на сертификата или заявителя, или да попада извън неговия обхват, когато е включен в устройство, предоставено от крайния ползвател. Освен това в националните схеми за сертифициране се определят дейностите по оценка за проверка на пригодността на ЗКУП в следните два случая:

   а) ако ЗКПП зависи от конкретното ЗКУП (т.е. ако трябва да бъде оценен като съставен продукт, базиран на ЗКУП), тогава оценката на ЗКПП ще изисква достъп до допълнителна информация, свързана със сертифицирането на ЗКУП, включително по-специално неговия доклад за техническа оценка;

   б) ако дадена архитектура, разглеждана в схемата, използва няколко ЗКУП или ако някои от операциите на критични активи се извършват извън ЗКУП, тогава националните схеми за сертифициране включват дейности по оценка, за да се гарантира, че цялостното решение предлага очакваното равнище на сигурност.

(3) Като предпоставка за сертифициране съгласно национални схеми за сертифициране, ЗКУП се оценява спрямо изискванията за ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502.

а) Когато са изпълнени условията на член 3, параграф 3, буква б), оценката на ЗКУП или на част от него включва оценка на уязвимостта, както е определено в EN ISO/IEC 15408-3:2022 на ниво AVA_VAN.5, съгласно посоченото в приложение I към Регламент за изпълнение (ЕС) 2024/482 на Комисията ([2]), освен ако не е надлежно обосновано пред органа за сертифициране, че характеристиките за сигурност на ЗКПП позволяват да се използва по-ниско ниво на оценка, като същевременно се поддържа същото общо ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502.

([1]) 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).

([2]) Регламент за изпълнение (ЕС) 2024/482 на Комисията от 31 януари 2024 година за определяне на правила за прилагането на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета по отношение на приемането на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) (ОВ L, 2024/482, 7.2.2024 г., ELI: https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj).

4) Освен това по отношение на свързаната с всяка конкретна архитектура документация в националните схеми за сертифициране се формулират допускания за тази оценка на ЗКУП, при които може да се осигури устойчивост срещу атакуващи с голям потенциал за атаки в съответствие с Регламент за изпълнение (ЕС) 2015/1502 и се уточняват дейностите по оценка за потвърждаване на тези допускания и за потвърждаване след издаването на сертификата, че допусканията все още са проверени. Националните схеми също така изискват от кандидатите за сертифициране да прецизират тези допускания във връзка с конкретното им прилагане и да опишат въведените мерки, за да се гарантира, че допусканията се проверяват през целия жизнен цикъл на сертифицирането.

5) Във всички случаи националните схеми за сертифициране включват дейност по оценка с цел да се провери дали наличната за ЗКУП информация във връзка с осигуреността е подходяща за целите на технологичното решение за портфейла, чрез анализ на въпросната информация, като целевото ниво на сигурност за сертификатите по ЕССК, включително следните дейности:

   а) проверка дали обхватът на оценката е подходящ, което за сертификатите по ЕССК означава например проверка дали целевото ниво на сигурност претендира за съответствие с един от препоръчаните в ЕССК защитни профили;

   б) проверка дали допусканията за операционната среда са съвместими с технологичното решение за портфейла, което например за сертификатите по ЕССК означава, че тези допускания може да бъдат намерени в целевото ниво на сигурност;

   в) проверка дали препоръките в ръководството за ползвателя или документацията са съвместими с условията, при които ЗКУП трябва да се използва в технологичното решение за портфейла;

   г) проверка, че направените в националната схема за сертифициране допускания относно ЗКУП са проверени и обхванати в информацията във връзка с осигуреността.

6) В случаите, когато някои от проверките не са напълно убедителни, националните схеми за сертифициране изискват от сертифициращите органи да определят компенсационни изисквания за защитеното криптографско приложение на портфейла (ЗКПП), базирано на ЗКУП, което да бъде включено в оценката на ЗКПП. Ако това не е възможно, националните схеми за сертифициране ще считат ЗКУП за неподходящ, което означава, че технологичното решение за портфейла няма да получи сертификат за съответствие.

3. **Оценка на дейностите, свързани със защитеното криптографско приложение на портфейла (ЗКПП)**

1) Националните схеми за сертифициране изискват ЗКПП, като част от технологично решение за портфейла, да бъде оценено спрямо изискванията за най-малко ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502.

2) Тази оценка включва оценка на уязвимостта, както е определено в EN ISO/IEC 15408-3:2022 на ниво AVA_VAN.5, съгласно посоченото в приложение I към Регламент за изпълнение (ЕС) 2024/482, освен ако не е надлежно обосновано пред органа за сертифициране, че характеристиките за сигурност на ЗКПП позволяват да се използва по-ниско ниво на оценка, като същевременно се поддържа същото общо ниво на осигуреност „високо“, както е посочено в Регламент за изпълнение (ЕС) 2015/1502.

3) Когато ЗКПП не е предоставено от доставчика на портфейла, в националните схеми за сертифициране се формулират допускания за тази оценка на ЗКПП, при които може да се осигури устойчивост срещу атакуващи с голям потенциал за атаки в съответствие с Регламент за изпълнение (ЕС) 2015/1502 и се уточняват дейностите по оценка за потвърждаване на тези допускания и за потвърждаване след издаването на сертификата, че допусканията все още са проверени. Националните схеми също така изискват от кандидатите за сертифициране да прецизират тези допускания във връзка с конкретното им прилагане и да опишат въведените мерки, за да се гарантира, че допусканията се проверяват през целия жизнен цикъл на сертифицирането.

4) Във всички случаи националните схеми за сертифициране включват дейност по оценка с цел да се провери дали наличната за ЗКПП информация във връзка с осигуреността е подходяща за целите на технологичното решение за портфейла, чрез анализ на въпросната информация, като целевото ниво на сигурност за сертификатите по ЕССК, включително следните дейности:

   а) проверка дали обхватът на оценката е подходящ, което за сертификатите по ЕССК означава например проверка дали целевото ниво на сигурност претендира за съответствие с един от препоръчаните в ЕССК защитни профили;

   б) проверка дали допусканията за операционната среда са съвместими с технологичното решение за портфейла, което например за сертификатите по ЕССК означава, че тези допускания може да бъдат намерени в целевото ниво на сигурност;

в) проверка дали препоръките в ръководството за ползвателя или документацията са съвместими с условията, при които ЗКПП трябва да се използва в технологичното решение за портфейла;

г) проверка, че направените в националната схема за сертифициране допускания относно ЗКПП са проверени и обхванати в информацията във връзка с осигуреността.

5) Националните схеми за сертифициране изискват оценката на ЗКПП да обхваща всички проверки за сигурност, прилагани от това ЗКПП.

4. **Оценка на дейностите, свързани с устройството на краен ползвател**

Тъй като в регистъра на рисковете, както е посочено в приложение I към настоящия регламент, се идентифицират рискове, които са пряко свързани със сигурността на устройството на крайния ползвател, националните схеми за сертифициране определят изискванията за сигурност на устройствата на крайния ползвател. Тъй като обаче тези устройства се предоставят от крайния ползвател, а не от доставчика на портфейла, тези изисквания се покриват от допускания.

За всяко допускане технологичното решение за портфейла включва механизъм за проверка за всеки портфейлен блок дали основното устройство на крайния ползвател отговаря на допускането. Такива механизми се считат за проверки на сигурността и се обхващат от дейности по оценка, за да се докаже както тяхната пригодност, така и тяхната ефективност при подходящо равнище на сигурност.

По-долу са посочени два примери за това:

а) устройство на краен ползвател може да включва сертифицирано ЗКУП, което трябва да бъде доказано. Обикновено това се прави чрез използване на криптографски механизъм за проверка на наличието в сертифицираното ЗКУП на криптографска тайна, която е достъпна само в сертифицираното ЗКУП. В този случай тази криптографска тайна следва да се счита за стратегически актив и да бъде обхванатa от сертифицирането на ЗКУП и/или на ЗКПП;

б) типично изискване за устройства на краен ползвател би било задължението за получаване от устройствата на актуализации, свързани със сигурността. Тъй като това изискване е свързано с инстанцията на портфейла, използваният механизъм за проверка на наличността на свързани със сигурността актуализации трябва да бъде обхванат само от дейности по оценка на подходящо за инстанцията на портфейла ниво на осигуреност, особено поради вероятността за интегрирането му в инстанцията на портфейла.

5. **Оценка на дейностите, свързани с инстанцията на портфейла**

1) При оценката на инстанцията на портфейла се вземат предвид следните две основни промени:

а) налице е вероятност инстанцията на портфейла да съществува в набор от варианти на едно и също основно приложение, като всеки вариант е специализиран за конкретна категория устройства на крайния ползвател;

б) различните варианти на инстанцията на портфейла вероятно ще се нуждаят от чести актуализации, за да следват развитието на основната платформа за сигурност, например когато се установят уязвимости, които изискват промени в приложенията.

2) При оценката на инстанцията на портфейла се вземат предвид тези специфични предизвикателства. Една от непосредствените последици е, че рамката на общите критерии може да не е подходяща във всички случаи. Поради това, когато е необходимо се вземат предвид алтернативни методики за оценка. В националните схеми за сертифициране се обмисля използването на методиката EN 17640:2018 за следното:

а) като част от самата схема;

б) чрез национални схеми, основани на методиката;

в) чрез национални схеми, основани на подобни принципи, но създадени преди разработването на методиката EN 17640:2018.

3) Освен това, тъй като може да има ограничена добавена стойност при извършването на пълна специална оценка на всеки вариант, в националните схеми за сертифициране се обмисля уточняването на критерии, позволяващи изготвянето на извадка с цел да се избегне повторението на идентични дейности по оценка и да се постави акцент върху дейности, които са специфични по отношение на даден вариант. Националните схеми за сертифициране изискват от всички сертифициращи органи да обосноват използването на изготвянето на извадки.

4) Националните схеми за сертифициране включват актуализации на инстанцията на портфейла в общия процес на управление на промените, определен за технологичното решение за портфейла. Те също така определят правила за процедурите, които се изпълняват от доставчика на портфейла за всяка актуализация (например анализиране на въздействието на промените върху проверките за сигурност), както и за дейностите по оценка, които се извършват от сертифициращия орган за актуализации съгласно определени условия (например оценка на оперативната ефективност на изменена проверка на сигурността). Процесът на управление на промените е един от процесите, чиято оперативна ефективност трябва да се проверява ежегодно в съответствие с член 18, параграф 3.

6. **Дейности по оценка, свързани с услугите и процесите, използвани за предоставяне и управление на технологичното решение за портфейла**

1) За оценката на услугите и процесите, които играят роля в предоставянето и управлението на технологичното решение за портфейл и схемата за електронна идентификация, съгласно която то се предоставя, екипът за оценка събира доказателства чрез извършване на дейности по оценка, които могат да включват одит, инспекция, проверка и дейности по валидиране.

2) Сертифициращият орган трябва да потвърди достатъчността и уместността на доказателствата, за да предостави достатъчно ниво на осигуреност, че услугите и процесите отговарят на изискванията за сертифициране, като потвърди следното::

   а) точността на информацията, представена в описанието на процесите и услугите;

   б) пригодността на проекта и проверките на процесите и услугите да отговарят на критериите за оценка;

   в) оперативната ефективност на прилагането на тези проверки през определен период преди оценката.

3) Точността на описанието и оперативната ефективност на изпълнение на проверките могат да се считат за цели на проверката, по смисъла на ISO/IEC 17000:2020, на съответните твърдения от доставчика на портфейла (т.е. потвърждение на справедливостта на събития, които вече са възникнали или резултати, които вече са получени), като се има предвид, че пригодността на проекта и проверките на услугите и процесите, за да отговарят на критериите за оценка, може да се счита за цел на валидирането, по смисъла на ISO/IEC 17000:2020, на съответна претенция от доставчика на портфейла (т.е. потвърждение за правдоподобност по отношение на планирана бъдеща употреба или прогнозиран резултат).

(4) Като се има предвид, че технологичното решение за портфейл не може да работи, преди да бъде сертифицирано, ефективността на работа не може да бъде потвърдена въз основа на действителната работа на решението. Ето защо това се потвърждава с помощта на доказателства, събрани по време на изпитвания или пилотни проекти.

5) Национални схеми за сертифициране може вече да съществуват за конкретни услуги и процеси, например за интегриране на ползватели. Използването на такива схеми се разглежда в националните схеми за сертифициране, ако е приложимо.

7. **Дейности по оценка, свързани с услуги в областта на ИКТ, използвани за предоставяне и управление на технологичното решение за портфейла**

1) Някои архитектури на портфейли могат да разчитат на специализирани ИКТ услуги, включително услуги в облак за предоставяне и управление на технологично решение за портфейла, и тези услуги могат да хостват чувствителни данни, както и чувствителни операции. В този случай националните схеми за сертифициране определят специфични изисквания за тези ИКТ услуги.

2) Вече съществуват много схеми за сертифициране за ИКТ услуги, услуги в облак и други източници на информация за сигурност, включително изброените в приложение II. Когато тези съществуващи механизми са налични и приложими, националните схеми за сертифициране се позовават на един от следните механизми:

   а) налагане на задължително използване на конкретна схема или на набор от схеми, като се определят условията, при които ИКТ или услугите в облака трябва да бъдат оценени с помощта на тези схеми;

   б) предоставяне на избора на оценка на доставчика на портфейла и използване на дейността за анализ на зависимостта, за да се анализира пригодността на информацията за ниво на осигуреност, получена чрез тези оценки.

3) И в двата случая националните схеми за сертифициране определят допълнителни дейности по оценка, необходими за анализиране или допълване на получената чрез тези схеми информация.

ПРИЛОЖЕНИЕ V

СПИСЪК НА ПУБЛИЧНО ДОСТЪПНАТА ИНФОРМАЦИЯ ЗА ПОРТФЕЙЛИТЕ

1. Предоставяната публично информация съгласно член 8, параграф 5 включва най-малко следното:

   а) всякакви ограничения върху използването на технологично решение за портфейл;

   б) насоки и препоръки от доставчика на портфейла за подпомагане на крайните ползватели със сигурната конфигурация, инсталиране, внедряване, работа и поддръжка на портфейли;

   в) периода, през който на крайните ползватели ще бъде предложена подкрепа във връзка със сигурността, по-специално по отношение на наличността на актуализации, свързани с киберсигурността;

   г) информация за връзка с производителя или доставчика и приемливи начини за получаване на информация за уязвимостта от крайните ползватели или научните изследователи в областта на сигурността;

   д) препратка към онлайн хранилища, съдържащи списък с публично оповестени уязвимости, свързани с портфейли, и всички съответни съвети във връзка с киберсигурността.

2. Посочената в параграф 1 информация се предоставя по ясен, изчерпателен и лесно достъпен начин, на публично достъпно място за всяко лице, което иска да използва технологично решение за портфейл.

ПРИЛОЖЕНИЕ VI

МЕТОДИКА ЗА ОЦЕНКА НА ПРИЕМЛИВОСТТА НА ИНФОРМАЦИЯТА ВЪВ ВРЪЗКА С ОСИГУРЕНОСТТА

1. **Оценка на наличието на документацията във връзка с осигуреността**

Оценителите изброяват наличната документация за гарантиране на всеки съответен компонент на технологичното решение за портфейл и схемата за електронна идентификация, съгласно която то се предоставя. Впоследствие оценителите трябва да оценят цялостната уместност на всяка част от документацията за сигурност за прегледа на зависимостта.

При анализа се вземат предвид следните аспекти:

1) относно самата документация във връзка с осигуреността:

   а) вида на документацията във връзка с осигуреността, заедно с необходимите подробности,

   (примери за такива документи са сертификатите за съответствие съгласно EN ISO/IEC 27001:2022 или тип 1 или тип 2 за докладите по ISAE);

   б) обхванатия период или срока на валидност,

   (този период може да бъде допълнен със свързващо писмо (документ, обхващащ период от време между крайната дата на отчетния период на текущия доклад за ISAE и публикуването на нов доклад за ISAE) или подобно изявление);

   в) приложимата рамка (например съществуващи стандарти);

   г) дали документацията във връзка с осигуреността включва обозначаване на изискванията на схемата;

2) относно професионалната компетентност и безпристрастност на издателя на доклада за сигурността:

   а) наименование на сертифициращия орган и, ако е налично — името на водещия оценител;

   б) доказателство за компетентността на сертифициращия орган и оценителя (например акредитация, лично сертифициране и др.);

   в) доказателство за безпристрастност на сертифициращия орган и оценителя (например акредитация).

2. **Оценка на осигуреността, свързана с индивидуални изисквания**

Оценителите проверяват дали наличната документация във връзка с осигуреността за технологичното решение за портфейл и схемата за електронна идентификация, съгласно която то се предоставя, е подходяща, за да се определи дали технологичното решение за портфейл отговаря на очакванията по отношение на индивидуалните изисквания на схемата за сертифициране.

Тази оценка се извършва за всеки съответен компонент на технологичното решение за портфейл и схемата за електронна идентификация, съгласно която то се предоставя, чрез формулиране на допускане относно проверките за сигурност на технологичното решение за портфейл.

За всяко такова допускане екипът за оценка трябва да определи дали гаранцията, предоставена в наличната документация за гаранция, е подходяща.

Определянето, че въпросното допускане е подходящо, се основава на следното:

1) изискваната информация е налична, с очакваното ниво на осигуреност, в документацията във връзка с осигуреността;

2) наличната в документацията във връзка с осигуреността информация не покрива целия обхват на изискването, но допълнителни проверки или компенсиращи проверки (т.е. вътрешни проверки, които намаляват риска от съществуваща или потенциална слабост на контрола), въведени в технологичното решение за портфейла или в схемата за електронна идентификация, съгласно която то се предоставя, предоставят възможност на оценителите да определят дали информацията е подходяща;

3) наличната в документацията във връзка с осигуреността информация не предлага очакваното ниво на осигуреност, но проверките, въведени с цел оценка и наблюдение на доставчика на портфейла предоставят възможност на оценителите да определят дали тази информация е подходяща;

4) ако в документацията във връзка с осигуреността се посочват несъответствия в проекта или изпълнението на проверките, използвани за изпълнение на допускането, коригиращите действия, предложени и изпълнени от доставчика на портфейла и прегледани от неговите оценители, трябва да бъдат адекватни, за да гарантират, че допускането в действителност е изпълнено.

ПРИЛОЖЕНИЕ VII

СЪДЪРЖАНИЕ НА СЕРТИФИКАТА ЗА СЪОТВЕТСТВИЕ

1. Уникален идентификационен код, определен от сертифициращия орган, който издава сертификата за съответствие.

2. Информация, свързана със сертифицираното технологично решение за портфейл и схемите за електронна идентификация, съгласно които то се предоставя, и относно притежателя на сертификата за съответствие, включително следното:

   a) наименование на технологичното решение за портфейла;

   b) наименованието на схемата за електронна идентификация, съгласно която се предоставя технологичното решение за портфейла;

   c) версия на технологичното решение за портфейла, което е оценено;

   d) име, адрес и информация за връзка на титуляря на сертификата за съответствие;

   e) връзка към уебсайта на притежателя на сертификата за съответствие, съдържащ информацията, която се изисква да бъде публично достъпна.

3. Информация, свързана с оценката и сертифицирането на технологичното решение за портфейл и схемите за електронна идентификация, съгласно които то се предоставя, включително следното:

   а) наименование, адрес и информация за връзка на сертифициращия орган, който е издал сертификата за съответствие;

   б) когато се различава от сертифициращия орган — наименование на органа за оценка на съответствието, извършил оценката, заедно с информация за неговата акредитация;

   в) наименование на собственика на схемата;

   г) препратки към Регламент (ЕС) № 910/2014 и към настоящия регламент;

   д) препратка към доклада за сертифициране, свързан със сертификата за съответствие;

   е) препратка към доклада за оценка на сертифицирането, свързан със сертификата за съответствие;

   ж) препратка към стандартите, използвани за оценката, включително техните версии;

   з) датата на издаване на сертификата за съответствие;

   и) срока на валидност на сертификата за съответствие.

ПРИЛОЖЕНИЕ VIII

СЪДЪРЖАНИЕ НА ПУБЛИЧНИЯ ДОКЛАД ЗА СЕРТИФИЦИРАНЕТО И ДОКЛАДА ЗА ОЦЕНКА НА СЕРТИФИЦИРАНЕТО

1. Публичният доклад за сертифицирането съдържа най-малко следните аспекти:

   а) резюме;

   б) идентификация на технологичното решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя;

   в) описание на технологичното решение за портфейла и на схемата за електронна идентификация, съгласно която то се предоставя;

   г) информацията за сигурността, която трябва да бъде публично достъпна, както е посочено в приложение V, или указател към тази информация;

   д) резюме на предварителния одит и плана за валидиране;

   е) резюме на преразглеждането и решението за сертифициране.

2. Докладът за оценка на сертифицирането съдържа най-малко:

   а) описание на проекта на технологичното решение за портфейла, системата за идентификация и процеса на включване, заедно с оценката на риска и конкретния план за валидиране;

   б) описание на това как технологичното решение за портфейла отговаря на изискванията за ниво на осигуреност „високо“ и как това се доказва от резултатите от оценката на сертифицирането на технологичното решение за портфейла, извършена в съответствие с настоящия регламент;

   в) описание на резултата от оценката на съответствието на технологичното решение за портфейла и на схемата за електронна идентификация, съгласно която се предоставят съответните портфейлни блокове, по-специално съответствието със следното:

      — изискванията по член 5а, параграфи 4, 5 и 8 от Регламент (ЕС) № 910/2014;

      — изискването за логическо разделяне по член 5а, параграф 14 от Регламент (ЕС) № 910/2014;

      — когато е приложимо, стандартите и техническите спецификации, посочени в член 5а, параграф 24 от Регламент (ЕС) № 910/2014, като същевременно се посочва как тези изисквания са свързани със съответните нормативни изисквания, определени от националните схеми за сертифициране;

   г) обобщение на резултата от изпълнението на плана за валидиране, включително всички установени несъответствия.

ПРИЛОЖЕНИЕ IX

ГРАФИК ЗА ЗАДЪЛЖИТЕЛНИ НАДЗОРНИ ОЦЕНКИ

1. В член 18 се определят изискванията за жизнения цикъл на сертифицирането, по-специално извършването на редовни дейности по оценка. Тези дейности включват най-малко следното:

   а) пълна оценка на обекта на оценка на съответствието при първоначалната оценка и при всяка оценка на повторно сертифициране, включително функция за актуализиране на всеки компонент на продукта;

   б) оценка на уязвимостта при първоначалната оценка и при всяка оценка за повторно сертифициране и най-малко на всеки две години в надзорните оценки, обхващаща най-малко промените в обекта на оценка на съответствието и промените в средата на заплаха след последната оценка на уязвимостта;

   в) допълнителни дейности като изпитване за проникване в случай на повишено ниво на риск или поява на нови заплахи;

   г) оценка на оперативната ефективност на процесите на поддръжка най-малко всяка година при надзорни оценки и оценки за повторно сертифициране, обхващащи поне процеси за контрол, актуализиране и управление на уязвимостите на последната версия;

   д) след успешен преглед и решение за сертифициране, издаване на сертификат за съответствие след първоначалната оценка и след всяка оценка за повторна сертификация.

2. Референтен график е изложен в таблица 1 въз основа на 4-годишен цикъл, където:

   а) година 1 започва с първото издаване на сертификата за съответствие; и

   б) всички дейности по оценката се извършват в срок от 12 месеца от оценката за предходната година.

3. Посоченият в таблица 1 график е препоръка за осигуряване на навременна повторна сертификация и за избягване на прекъсвания в предоставянето на технологичното решение за портфейла. Възможно е да има и други графици, доколкото валидността на сертификата за съответствие не надвишава пет години, както е посочено в член 5в, параграф 4 от Регламент (ЕС) № 910/2014.

4. В допълнение към редовните оценки може да се задейства специална оценка по искане на сертифициращия орган или на притежателя на сертификата за съответствие, след значителна промяна в обекта на сертифициране или в заплахата.

5. Всяка оценка, включително надзорни оценки и специални оценки, може да доведе до издаване на нов сертификат за съответствие, по-специално в случай на значителни промени в обекта на сертифициране, но със същата дата на изтичане като тази на първоначалния сертификат за съответствие.

Таблица 1

Пълен четиригодишен цикъл на оценка

Час	Вид оценка	Дейности
Година 0	Първоначална	— Цялостна оценка на обекта на сертифициране, включително оценка на уязвимостите — Включително функция за извършване на актуализации на всеки софтуерен компонент — Оценка на процесите на поддръжка, с изключение на тяхната оперативна ефективност — Издаване на сертификат за съответствие и започване на четиригодишен цикъл —
Година 1	Надзор	— Оценка на оперативната ефективност на процесите на поддръжка — Най-малко проверка на версията, актуализацията, управлението на уязвимости — Оценка на промените, оказващи въздействие върху сигурността на продукта

Час	Вид оценка	Дейности
Година 2	Надзор	— Оценка на уязвимостта на цялостното решение — Оценка на оперативната ефективност на процесите на поддръжка — Най-малко проверка на версията, актуализацията, управлението на уязвимости — Оценка на промените, оказващи въздействие върху сигурността на продукта
Година 3	Надзор	— Оценка на оперативната ефективност на процесите на поддръжка — Най-малко проверка на версията, актуализацията, управлението на уязвимости — Оценка на промените, оказващи въздействие върху сигурността на продукта
Година 4	Повторно сертифициране	(1) Цялостна оценка на обекта на сертифициране, включително оценка на уязвимостите (2) Опростена оценка за функции/процеси, които не са променени (3) Включително функция за извършване на актуализации на всеки софтуерен компонент (4) Оценка на процесите на поддръжка, включително тяхната оперативна ефективност (5) Издаване на нов сертификат за съответствие