2025/2462

9.12.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/2462 НА КОМИСИЯТА

от 8 декември 2025 година

за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на определенията, сертифицирането на сериите ИКТ продукти, непрекъснатостта на увереността и актуалните технически документи

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид 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) ([1]), и по-специално член 49, параграф 7 от него,

като има предвид, че:

(1) С Регламент за изпълнение (ЕС) 2024/482 на Комисията ([2]) се определят ролите, правилата и задълженията, както и структурата на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК), в съответствие с европейската рамка за сертифициране на киберсигурността, установена в Регламент (ЕС) 2019/881.

(2) Общата методика за оценка, придружаваща общите критерии, представлява международен стандарт за оценка на информационната сигурност и позволява оценка на сигурността на ИКТ продуктите за целите на сертифицирането. В този контекст някои ИКТ продукти могат да бъдат изградени на една и съща функционална основа, за да предлагат сходни функционалности за сигурност на различни платформи или устройства, наричани също така серия продукти. Дизайнът, хардуерът, фърмуерът или софтуерът могат обаче да се различават при различните ИКТ продукти. Сертифициращият орган решава за всеки отделен случай дали може да се извърши сертифициране на дадена серия продукти. Условията за сертифициране на серии продукти могат да бъдат допълнително илюстрирани в подкрепа на насоките на ЕССК.

(3) За да се поддържа надеждността на сертифицираните продукти, е важно да се определи какво представлява съществена и какво — несъществена промяна в обекта на оценката или в неговата среда, включително в оперативната или развойната му среда. Поради това е необходимо да се уточнят тези понятия, като се вземат предвид съществуващите и широко използвани технически спецификации на Групата на висшите служители по сигурността на информационните системи (SOG-IS) и участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността (CCRA).

(4) Несъществените промени често се характеризират с ограниченото си въздействие върху декларацията за достоверност на продукта, предоставена от издадения сертификат по ЕССК. Поради това несъществените промени следва да се управляват в рамките на процедури за поддържане и не изискват повторна оценка на функционалностите за сигурност на продукта. Примерите за несъществени промени, които следва да бъдат разгледани чрез поддържане, включват, но не се ограничават до редакционни промени, промени в средата на обекта на оценка, които не променят сертифицирания обект на оценка, и промени в сертифицирания обект на оценка, които не засягат доказателствата за получаване на увереност. Промените в развойната среда също могат да се считат за незначителни, при условие че нямат последващо въздействие върху съществуващите мерки за увереност. В някои случаи обаче те могат да изискват частична оценка на съответните мерки.

([1]) ОВ L 151, 7.6.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

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

(5) Съществена промяна е всяка промяна в сертифицирания обект на оценка или неговата среда, която може да окаже неблагоприятно въздействие върху увереността, посочена в сертификата по ЕССК, поради което тя следва да изисква повторна оценка. Примерите за съществени промени включват, но не се ограничават до, промени в набора от декларирани изисквания за увереност, с изключение на изискванията за увереност на група CC ALC_FLR (отстраняване на дефекти); промени в проверките за поверителност или цялостност на развойната среда, когато такива изменения биха могли да засегнат сигурното разработване или производство на обекта на оценка, или промени в обекта на оценка с цел отстраняване на уязвимост, която може да бъде използвана. Освен това съвкупност от несъществени промени, които колективно оказват значително въздействие върху сигурността, също може да бъде определена като съществена промяна. Важно е също така да се отбележи, че макар отстраняването на софтуерен дефект да засяга само конкретен аспект на обекта на оценка, непредсказуемостта му и потенциалното му въздействие върху увереността могат да доведат до съществена промяна, ако компрометират гаранциите за сигурност, предоставени от сертифицирането.

(6) Промените в средата по отношение на заплахите спрямо непроменен сертифициран ИКТ продукт може да изискват повторна оценка. Възможните резултати от този процес на повторна оценка следва да бъдат ясно установени, по-специално неговото въздействие върху сертификата по ЕССК. Ако повторната оценка е приключила успешно, сертифициращият орган следва да потвърди сертификата или да издаде нов сертификат с удължен срок на валидност. Ако процесът на повторна оценка не е успешен, сертифициращият орган следва да оттегли сертификата или да издаде нов сертификат с различен обхват. Тези разпоредби следва да се прилагат *mutatis mutandis* за повторната оценка на защитните профили.

(7) В приложение I към Регламент за изпълнение (ЕС) 2024/482 са изброени приложимите актуални технически документи за оценка на ИКТ продукти и защитни профили. Тези актуални технически документи следва да бъдат осъвременени, за да отразяват последните развития, като например свързаните с технологичното развитие, обстановката по отношение на киберзаплахите, практиките в сектора или международните стандарти. Такава актуализация е подходяща за актуалните технически документи, свързани с минималните изисквания за сигурност на обекти, прилагането на потенциалите за атака към смарткартите, прилагането на потенциалите за атака към хардуерните устройства с кутии за сигурност, прилагането на общи критерии за интегралните схеми и оценката на съставни продукти за смарткартите и подобните устройства. Освен това не са включени актуалните технически документи, свързани с оценката и сертифицирането на съставни продукти, като се използва последната версия на стандартите за общи критерии, повторното използване на резултатите от оценките от одитите на обекти и разясненията относно тълкуването на защитните профили, свързани с устройствата за създаване на квалифициран електронен подпис, тахографите и хардуерните модули за сигурност. За да се гарантира единна оценка на ИКТ продуктите по ЕССК, приложение I следва да бъде изменено, за да се включат осъвремененните и новите актуални технически документи след одобряването им от Европейската група за сертифициране на киберсигурността (ECCG).

(8) Освен това към схемата следва да се добави актуалният технически документ „ADV_SPM.1 interpretation for CC:2022 transition“, за да се гарантира, че процесите на сертифициране, основаващи се на специфични защитни профили, могат да продължат да използват формално моделиране (ADV_SPM.1) до актуализирането на съответните защитни профили, например с добавянето на спазваща CC:2022 конфигурация на защитен профил с мулти-увереност, която поддържа ADV_SPM.1. За да се осигури достатъчно време на пазара да премине към осъвремененните стандарти на общите критерии, трябва да се предвидят специфични преходни правила за защитните профили Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, или Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. За да се избегнат смущения на пазара, е целесъобразно да се установи, че актуалният технически документ за тълкуване на ADV_SPM.1 за прехода към CC:2022 е приложим за процесите на сертифициране, започнати преди приемането на настоящия регламент. Прилагането на този документ обаче следва да бъде строго ограничено до необходимото, като се има предвид времето, необходимо за приключване на осъвременяването на съответните защитни профили. По-конкретно, за процесите на сертифициране, при които се използват защитни профили Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, или Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, и са започнати преди 1 октомври 2026 г., следва да се прилага актуалният технически документ. За процеси на сертифициране, при които се използва защитен профил Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, актуалният технически документ следва да се прилага само за процесите, започнати преди датата на влизане в сила на настоящия регламент, с оглед на това, че вече е налична нова версия на посочения защитен профил.

(9) Промяна в актуалните технически документи по време на процеса на сертифициране би могла да наруши оценката на продукта и да забави издаването на сертификата. Поради това са необходими подходящи преходни правила за нови или актуални технически документи, за да се даде възможност на доставчиците, ITSEF, сертифициращите органи и други заинтересовани страни да направят необходимите корекции. Приложимите осъвременени и нови актуални технически документи следва да се отнасят за заявления за сертифициране, включително заявления за преоценка и повторна оценка, като същевременно следва да бъде възможно текущите процеси на сертифициране да продължат да използват по-ранни версии на актуалните технически документи.

(10) В приложения II и III към Регламент за изпълнение (ЕС) 2024/482 са изброени съответно защитните профили, сертифицирани на ниво 4 или 5 на AVA_VAN, и препоръчителните защитни профили. Няколко позовавания са непълни или остарели поради актуализиране на защитните профили. Тези позовавания следва да бъдат допълнени и освен това следва да бъдат включени нови позовавания, за да се гарантира по-всеобхватно обхващане на защитените интегрални схеми, смарткартите и свързаните с тях устройства и доверителните изчисления.

(11) Необходимо е да се направят изменения в член 19 от Регламент за изпълнение (ЕС) 2024/482, за да се поясни, че приложение IV се прилага, заедно с необходимите промени, за прегледа на сертификатите по ЕССК за защитни профили.

(12) С оглед на това, че целевото ниво на сигурност е ключов елемент за разбиране на обхвата на процеса на сертифициране, е необходимо също така ENISA да публикува на своя уебсайт целевото ниво на сигурност, съответстващо на всеки сертификат по ЕССК.

(13) Освен това сертифициращите органи следва да предоставят на ENISA версия на английски език на целевото ниво на сигурност и сертификационния доклад, за да може агенцията да предостави тази информация на английски език на съответния уебсайт съгласно член 42, параграф 2 от Регламент за изпълнение (ЕС) 2024/482. Поради тази причина при поискване заявителите за сертифициране следва да предоставят на сертифициращите органи версия на английски език на целевото ниво на сигурност.

(14) Не е необходимо позоваването на наименованието на сертифициращия орган да фигурира в уникалната идентификация на сертификата, тъй като идентификационният номер на сертифициращия орган е достатъчен, за да се идентифицира този орган еднозначно. Не е необходимо да се посочва и месецът на издаване, тъй като сертификатите се броят на годишна база. Поради това посоченото изискване следва да бъде заличено с цел опростяване. Тъй като годината на издаване на сертификата съответства на издаването на първия сертификат, същата дата следва да фигурира в уникалната идентификация върху сертификатите, издадени след преглед, за да се гарантира проследимостта.

(15) Поради това Регламент за изпълнение (ЕС) 2024/482 следва да бъде съответно изменен.

(16) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 66 от Регламент (ЕС) 2019/881,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Регламент за изпълнение (ЕС) 2024/482 се изменя, както следва:

1) В член 2 се добавят следните точки 16, 17 и 18:

„16) „серия продукти“ означава набор от ИКТ продукти на заявител, изградени на една и съща функционална основа, за да се отговори на едни и същи нужди относно сигурността, с дизайн, хардуер, фърмуер или софтуер, които могат да се различават в зависимост от ИКТ продукта;

17) „несъществена промяна“ е всяка промяна в сертифицирания обект на оценка или неговата среда, която не оказва неблагоприятно въздействие върху увереността, посочена в сертификата по ЕССК;

18) „съществена промяна“ е всяка промяна в сертифицирания обект на оценка или неговата среда, която може да окаже неблагоприятно въздействие върху увереността, посочена в сертификата по ЕССК.“

2) В член 5 се добавя следният параграф 3:

„3. Сертифициращият орган може да разреши сертифицирането на серия продукти.“

3) В член 9, параграф 2 буква а) заменя със следното:

„а) да предостави на сертифициращия орган и на ITSEF цялата необходима пълна и вярна информация, както и да предостави необходимата допълнителна информация при поискване, включително версия на английски език на целевото ниво на сигурност;“.

4) В член 11, параграф 3 буква б) се заменя със следното:

„б) уникалната идентификация на сертификата, състояща се от:

1) наименованието на схемата;

2) идентификационния номер в съответствие с член 3 от Регламент за изпълнение (ЕС) 2024/3143 на сертифициращия орган, който е издал сертификата;

3) годината на издаване на първоначалния сертификат;

4) идентификационния номер, определен от сертифициращия орган, издал сертификата.“

5) В член 19 параграф 1 се заменя със следното:

„1. По искане на титуляря на сертификата или по други основателни причини сертифициращият орган може да реши да извърши преглед на сертификата по ЕССК за даден защитен профил. Прегледът се извършва в съответствие с приложение IV. Сертифициращият орган определя обхвата на прегледа. В случай че е необходимо за прегледа, сертифициращият орган отправя искане до ITSEF за извършване на повторна оценка на сертифицирания защитен профил.“

6) Член 42 се изменя, както следва:

а) в параграф 1 се добавя следната буква и):

„и) целевото ниво на сигурност, съответстващо на всеки сертификат по ЕССК;“;

б) параграф 2 се заменя със следното:

„2. Информацията, посочена в параграф 1, се предоставя поне на английски език. За тази цел сертифициращите органи предоставят на ENISA оригиналните езикови версии на сертификационните доклади и целевите нива за сигурност, като освен това предоставят без ненужно забавяне и версията на тези документи на английски език.“

7) В член 48 параграф 4 се заменя със следното:

„4. Освен ако не е посочено друго в приложение I или II, актуалните технически документи се прилагат за процесите за сертифициране, включително преоценка и повторна оценка, започнати от датата на прилагане на акта за изменение, с който са били включени в приложение I или II.“

8) Приложение I се заменя с текста в приложение I към настоящия регламент.

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

10) Приложение III се заменя с текста в приложение III към настоящия регламент.

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

12) Приложение V се изменя в съответствие с приложение V към настоящия регламент.

13) Приложение IX се заменя с текста в приложение VI към настоящия регламент.

Член 2

Настоящият регламент влиза в сила на двадесетия ден след 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 8 декември 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

„ПРИЛОЖЕНИЕ I

Актуални технически документи в подкрепа на техническите области и други актуални технически документи

1. Актуални технически документи в подкрепа на техническите области на нива 4 или 5 на AVA_VAN:

   а) следните документи, свързани с хармонизираната оценка на техническата област „Смарт карти и подобни устройства“:

      1) „Минимални изисквания на ITSEF за оценяване на сигурността на смарт карти и подобни устройства“, версия 1.1;

      2) „Minimum Site Security Requirements“, версия 2;

      3) „Reusing evaluation results of site audits (STAR)“, версия 1;

      4) „Application of Common Criteria to integrated circuits“, версия 2;

      5) „Security Architecture requirements (ADV_ARC) for smart cards and similar devices“, версия 1.1;

      6) „Certification of ‘open’ smart card products“, версия 1.1;

      7) „Composite product evaluation for smart cards and similar devices for CC3.1“, версия 2;

      8) „Composite product evaluation and certification for CC:2022“, версия 1;

      9) „Application of Attack Potential to Smartcards and Similar Devices“, версия 2;

      10) „Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices“, версия 1;

      11) „ADV_SPM.1 interpretation for CC:2022 transition“, версия 1.1, приложим за процеси на сертифициране, при които се използват защитни профили, както следва:

         а) защитни профили BSI-CC-PP-0084-2014 (Security IC Platform PP with Augmentation Packages (v1.0) или BSI-CC-PP-0101-V2-2020 (Java Card System – Closed Configuration (v3.1), започнати преди 1 октомври 2026 г.;

         б) защитен профил BSI-CC-PP-0099-V2-2020 (Java Card System – Open Configuration (v3.1), започнати преди 29 декември 2025 г.;

   б) следните документи, свързани с хармонизираната оценка на техническата област „Хардуерни устройства с кутии за сигурност“:

      1) „Minimum ITSEF requirements for security evaluations of hardware devices with security boxes“, версия 1.1;

      2) „Minimum Site Security Requirements“, версия 2;

      3) „Reusing evaluation results of site audits (STAR)“, версия 1;

      4) „Application of Attack Potential to hardware devices with security boxes“, версия 2;

      5) „Hardware assessment in EN 419221-5 (HSM PP)“, версия 1;

      6) „JIL Tachograph MS PP Clarification“, версия 1.

2. Актуални технически документи, свързани с хармонизираната акредитация на органите за оценяване на съответствието:

   а) „Accreditation of ITSEFs for the EUCC“, версия 1.1 за акредитации, издадени преди 8 юли 2025 г.;

   б) „Accreditation of ITSEFs for the EUCC“, версия 1.6c за новоиздадени или подложени на преглед акредитации след 8 юли 2025 г.;

   в) „Accreditation of CBs for the EUCC“, версия 1.6b.“

ПРИЛОЖЕНИЕ II

„*ПРИЛОЖЕНИЕ II*

Защитни профили, сертифицирани на ниво 4 или 5 на AVA_VAN

1. За устройствата за създаване на квалифициран електронен подпис и печат от разстояние:

   а) EN 419241-2:2019 — Надеждни системи, поддържащи сървърно подписване. Част 2: Защитен профил за QSCD за сървърно подписване (версия 0.16), ANSSI-CC-PP-2018/02-M01;

   б) EN 419221-5:2018 — Защитни профили за TSP криптографски модули. Част 5: Криптографски модул за удостоверителни услуги (версия 0.15), ANSSI-CC-PP-2016/05-M01

2. Защитни профили, които са били приети като актуални технически документи:

   [ПРАЗНО ПОЛЕ].“

ПРИЛОЖЕНИЕ III

„ПРИЛОЖЕНИЕ III

Препоръчителни защитни профили

Защитни профили, използвани при сертифицирането на ИКТ продукти, включително продукти в техническите области:

1. Смарткарти и подобни устройства

   а) паспорт:

      1) PP Machine Readable Travel Document with "ICAO Application" Basic Access Control (v1.10), BSI-CC-PP-0055-2009;

      2) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3) PP Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   б) устройства за създаване на защитени подписи (SSCD):

      1) EN 419211-2:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 2: Устройство с генериране на ключове (версия 1.03), BSI-CC-PP-0059-2009-MA-02;

      2) EN 419211-3:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 3: Устройство с внасяне на ключове (версия 1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3) EN 419211-4:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 4: Разширение за устройство с генериране на ключове и надежден канал към приложение за генериране на сертификати (версия 1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4) EN 419211-5:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 5: Разширение за устройство с генериране на ключове и надежден канал към приложение за създаване на подписи (версия 1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5) EN 419211-6:2014 — Защитни профили за устройство за създаване на защитени подписи. Част 6: Разширение за устройство с внасяне на ключове и надежден канал към приложение за създаване на подписи (версия 1.0.4), BSI-CC-PP-0076-2013-MA-01;

   в) тахограф: Digital Tachograph – Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   г) защитени интегрални схеми, платформа Java Card и eUICC:

      1) Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations (v2.0.2), ANSSI-CC-PP-2010/04 (Basic), ANSSI-CC-PP-2010/05 (Basic and SCWS);

      2) Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014;

      3) Embedded UICC (eUICC) for Machine-to-Machine Devices (v1.1), BSI-CC-PP-0089-2015;

      4) Cryptographic Service Provider – CSP (v0.9.8), BSI-CC-PP-0104-2019;

      5) Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019;

      6) Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl) Version 0.9.4, BSI-CC-PP-0108-2019;

      7) Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020;

      8) Secure Element Protection Profile – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      9) Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (v1.8), BSI-CC-PP-0117-V2-2023;

      10) Java Card System – Open Configuration (v3.2), BSI-CC-PP-0099-V3-2024;

      11) Embedded UICC for Consumer Devices Protection Profile (v2.1), BSI-CC-PP-0100-V2-2025;

   д) модул за надеждна платформа (TPM): Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Хардуерни устройства с кутии за сигурност

а) точки за (платежно) взаимодействие и терминални устройства ПОС:

1) точка за взаимодействие „POI-CHIP-ONLY“ (версия 4.0), ANSSI-CC-PP-2015/01;

2) точка за взаимодействие „POI-CHIP-ONLY и пакет с отворен протокол“ (версия 4.0), ANSSI-CC-PP-2015/02;

3) точка за взаимодействие „POI-COMPREHENSIVE“ (версия 4.0), ANSSI-CC-PP-2015/03;

4) точка за взаимодействие „POI-COMPREHENSIVE и пакет с отворен протокол“ (версия 4.0), ANSSI-CC-PP-2015/04;

5) точка за взаимодействие „POI-PED-ONLY“ (версия 4.0), ANSSI-CC-PP-2015/05;

6) точка за взаимодействие „POI-PED-ONLY и пакет с отворен протокол“ (версия 4.0), ANSSI-CC-PP-2015/06;

б) хардуерен модул за сигурност:

1) Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;

2) Cryptographic Module for CSP Key Generation Services – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;

3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

в) тахограф:

1) Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CC-PP-0093-2017;

2) Digital Tachograph – Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;

3) Digital Tachograph – External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021;

3. Други: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.“

ПРИЛОЖЕНИЕ IV

Приложение IV към Регламент за изпълнение (ЕС) 2024/482 се изменя, както следва:

1. В раздел IV.2 точка 4 се заменя със следното:

„4. Сертифициращият орган извършва преглед на актуализирания технически доклад за оценка и изготвя доклад за повторна оценка. След това статусът на първоначалния сертификат се променя в съответствие с член 13 или член 19. Ако процесът на повторна оценка е успешен, в случай на сертифициране на продукт се прилага член 13, параграф 2, букви а) или в), а в случай на сертифициране на защитен профил се прилага член 19, параграф 2, буква а) или в). Ако процесът на повторна оценка не е успешен, в случай на сертифициране на продукт се прилага член 13, параграф 2, букви б) или г), а в случай на сертифициране на защитен профил се прилага член 19, параграф 2, буква б) или г).“

2. Раздел IV.3 се изменя, както следва:

а) заглавието на раздел IV.3 се заменя със следното:

„IV.3 **Промени в сертифициран ИКТ продукт — поддържане и повторна оценка**“

б) точки 4 и 5 се заменят със следното:

„4. След проверката сертифициращият орган определя мащаба на промяната като несъществен или съществен в съответствие с нейното въздействие върху увереността, посочена в сертификата по ЕССК.

5. Когато сертифициращият орган потвърди, че промените са несъществени, за изменения ИКТ продукт не се издава нов сертификат в съответствие с член 13, параграф 2, буква а) или член 19, параграф 2, буква а), а се изготвя доклад за поддържане към първоначалния сертификационен доклад.“;

в) вмъква се следната точка 5а:

„5а. В случай на промени в мерките за увереност в развойната среда, включително добавянето на изискванията за увереност от група CC ALC_FLR (отстраняване на дефекти), сертифициращият орган може да поиска от ITSEF да извърши частична оценка на засегнатите мерки за увереност. ITSEF издава технически доклад за частична оценка, въз основа на който сертифициращият орган потвърждава, че промените са несъществени или съществени. Когато сертифициращият орган потвърди, че промените са несъществени, се прилага раздел IV.3, точка 5. Когато сертифициращият орган потвърди, че промените са съществени, се прилага раздел IV.3, точка 7.“

ПРИЛОЖЕНИЕ V

Точка V.1 от приложение V към Регламент за изпълнение (ЕС) 2024/482 се заменя със следното:

„V.1 **Сертификационен доклад**

1. Въз основа на техническите доклади за оценка, предоставени от ITSEF, сертифициращият орган изготвя сертификационен доклад, който се публикува заедно със съответния сертификат по ЕССК и целево ниво на сигурност.

2. Сертификационният доклад е източник на подробна и практическа информация за ИКТ продукта и за сигурното внедряване на ИКТ продукта. Поради това в него се включва цялата публично достъпна и подлежаща на споделяне информация, която е от значение за ползвателите и заинтересованите страни. В сертификационния доклад може да се съдържат препратки към публично достъпна и подлежаща на споделяне информация.

3. Сертификационният доклад съдържа най-малко следната информация:

   а) резюме;

   б) идентификация на ИКТ продукта;

   в) информация за контакт, свързана с оценката на ИКТ продукта;

   г) политики за сигурност;

   д) допускания и изясняване на обхвата;

   е) информация за архитектурата;

   ж) допълнителна информация за киберсигурността, ако е приложимо;

   з) резюме на оценката на ИКТ продукта и оценената конфигурация;

   и) резултатите от оценката и информация относно сертификата;

   й) коментари и препоръки, ако е приложимо;

   к) приложения, ако е приложимо;

   л) посочване на целевото ниво на сигурност на ИКТ продукта, представен за сертифициране;

   м) маркировката или етикета, свързани със схемата, когато има такива;

   н) речник на термините, ако е приложимо;

   о) библиография.

4. Резюмето по параграф 3, буква а) представлява кратък преглед на целия сертификационен доклад. То съдържа ясно и кратко обобщение на резултатите от оценката и включва следната информация:

   а) наименование на оценявания ИКТ продукт;

   б) наименование на ITSEF, извършил оценката;

   в) дата на приключване на оценката;

   г) дата на издаване на сертификата;

   д) дата на издаване на първоначалния сертификат, ако е приложимо;

   е) срок на валидност;

   ж) уникална идентификация на сертификата, както е описано в член 11;

   з) кратко описание на резултатите от сертификационния доклад, включително:

      i) версията и, ако е приложимо, изданието на общите критерии, приложени към оценката;

      ii) пакета за получаване на увереност по общите критерии или списък на компонентите за гаранциите за сигурност, включително нивото на AVA_VAN, приложено по време на оценката, и съответното ниво на увереност, както е посочено в член 52 от Регламент (ЕС) 2019/881, за което се отнася сертификатът по ЕССК;

      iii) когато е приложимо, защитните профили, с които ИКТ продуктът декларира съответствие;

      iv) препратка към политиката за сигурност на оценявания ИКТ продукт;

      v) отказ(и) от отговорност, ако е приложимо.

5. Идентификацията по параграф 3, буква б) ясно идентифицира оценявания ИКТ продукт, като включва следната информация:

   а) уникалната идентификация на оценявания ИКТ продукт;

   б) изброяване на компонентите на ИКТ продукта, които са част от оценката, с номера на версията на всеки компонент;

   в) посочване на допълнителните изисквания към оперативната среда на сертифицирания ИКТ продукт.

6. Информацията за контакт по параграф 3, буква в) включва най-малко следната информация:

   а) име на разработчика;

   б) име и информация за връзка на титуляря на сертификата по ЕССК;

   в) наименование на сертифициращия орган, издал сертификата;

   г) отговорен национален орган за сертифициране на киберсигурността;

   д) наименование на ITSEF, който е извършил оценката, и, когато е приложимо, списък на подизпълнителите.

7. Политиката за сигурност по параграф 3, буква г) съдържа описание на политиката за сигурност на ИКТ продукта като сбор от услуги за сигурност и политиките или правилата, които се налагат с оценявания ИКТ продукт или на които той отговаря. Тя също така включва следната информация:

   а) описание на процедурите на титуляря на сертификата за управление на уязвимости и оповестяване на уязвимости, което се попълва единствено с информация, която може да бъде публично достъпна;

   б) политиката за непрекъснатост на увереността на титуляря на сертификата, включително, когато е приложимо, описание на управлението на жизнения цикъл или производствените процеси при титуляря на сертификата в съответствие с раздел IV.1 от приложение IV;

   в) когато е приложимо, наличието на процедура за управление на софтуерните поправки и резултатите от нейната оценка в съответствие с раздел IV.4 от приложение IV.

8. Допусканията и изясняването на обхвата по параграф 3, буква д) съдържат информация относно обстоятелствата и целите, свързани с предвидената употреба на продукта, както е посочено в член 7, параграф 1, буква в), и включват следното:

   а) допускания за използването и внедряването на ИКТ продукта под формата на минимални изисквания, като например правилно инсталиране и конфигуриране и изпълнение на хардуерните изисквания;

   б) допускания за оперативната среда с оглед на съвместимата работа на ИКТ продукта;

   в) описание на всички заплахи за ИКТ продукта, които не се неутрализират от оценените функции за сигурност на продукта в съответствие с предвидената употреба, ако се счита, че са от значение за потенциален ползвател на ИКТ продукта.

   Информацията, посочена в първата алинея, е възможно най-ясна и разбираема, за да могат потенциалните ползватели на сертифицирания ИКТ продукт да вземат информирани решения относно рисковете, свързани с неговата употреба.

9. Информацията за архитектурата по параграф 3, буква е) включва описание на високо ниво на ИКТ продукта и неговите основни компоненти въз основа на резултатите, определени в групата за получаване на увереност по общите критерии: Development - TOE Design (ADV_TDS).

10. Допълнителната информация за киберсигурността по параграф 3, буква ж) включва връзката към уебсайта на титуляря на сертификата по ЕССК, посочен в член 55 от Регламент (ЕС) 2019/881.

11. В оценката и конфигурацията на ИКТ продукта, посочени в параграф 3, буква з), се описват усилията за изпитване както на разработчика, така и на оценителя, като се очертават подходът, конфигурацията и дълбочината на изпитването. Там се включва най-малко следната информация:

    а) идентификация на използваните компоненти на увереността от стандартите, посочени в член 3;

    б) версията на актуалните технически документи и допълнителните критерии за оценка на сигурността, използвани при оценката;

    в) настройките и конфигурацията на обекта на оценка, използвани за изпитването и анализа на уязвимостта;

    г) всеки използван защитен профил, включително следната информация: наименованието, версията, датата и сертификата на защитния профил.

12. Резултатите от оценката и информацията относно сертификата по параграф 3, буква и) включват информация относно постигнатото ниво на увереност, както е посочено в член 4 от настоящия регламент и член 52 от Регламент (ЕС) 2019/881.

13. Коментарите и препоръките по параграф 3, буква й) се използват за съобщаване на допълнителна информация относно резултатите от оценката. Тези коментари и препоръки могат да описват недостатъци на ИКТ продукта, открити по време на оценката, или да посочват характеристики, които са особено полезни.

14. Приложенията по параграф 3, буква к) се използват за предаване на всякаква допълнителна информация, която може да бъде полезна за аудиторията на доклада, но логически не попада в предписаните раздели на доклада, включително в случаите на пълно описание на политиката за сигурност.

15. Целевото ниво на сигурност по параграф 3, буква л) описва оценената целево ниво на сигурност. Оценената целево ниво на сигурност се предоставя заедно със сертификационния доклад за целите на публикуването на уебсайта по член 50, параграф 1 от Регламент (ЕС) 2019/881. Когато е необходимо коригиране на оценената целево ниво на сигурност преди публикуването, това се извършва в съответствие с раздел V.2 от приложение V към настоящия регламент.

16. Маркировките или етикетите по параграф 3, буква м), свързани с ЕССК, се вмъкват в сертификационния доклад в съответствие с установените правила и процедури в член 11.

17. Речникът на термините, посочен в параграф 3, буква н), се използва за повишаване на четивността на доклада чрез предоставяне на определения на акроними или термини, чиито значения може да не са очевидни.

18. Библиографията по параграф 3, буква о) включва препратки към всички документи, използвани при изготвянето на сертификационния доклад. Тази информация включва най-малко следното:

    а) критериите за оценка на сигурността, използваните актуални технически документи и други съответни спецификации;

    б) техническия доклад за оценка;

    в) техническия доклад за оценка на съставен продукт, когато е приложимо;

    г) техническа справочна документация;

    д) насоките за сигурност на разработчика;

    е) списъка на конфигурацията на разработчика.

    За да се гарантира възпроизводимостта на оценката, цялата документация, на която се прави позоваване, трябва да бъде посочена еднозначно с правилната дата на издаване и правилния номер на версията.“

ПРИЛОЖЕНИЕ VI

„ПРИЛОЖЕНИЕ IX

Маркировка и етикет

1. Форма на маркировката и етикета:



2. Ако размерите на маркировката и етикета се намаляват или увеличават, задължително се спазват пропорциите, посочени в точка 1.

3. Когато присъстват физически, маркировката и етикетът са с височина най-малко 5 mm.“