REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2024/482 AL COMISIEI

din 31 ianuarie 2024

de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC)

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) ([1]), în special articolul 49 alineatul (7),

întrucât:

(1) Prezentul regulament precizează rolurile, normele și obligațiile, precum și structura sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) în conformitate cu cadrul european de certificare a securității cibernetice prevăzut în Regulamentul (UE) 2019/881. EUCC se bazează pe Acordul de recunoaștere reciprocă („ARR”) a certificatelor de securitate informatică ale Grupului înalților funcționari pentru securitatea sistemelor informatice („SOG-IS”) ([2]) și utilizează criteriile comune, inclusiv procedurile și documentele grupului.

(2) Sistemul ar trebui să se bazeze pe standarde internaționale consacrate. Criteriile comune sunt un standard internațional pentru evaluarea securității informatice publicat, de exemplu, ca ISO/IEC 15408 Securitatea informațiilor, securitatea cibernetică și protecția vieții private – Criterii de evaluare a securității informatice. Acestea se bazează pe evaluarea efectuată de terți și prevede șapte niveluri de evaluare a asigurării (*Evaluation Assurance Levels*, EAL). Criteriile comune sunt însoțite de metodologia comună de evaluare, publicată, de exemplu, ca ISO/IEC 18045 – Securitatea informațiilor, securitatea cibernetică și protecția vieții private – Criterii de evaluare a securității informatice – Metodologia de evaluare a securității informatice. Specificațiile și documentele care aplică dispozițiile prezentului regulament se pot referi la un standard disponibil public care reflectă standardul utilizat pentru certificare în temeiul prezentului regulament, cum ar fi criteriile comune de evaluare a securității informatice și metodologia comună de evaluare a securității informatice.

(3) EUCC utilizează familia elementelor de evaluare a vulnerabilității bazate pe criteriile comune (AVA_VAN), componentele 1-5. Cele cinci componente furnizează toți determinanții principali necesari și toate dependențele principale necesare pentru analizarea vulnerabilităților produselor TIC. Întrucât componentele corespund nivelurilor de asigurare prevăzute în prezentul regulament, ele permit o alegere în cunoștință de cauză a nivelului de asigurare, pe baza evaluărilor efectuate cu privire la cerințele de securitate și la riscul asociat utilizării preconizate a produsului TIC. Solicitantul unui certificat EUCC ar trebui să furnizeze documentația referitoare la utilizarea preconizată a produsului TIC și analiza nivelurilor de risc asociate unei astfel de utilizări, pentru a permite organismului de evaluare a conformității să evalueze caracterul adecvat al nivelului de asigurare ales. În cazul în care activitățile de evaluare și certificare sunt efectuate de același organism de evaluare a conformității, solicitantul ar trebui să prezinte informațiile necesare o singură dată.

(4) Un domeniu tehnic este un cadru de referință care acoperă un grup de produse TIC cu funcționalități de securitate specifice și similare și care atenuează atacurile atunci când caracteristicile sunt comune unui anumit nivel de asigurare. Domeniul tehnic descrie, în documente ce reflectă stadiul actual al tehnologiei, cerințele de securitate specifice, precum și metodele, tehnicile și instrumentele de evaluare suplimentare care se aplică certificării produselor TIC aflate sub incidența respectivului domeniu tehnic. Prin urmare, domeniul tehnic promovează, de

([1]) JO L 151, 7.6.2019, p. 15.

([2]) Acordul de recunoaștere reciprocă a certificatelor de evaluare a securității informatice (versiunea 3.0 din ianuarie 2010), disponibil pe site-ul sogis.eu, aprobat de Grupul înalților funcționari pentru securitatea sistemelor informatice al Comisiei Europene ca răspuns la punctul 3 din Recomandarea 95/144/CE a Consiliului din 7 aprilie 1995 privind criteriile comune de evaluare a securității în tehnologia informației (JO L 93, 26.4.1995, p. 27).

asemenea, armonizarea evaluării produselor TIC vizate. În prezent, două domenii tehnice sunt foarte des utilizate pentru certificare la nivelurile AVA_VAN.4 și AVA_VAN.5. Primul domeniu tehnic este domeniul „Cartele inteligente și dispozitive similare”, în care părți semnificative ale funcționalității de securitate necesare depind de elemente hardware specifice, personalizate și adesea separabile (de exemplu, hardware pentru cartele inteligente, circuite integrate, produse compozite pentru cartele inteligente, module de platformă de încredere, astfel cum sunt utilizate în calculul de încredere, sau carduri de tahograf digital). Al doilea domeniu tehnic este domeniul „Dispozitive hardware cu cutii de securitate”, în care porțiuni semnificative ale funcționalității de securitate necesare depind de un înveliș fizic, hardware (denumit „cutie de securitate”) care este conceput pentru a rezista la atacuri directe, de exemplu terminale de plată, unități montate pe vehicul pentru tahografe, contoare inteligente, terminale de control al accesului și module de securitate hardware).

(5) Atunci când depune o cerere de certificare, solicitantul ar trebui să lege argumentele privind alegerea unui anumit nivel de asigurare de obiectivele prevăzute la articolul 51 din Regulamentul (UE) 2019/881 și de alegerea componentelor din catalogul cerințelor funcționale de securitate și al cerințelor de asigurare a securității cuprinse în criteriile comune. Organismele de certificare ar trebui să evalueze caracterul adecvat al nivelului de asigurare ales și să se asigure că nivelul respectiv este proporțional cu nivelul de risc asociat utilizării preconizate a produsului TIC.

(6) În conformitate cu criteriile comune, certificarea se efectuează în raport cu un obiectiv de securitate care cuprinde o definiție a problemei de securitate a produsului TIC, precum și cu obiectivele de securitate care abordează problema de securitate. Problema de securitate oferă detalii privind utilizarea preconizată a produsului TIC și riscurile asociate unei astfel de utilizări. Un set ales de cerințe de securitate răspunde atât problemei de securitate, cât și obiectivelor de securitate ale unui produs TIC.

(7) Profilurile de protecție reprezintă un mijloc eficace de a determina în prealabil criteriile comune aplicabile unei anumite categorii de produse TIC și, prin urmare, sunt un element esențial în procesul de certificare a produselor TIC vizate de acel profil de protecție. Un profil de protecție este utilizat pentru a evalua viitoarele obiective de securitate care se încadrează în categoria de produse TIC vizată de respectivul profil de protecție. Profilurile de protecție simplifică și sporesc eficiența procesului de certificare a produselor TIC și ajută utilizatorii să specifice în mod corect și eficace funcționalitatea unui produs TIC. Acestea ar trebui, prin urmare, să fie considerate ca făcând parte integrantă din procesul TIC care conduce la certificarea produselor TIC.

(8) Pentru a le permite să își îndeplinească rolul în procesul TIC care sprijină dezvoltarea și furnizarea unui produs TIC certificat, profilurile de protecție ar trebui ele însele să poată fi certificate în mod independent de certificarea produsului TIC specific care se încadrează în profilul de protecție respectiv. Prin urmare, pentru a se asigura un nivel ridicat de securitate cibernetică, este esențial ca profilurilor de protecție să li se aplice cel puțin același nivel de control ca obiectivelor de securitate. Profilurile de protecție ar trebui evaluate și certificate separat de produsul TIC aferent și exclusiv prin aplicarea clasei de asigurare pentru profilurile de protecție (APE) și, după caz, pentru configurațiile profilurilor de protecție (ACE) din cadrul criteriilor comune și al metodologiei comune de evaluare. Având în vedere rolul lor important și delicat ca punct de referință în certificarea produselor TIC, profilurile de protecție ar trebui să fie certificate exclusiv de organisme publice sau de organisme de certificare care au primit aprobarea prealabilă pentru profilul de protecție specific din partea autorității naționale de certificare a securității cibernetice. Având în vedere rolul lor fundamental în certificarea pentru nivelul de asigurare „ridicat”, în special în afara domeniilor tehnice, profilurile de protecție ar trebui elaborate ca documente ce reflectă stadiul actual al tehnologiei și ar trebui aprobate de Grupul european pentru certificarea securității cibernetice.

(9) Profilurile de protecție certificate ar trebui incluse în monitorizarea conformității și a respectării EUCC de către autoritățile naționale de certificare a securității cibernetice. În cazul în care metodologia, instrumentele și competențele aplicate abordărilor privind evaluarea produselor TIC sunt disponibile pentru profiluri de protecție certificate specifice, domeniile tehnice se pot baza pe respectivele profiluri de protecție specifice.

(10) Pentru a atinge un nivel ridicat de încredere și de asigurare în ceea ce privește produsele TIC certificate, autoevaluarea nu ar trebui să fie permisă în temeiul prezentului regulament. În ceea ce privește evaluarea conformității de către părți terțe, ar trebui să fie permisă doar evaluarea de către ITSEF și organismele de certificare.

(11) Comunitatea SOG-IS a pus la dispoziție interpretări și abordări comune privind aplicarea criteriilor comune și a metodologiei comune de evaluare în procesul de certificare, în special pentru nivelul de asigurare „ridicat” urmărit de domeniile tehnice „Cartele inteligente și dispozitive similare” și „Dispozitive hardware cu cutii de securitate”. Reutilizarea acestor documente justificative în sistemul EUCC asigură o tranziție ușoară de la schemele SOG-IS implementate la nivel național la sistemul armonizat EUCC. Prin urmare, în prezentul regulament ar trebui incluse metodologii de evaluare armonizate cu relevanță generală pentru toate activitățile de certificare. În plus, Comisia ar trebui să poată solicita Grupului european pentru certificarea securității cibernetice să adopte un aviz prin care să aprobe și să recomande aplicarea metodologiilor de evaluare specificate în documentele ce reflectă stadiul actual al tehnologiei pentru certificarea produselor TIC sau a profilurilor de protecție în cadrul sistemului EUCC. Prin urmare, prezentul regulament enumeră în anexa I documentele ce reflectă stadiul actual al tehnologiei pentru activitățile de evaluare desfășurate de organismele de evaluare a conformității. Grupul european pentru certificarea securității cibernetice ar trebui să aprobe și să păstreze documentele ce reflectă stadiul actual al tehnologiei. Acestea ar trebui utilizate în procesul de certificare. Organismele de evaluare a conformității au permisiunea să nu recurgă la ele doar în cazuri excepționale și justificate în mod corespunzător, sub rezerva unor condiții specifice, în special a aprobării de către autoritatea națională de certificare a securității cibernetice.

(12) Certificarea produselor TIC la nivelul AVA_VAN 4 sau 5 ar trebui să fie posibilă doar în anumite condiții și în cazul în care este disponibilă o metodologie de evaluare specifică. Metodologia de evaluare specifică poate fi consacrată în documentele ce reflectă stadiul actual al tehnologiei relevante pentru domeniul tehnic sau în profilurile de protecție specifice – adoptate drept documente ce reflectă stadiul actual al tehnologiei – relevante pentru categoria de produse în cauză. Certificarea la aceste niveluri de asigurare ar trebui să fie posibilă doar în cazuri excepționale și justificate în mod corespunzător, sub rezerva unor condiții specifice, în special a aprobării acestora – și inclusiv a metodologiei de evaluare aplicabile – de către autoritatea națională de certificare a securității cibernetice. Astfel de cazuri excepționale și justificate în mod corespunzător pot exista atunci când legislația Uniunii sau legislația națională impune certificarea unui produs TIC la nivelul AVA_VAN 4 sau 5. În mod similar, în cazuri excepționale și justificate în mod corespunzător, profilurile de protecție vor putea fi certificate fără aplicarea documentelor relevante ce reflectă stadiul actual al tehnologiei, sub rezerva unor condiții specifice, în special a aprobării acestora – și inclusiv a metodologiei de evaluare aplicabile – de către autoritatea națională de certificare a securității cibernetice.

(13) Mărcile și etichetele utilizate în cadrul EUCC urmăresc să le arate utilizatorilor în mod vizibil fiabilitatea produsului TIC certificat și să le permită acestora să facă o alegere în cunoștință de cauză atunci când achiziționează produse TIC. Utilizarea mărcilor și a etichetelor ar trebui, de asemenea, să facă obiectul normelor și condițiilor stabilite în ISO/IEC 17065 și, după caz, în ISO/IEC 17030, cu orientările aplicabile.

(14) Organismele de certificare ar trebui să decidă cu privire la durata valabilității certificatelor, ținând seama de ciclul de viață al produsului TIC în cauză. Durata valabilității nu ar trebui să depășească cinci ani. Autoritățile naționale de certificare a securității cibernetice ar trebui să depună eforturi pentru a armoniza durata valabilității la nivelul Uniunii.

(15) În cazul în care sfera de aplicare a unui certificat EUCC existent este redusă, certificatul trebuie retras și ar trebui emis un nou certificat cu noua sferă de aplicare, pentru a se asigura că utilizatorii sunt informați în mod clar cu privire la sfera de aplicare și nivelul de asigurare actuale ale certificatului unui anumit produs TIC.

(16) Certificarea profilurilor de protecție diferă de cea a produselor TIC, deoarece se referă la un proces TIC. Întrucât un profil de protecție acoperă o categorie de produse TIC, evaluarea și certificarea acestuia nu pot fi realizate pe baza unui singur produs TIC. Întrucât un profil de protecție unifică cerințele generale de securitate referitoare la o categorie de produse TIC și este independent de descrierea produsului TIC de către furnizor, perioada de valabilitate a unui certificat EUCC pentru un profil de protecție ar trebui, în principiu, să acopere cel puțin cinci ani și să se poată prelungi pe toată durata de viață a profilului de protecție.

(17) Organismul de evaluare a conformității este definit ca un organism care desfășoară activități de evaluare a conformității, inclusiv etalonarea, testarea, certificarea și inspecția. Pentru a asigura o înaltă calitate a serviciilor, prezentul regulament precizează că activitățile de testare, pe de o parte, și activitățile de certificare și inspecție, pe de altă parte, ar trebui să fie efectuate de entități care își desfășoară activitatea în mod independent una față de cealaltă, și anume de unitățile de evaluare a securității informatice (*Information Technology Security Evaluation Facilities*, ITSEF) și, respectiv, de organismele de certificare. Ambele tipuri de organisme de evaluare a conformității ar trebui să fie acreditate și, în anumite situații, autorizate.

(18) Un organism de certificare ar trebui să fie acreditat în conformitate cu standardul ISO/IEC 17065 de către organismul național de acreditare pentru nivelurile de asigurare „substanțial” și „ridicat”. Pe lângă acreditarea în conformitate cu Regulamentul (UE) 2019/881 coroborat cu Regulamentul (CE) nr. 765/2008, organismele de evaluare a conformității ar trebui să îndeplinească cerințe specifice pentru a garanta propria competență tehnică, confirmată printr-o autorizație, în ceea ce privește evaluarea cerințelor de securitate cibernetică pentru nivelul de asigurare „ridicat” al EUCC. Pentru a sprijini procesul de autorizare, ar trebui elaborate documente relevante ce reflectă stadiul actual al tehnologiei, care să fie publicate de ENISA după aprobarea de către Grupul european pentru certificarea securității cibernetice.

(19) Competența tehnică a unei unități ITSEF ar trebui evaluată prin acreditarea laboratorului de testare în conformitate cu norma ISO/IEC 17025, completată de ISO/IEC 23532-1 pentru întregul set de activități de evaluare care sunt relevante pentru nivelul de asigurare și care sunt specificate în norma ISO/IEC 18045 coroborată cu ISO/IEC 15408. Atât organismul de certificare, cât și ITSEF ar trebui să instituie și să mențină un sistem adecvat de gestionare a competențelor pentru personalul care se bazează pe ISO/IEC 19896-1 pentru elementele și nivelurile de competență și pentru evaluarea competențelor. În ceea ce privește nivelul de cunoștințe, competențe, experiență și educație, cerințele aplicabile evaluatorilor ar trebui să se bazeze pe ISO/IEC 19896-3. Dispozițiile și măsurile echivalente care abordează abaterile de la astfel de sisteme de gestionare a competențelor ar trebui demonstrate, în conformitate cu obiectivele sistemului.

(20) Pentru a fi autorizată, unitatea ITSEF ar trebui să își demonstreze capacitatea de a determina absența vulnerabilităților cunoscute, punerea în aplicare corectă și consecventă a funcționalităților de securitate de ultimă generație pentru tehnologia specifică vizată și rezistența respectivului produs TIC în fața atacatorilor calificați. În plus, pentru autorizațiile în domeniul tehnic „Cartele inteligente și dispozitive similare”, ITSEF ar trebui să demonstreze, de asemenea, capacitățile tehnice necesare pentru activitățile de evaluare și sarcinile conexe, astfel cum sunt definite într-un document-suport pentru criteriile comune intitulat „Cerințe minime ale ITSEF privind evaluările de securitate ale cartelelor inteligente și dispozitivelor similare” ([3]). Pentru autorizarea în domeniul tehnic „Dispozitive hardware cu cutii de securitate”, ITSEF ar trebui, în plus, să demonstreze cerințele tehnice minime necesare pentru desfășurarea activităților de evaluare și a sarcinilor conexe privind dispozitivele hardware cu cutii de securitate, conform recomandărilor ECCG. În contextul cerințelor minime, unitatea ITSEF ar trebui să fie capabilă să desfășoare diferitele tipuri de atacuri prevăzute în documentul-suport pentru criteriile comune intitulat „Aplicarea potențialului de atac la dispozitivele hardware cu cutii de securitate”. Aceste capacități includ cunoștințele și competențele evaluatorului, precum și echipamentele și metodele de evaluare necesare pentru a determina și a evalua diferitele tipuri de atacuri.

(21) Autoritatea națională de certificare a securității cibernetice ar trebui să monitorizeze respectarea de către organismele de certificare, ITSEF și titularii certificatelor a obligațiilor care le revin în temeiul prezentului regulament și al Regulamentului (UE) 2019/881. Autoritatea națională de certificare a securității cibernetice ar trebui să utilizeze orice surse adecvate de informații în acest scop, inclusiv informațiile primite de la participanții la procesul de certificare și provenite din investigații proprii.

(22) Organismele de certificare ar trebui să coopereze cu autoritățile relevante de supraveghere a pieței și să ia în considerare orice informație privind vulnerabilitatea care ar putea fi relevante pentru produsele TIC pentru care au eliberat certificate. Organismele de certificare ar trebui să monitorizeze profilurile de protecție pe care le-au certificat pentru a determina dacă cerințele de securitate stabilite pentru o categorie de produse TIC continuă să reflecte cele mai recente evoluții în ceea ce privește amenințările cibernetice.

(23) În sprijinul monitorizării conformității, autoritățile naționale de certificare a securității cibernetice ar trebui să coopereze cu autoritățile relevante de supraveghere a pieței în conformitate cu articolul 58 din Regulamentul (UE) 2019/881 și cu Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului ([4]). Operatorii economici din Uniune sunt obligați să facă schimb de informații și să coopereze cu autoritățile de supraveghere a pieței, în temeiul articolului 4 alineatul (3) din Regulamentul 2019/1020.

([3]) Joint Interpretation Library: Cerințe minime ale ITSEF privind evaluările de securitate ale cartelelor inteligente și dispozitivelor similare, versiunea 2.1 din februarie 2020, disponibilă la adresa sogis.eu.

([4]) Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului din 20 iunie 2019 privind supravegherea pieței și conformitatea produselor și de modificare a Directivei 2004/42/CE și a Regulamentelor (CE) nr. 765/2008 și (UE) nr. 305/2011 (JO L 169, 25.6.2019, p. 1).

(24) Organismele de certificare ar trebui să monitorizeze respectarea normelor de către titularii certificatelor și conformitatea tuturor certificatelor eliberate în temeiul EUCC. Monitorizarea ar trebui să asigure faptul că toate rapoartele de evaluare furnizate de o unitate ITSEF și concluziile formulate în acestea, precum și criteriile și metodele de evaluare sunt aplicate în mod consecvent și corect în toate activitățile de certificare.

(25) În cazul în care se detectează potențiale probleme de neconformitate care afectează un produs TIC certificat, este important să se asigure un răspuns proporțional. Prin urmare, certificatele pot fi suspendate. Suspendarea ar trebui să implice anumite limitări în ceea ce privește promovarea și utilizarea produsului TIC în cauză, dar nu ar trebui să afecteze valabilitatea certificatului. Suspendarea ar trebui să fie notificată de către titularul certificatului UE celor care achiziționează produsele TIC vizate și de către autoritatea națională de certificare a securității cibernetice relevantă autorităților relevante de supraveghere a pieței. Pentru a informa publicul, ENISA ar trebui să publice informații cu privire la suspendare pe un site web specific.

(26) Titularul unui certificat EUCC ar trebui să pună în aplicare procedurile necesare de gestionare a vulnerabilității și să se asigure că acestea sunt încorporate în structura sa. Atunci când ia cunoștință de o potențială vulnerabilitate, titularul certificatului EUCC ar trebui să efectueze o analiză a impactului vulnerabilității. În cazul în care analiza impactului vulnerabilității confirmă faptul că vulnerabilitatea poate fi exploatată, deținătorul certificatului ar trebui să trimită un raport de evaluare organismului de certificare, care, la rândul său, ar trebui să informeze autoritatea națională de certificare a securității cibernetice. Raportul ar trebui să informeze cu privire la impactul vulnerabilității, modificările sau soluțiile de remediere necesare, inclusiv posibilele implicații mai ample ale vulnerabilității, precum și soluțiile de remediere pentru alte produse. Dacă este necesar, standardul EN ISO/IEC 29147 ar trebui să completeze procedura de divulgare a vulnerabilității.

(27) În scopul certificării, organismele de evaluare a conformității și autoritățile naționale de certificare a securității cibernetice obțin date confidențiale și sensibile și secrete de afaceri, inclusiv în ceea ce privește proprietatea intelectuală sau monitorizarea conformității care necesită o protecție adecvată. Prin urmare, acestea ar trebui să aibă competențele și cunoștințele tehnice necesare și ar trebui să instituie sisteme de protecție a informațiilor. Cerințele și condițiile de protecție a informațiilor ar trebui să fie îndeplinite atât pentru acreditare, cât și pentru autorizare.

(28) ENISA ar trebui să furnizeze lista profilurilor de protecție certificate pe site-ul său privind certificarea securității cibernetice și să indice statutul acestora, în conformitate cu Regulamentul (UE) 2019/881.

(29) Prezentul regulament stabilește condițiile privind acordurile de recunoaștere reciprocă cu țările terțe. Aceste acorduri de recunoaștere reciprocă pot fi bilaterale sau multilaterale și ar trebui să înlocuiască acordurile similare în vigoare în prezent. În vederea facilitării unei tranziții ușoare către astfel de acorduri de recunoaștere reciprocă, statele membre pot continua să aplice acordurile de cooperare existente cu țările terțe pentru o perioadă limitată.

(30) Organismele de certificare care eliberează certificate EUCC pentru nivelul de asigurare „ridicat”, precum și unitățile ITSEF relevante conexe ar trebui să facă obiectul unor evaluări colegiale. Scopul evaluărilor colegiale ar trebui să fie de a determina dacă statutul și procedurile organismului de certificare supus evaluării colegiale continuă să îndeplinească cerințele sistemului EUCC. Evaluările colegiale sunt diferite de evaluările *inter pares* efectuate în rândul autorităților naționale de certificare a securității cibernetice, astfel cum sunt prevăzute la articolul 59 din Regulamentul (UE) 2019/881. Evaluările colegiale ar trebui să se asigure că organismele de certificare funcționează în mod armonizat și produc aceeași calitate a certificatelor și ar trebui să identifice eventualele puncte forte sau puncte slabe în ceea ce privește performanța organismelor de certificare, inclusiv în vederea schimbului de bune practici. Întrucât există diferite tipuri de organisme de certificare, ar trebui permise diferite tipuri de evaluare colegială. În cazuri mai complexe, cum ar fi cel al organismelor de certificare care eliberează certificate pentru diferite niveluri AVA_VAN, pot fi utilizate diferite tipuri de evaluare colegială, cu condiția ca toate cerințele să fie îndeplinite.

(31) Grupul european pentru certificarea securității cibernetice ar trebui să joace un rol important în menținerea sistemului. Aceasta ar trebui să se desfășoare, printre altele, prin cooperarea cu sectorul privat, prin crearea de subgrupuri specializate și prin activități de pregătire și de asistență relevante solicitate de Comisie. Grupul european pentru certificarea securității cibernetice ar trebui să joace un rol important în aprobarea documentelor ce reflectă stadiul actual al tehnologiei. La aprobarea și adoptarea documentelor ce reflectă stadiul actual al tehnologiei, ar trebui să se țină seama în mod corespunzător de elementele menționate la articolul 54 alineatul (1) litera (c) din

Regulamentul (UE) 2019/881. Domeniile tehnice și documentele ce reflectă stadiul actual al tehnologiei ar trebui publicate în anexa I la prezentul regulament. Profilurile de protecție care au fost adoptate ca documente ce reflectă stadiul actual al tehnologiei ar trebui publicate în anexa II. Pentru a se asigura că aceste anexe sunt dinamice, Comisia le poate modifica în conformitate cu procedura prevăzută la articolul 66 alineatul (2) din Regulamentul (UE) 2019/881 și ținând seama de avizul Grupului european pentru certificarea securității cibernetice. Anexa III conține profiluri de protecție recomandate care, la momentul intrării în vigoare a prezentului regulament, nu sunt documente ce reflectă stadiul actual al tehnologiei. Acestea ar trebui publicate pe site-ul web al ENISA menționat la articolul 50 alineatul (1) din Regulamentul (UE) 2019/881.

(32) Prezentul regulament ar trebui să înceapă să se aplice după 12 luni de la intrarea sa în vigoare. Cerințele din capitolul IV și din anexa V nu necesită o perioadă de tranziție și, prin urmare, ar trebui să se aplice de la intrarea în vigoare a prezentului regulament.

(33) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul Comitetului european pentru certificarea securității cibernetice instituit prin articolul 66 din Regulamentul (UE) 2019/881,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

Prezentul regulament instituie sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC).

Prezentul regulament se aplică tuturor produselor din domeniul tehnologiei informației și comunicațiilor („TIC”), inclusiv documentației aferente, care sunt prezentate spre certificare în temeiul EUCC, precum și tuturor profilurilor de protecție care sunt prezentate spre certificare ca parte a procesului TIC care duce la certificarea produselor TIC.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „criterii comune” înseamnă criteriile comune de evaluare a securității informatice, astfel cum sunt stabilite în standardul ISO/IEC 15408;

2. „metodologia comună de evaluare” înseamnă metodologia comună de evaluare a securității informatice, astfel cum este stabilită în standardul ISO/IEC 18045;

3. „obiectul evaluării” înseamnă un produs TIC sau o componentă a acestuia ori un profil de protecție ca parte a unui proces TIC, care face obiectul unei evaluări a securității cibernetice în vederea obținerii unui certificat EUCC;

4. „obiectiv de securitate” înseamnă pretinderea conformității cu cerințele de securitate dependente de implementare pentru un anumit produs TIC;

5. „profil de protecție” înseamnă un proces TIC care stabilește cerințele de securitate pentru o anumită categorie de produse TIC, descrie necesitățile în materie de securitate independente de implementare și poate fi utilizat pentru a evalua produse TIC ce se încadrează în categoria respectivă, în vederea certificării acestora;

6. „raport tehnic de evaluare” înseamnă un document elaborat de ITSEF care prezintă rezultatele, concluziile și justificările obținute în cursul evaluării unui produs TIC sau a unui profil de protecție în conformitate cu normele și obligațiile prevăzute în prezentul regulament;

7. „ITSEF” înseamnă o unitate de evaluare a securității informatice, care este un organism de evaluare a conformității, astfel cum este definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care efectuează sarcini de evaluare;

8. „nivel AVA_VAN” înseamnă un nivel de analiză a vulnerabilității în ceea ce privește nivelul de asigurare care indică gradul activităților de evaluare a securității cibernetice desfășurate pentru a determina nivelul de rezistență la posibila exploatare a deficiențelor sau a punctelor slabe ale obiectului evaluării în mediul său operațional, astfel cum se prevede în criteriile comune;

9. „certificat EUCC” înseamnă un certificat de securitate cibernetică eliberat în temeiul EUCC pentru produse TIC sau pentru profiluri de protecție care pot fi utilizate exclusiv în procesul TIC de certificare a produselor TIC;

10. „produs compozit” înseamnă un produs TIC care este evaluat împreună cu un alt produs TIC subiacent ce a primit deja un certificat EUCC și de a cărui funcționalitate de securitate depinde produsul TIC compozit;

11. „autoritate națională de certificare a securității cibernetice” înseamnă o autoritate desemnată de un stat membru în temeiul articolului 58 alineatul (1) din Regulamentul (UE) 2019/881;

12. „organism de certificare” înseamnă un organism de evaluare a conformității astfel cum este definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008 care desfășoară activități de certificare;

13. „domeniu tehnic” înseamnă un cadru tehnic comun legat de o anumită tehnologie pentru o certificare armonizată cu un set de cerințe de securitate caracteristice;

14. „un document ce reflectă stadiul actual al tehnologiei” înseamnă un document care specifică metodele, tehnicile și instrumentele de evaluare care se aplică certificării produselor TIC, cerințele de securitate ale unei categorii generice de produse TIC, precum și orice alte cerințe necesare pentru certificare, cu scopul de a armoniza evaluarea, în special cea a domeniilor tehnice sau a profilurilor de protecție;

15. „autoritate de supraveghere a pieței” înseamnă o autoritate astfel cum este definită la articolul 3 punctul 4 din Regulamentul (UE) 2019/1020.

Articolul 3

Standarde de evaluare

Următoarele standarde se aplică evaluărilor efectuate în cadrul sistemului EUCC:

(a) criteriile comune;

(b) metodologia comună de evaluare.

Articolul 4

Niveluri de asigurare

(1) Organismele de certificare eliberează certificate EUCC pentru nivelul de asigurare „substanțial” sau „ridicat”.

(2) Certificatele EUCC pentru nivelul de asigurare „substanțial” corespund certificatelor care acoperă nivelul AVA_VAN 1 sau 2.

(3) Certificatele EUCC pentru nivelul de asigurare „ridicat” corespund certificatelor care acoperă nivelul AVA_VAN 3, 4 sau 5.

(4) Nivelul de asigurare confirmat printr-un certificat EUCC face distincție între utilizarea conformă și utilizarea sporită a componentelor de asigurare, astfel cum se specifică în criteriile comune în conformitate cu anexa VIII.

(5) Organismele de evaluare a conformității aplică acele componente ale asigurării de care depinde nivelul AVA_VAN selectat în conformitate cu standardele menționate la articolul 3.

Articolul 5

Metode de certificare a produselor TIC

(1) Certificarea unui produs TIC se efectuează în raport cu obiectivul său de securitate:

(a) astfel cum este definit de solicitant sau

(b) care încorporează un profil de protecție certificat ca parte a procesului TIC, în cazul în care produsul TIC se încadrează în categoria de produse TIC aflată sub incidența respectivului profil de protecție.

(2) Un profil de protecție trebuie să fie certificat exclusiv în scopul certificării produselor TIC care se încadrează în categoria specifică de produse TIC acoperită de acel profil de protecție.

Articolul 6

Autoevaluarea conformității

Nu este permisă o autoevaluare a conformității în sensul articolului 53 din Regulamentul (UE) 2019/881.

CAPITOLUL II

CERTIFICAREA PRODUSELOR TIC

SECȚIUNEA I

STANDARDE ȘI CERINȚE SPECIFICE PENTRU EVALUARE

Articolul 7

Criterii și metode de evaluare pentru produsele TIC

(1) Un produs TIC prezentat spre certificare trebuie evaluat cel puțin în conformitate cu următoarele elemente:

(a) elementele aplicabile ale standardelor menționate la articolul 3;

(b) clasele de cerințe de asigurare a securității pentru evaluarea vulnerabilităților și testarea funcțională independentă, astfel cum sunt prevăzute în standardele de evaluare menționate la articolul 3;

(c) nivelul de risc asociat utilizării preconizate a produselor TIC în cauză în conformitate cu articolul 52 din Regulamentul (UE) 2019/881 și funcțiilor lor de securitate care sprijină obiectivele de securitate prevăzute la articolul 51 din Regulamentul (UE) 2019/881;

(d) documentele ce reflectă stadiul actual al tehnologiei aplicabile enumerate în anexa I și

(e) profilurile de protecție certificate aplicabile enumerate în anexa II.

(2) În cazuri excepționale și justificate în mod corespunzător, un organism de evaluare a conformității poate solicita să nu aplice documentul relevant ce reflectă stadiul actual al tehnologiei. În aceste cazuri, organismul de evaluare a conformității informează autoritatea națională de certificare a securității cibernetice, motivându-și cererea în mod corespunzător. Autoritatea națională de certificare a securității cibernetice evaluează motivele excepției și, dacă aceasta se

justifică, aprobă cererea. În așteptarea deciziei autorității naționale de certificare a securității cibernetice, organismul de evaluare a conformității nu eliberează niciun certificat. Autoritatea națională de certificare a securității cibernetice notifică excepția aprobată, fără întârzieri nejustificate, Grupului european pentru certificarea securității cibernetice, care poate emite un aviz. Autoritatea națională de certificare a securității cibernetice ține seama în cea mai mare măsură de avizul Grupului european pentru certificarea securității cibernetice.

(3) Certificarea produselor TIC la nivelul AVA_VAN 4 sau 5 trebuie să fie posibilă numai în următoarele scenarii:

(a) în cazul în care este vizat de oricare dintre domeniile tehnice enumerate în anexa I, produsul TIC este evaluat în conformitate cu documentele ce reflectă stadiul actual al tehnologiei aplicabile respectivelor domenii tehnice;

(b) în cazul în care se încadrează într-o categorie de produse TIC vizate de un profil de protecție certificat care include nivelurile AVA_VAN 4 sau 5 și care figurează în anexa II ca profil de protecție ce reflectă stadiul actual al tehnologiei, produsul TIC este evaluat în conformitate cu metodologia de evaluare specificată pentru respectivul profil de protecție;

(c) în cazul în care literele (a) și (b) de la prezentul alineat nu sunt aplicabile, iar includerea unui domeniu tehnic în anexa I sau a unui profil de protecție certificat în anexa II este puțin probabilă în viitorul apropiat și numai în cazuri excepționale și justificate în mod corespunzător, sub rezerva condițiilor prevăzute la alineatul (4).

(4) În cazul în care un organism de evaluare a conformității consideră că se află într-un caz excepțional și justificat în mod corespunzător dintre cele menționate la alineatul (3) litera (c), acesta notifică certificarea avută în vedere autorității naționale de certificare a securității cibernetice, furnizând o justificare și o propunere de metodologie de evaluare. Autoritatea națională de certificare a securității cibernetice evaluează motivele excepției și, dacă aceasta se justifică, aprobă sau modifică metodologia de evaluare care urmează să fie aplicată de organismul de evaluare a conformității. În așteptarea deciziei autorității naționale de certificare a securității cibernetice, organismul de evaluare a conformității nu eliberează niciun certificat. Autoritatea națională de certificare a securității cibernetice raportează certificarea avută în vedere, fără întârzieri nejustificate, Grupului european pentru certificarea securității cibernetice, care poate emite un aviz. Autoritatea națională de certificare a securității cibernetice ține seama în cea mai mare măsură de avizul Grupului european pentru certificarea securității cibernetice.

(5) În cazul unui produs TIC supus evaluării care vizează un produs compozit în conformitate cu documentele relevante ce reflectă stadiul actual al tehnologiei, unitatea ITSEF care a efectuat evaluarea produsului TIC subiacent pune informațiile relevante la dispoziția unității ITSEF care efectuează evaluarea produsului TIC compozit.

SECȚIUNEA II

ELIBERAREA, REÎNNOIREA ȘI RETRAGEREA CERTIFICATELOR EUCC

Articolul 8

Informații necesare pentru certificare

(1) Un solicitant al unui certificat EUCC transmite sau pune în alt mod la dispoziția organismului de certificare și a unității ITSEF toate informațiile necesare pentru activitățile de certificare.

(2) Informațiile menționate la alineatul (1) includ toate dovezile relevante în conformitate cu secțiunile referitoare la „Elementele privind acțiunea dezvoltatorilor”, în formatul corespunzător, astfel cum se prevede în secțiunile referitoare la „Elementele privind conținutul și prezentarea dovezilor” din criteriile comune și metodologia comună de evaluare pentru nivelul de asigurare ales și cerințele de asigurare a securității aferente. Dovezile includ, dacă este necesar, detalii privind produsul TIC și codul sursă al acestuia în conformitate cu prezentul regulament, sub rezerva unor garanții împotriva divulgării neautorizate.

(3) Solicitanții certificatelor pot furniza organismului de certificare și unității ITSEF rezultatele unei evaluări corespunzătoare provenite de la o certificare anterioară realizată în temeiul:

(a) prezentului regulament;

(b) unui alt sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 din Regulamentul (UE) 2019/881;

(c) unui sistem național dintre cele menționate la articolul 49 din prezentul regulament.

(4) În cazul în care rezultatele evaluării sunt relevante pentru sarcinile sale, ITSEF poate reutiliza rezultatele evaluării, cu condiția ca aceste rezultate să fie conforme cu cerințele aplicabile și ca autenticitatea lor să fie confirmată.

(5) În cazul în care organismul de certificare permite ca produsul să fie supus unei certificări pentru produse compozite, solicitantul certificării pune la dispoziția organismului de certificare și a unității ITSEF toate elementele necesare, după caz, în conformitate cu documentul ce reflectă stadiul actual al tehnologiei.

(6) Solicitanții certificatelor furnizează, de asemenea, organismului de certificare și unității ITSEF următoarele informații:

(a) linkul către site-ul lor care conține informațiile suplimentare în materie de securitate cibernetică menționate la articolul 55 din Regulamentul (UE) 2019/881;

(b) o descriere a procedurilor utilizate de solicitant pentru gestionarea și divulgarea vulnerabilităților.

(7) Toate documentele relevante menționate la prezentul articol sunt păstrate de organismul de certificare, de ITSEF și de solicitant pentru o perioadă de 5 ani de la expirarea certificatului.

Articolul 9

Condiții pentru eliberarea unui certificat EUCC

(1) Organismele de certificare eliberează un certificat EUCC în cazul în care sunt îndeplinite toate condițiile următoare:

(a) categoria de produse TIC intră în sfera de aplicare a acreditării și, după caz, a autorizării organismului de certificare și a unității ITSEF implicate în certificare;

(b) solicitantul certificatului a semnat o declarație prin care își asumă toate angajamentele enumerate la alineatul (2);

(c) ITSEF a încheiat evaluarea fără obiecții în conformitate cu standardele, criteriile și metodele de evaluare menționate la articolele 3 și 7;

(d) organismul de certificare a încheiat examinarea rezultatelor evaluării fără obiecții;

(e) organismul de certificare a verificat dacă rapoartele tehnice de evaluare furnizate de ITSEF sunt conforme cu dovezile furnizate și dacă standardele, criteriile și metodele de evaluare menționate la articolele 3 și 7 au fost aplicate corect.

(2) Solicitantul certificatului își asumă următoarele angajamente:

(a) să furnizeze organismului de certificare și unității ITSEF toate informațiile necesare, complete și corecte, și să furnizeze informații suplimentare necesare, la cerere;

(b) să nu promoveze produsul TIC ca fiind certificat în temeiul EUCC înainte de eliberarea certificatului EUCC;

(c) să promoveze produsul TIC ca fiind certificat numai în ceea ce privește sfera de aplicare stabilită în certificatul EUCC;

(d) să înceteze imediat promovarea produsului TIC ca fiind certificat în cazul suspendării, retragerii sau expirării certificatului EUCC;

(e) să se asigure că produsele TIC comercializate cu trimitere la certificatul EUCC sunt strict identice cu produsul TIC care face obiectul certificării;

(f) să respecte normele de utilizare a mărcii și a etichetei stabilite pentru certificatul EUCC în conformitate cu articolul 11.

(3) În cazul unui produs TIC supus certificării care vizează un produs compozit în conformitate cu documentele relevante ce reflectă stadiul actual al tehnologiei, organismul de certificare care a efectuat certificarea produsului TIC subiacent pune informațiile relevante la dispoziția organismului de certificare care efectuează certificarea produsului TIC compozit.

Articolul 10

Conținutul și formatul certificatului EUCC

(1) Certificatul EUCC include cel puțin informațiile prevăzute în anexa VII.

(2) Domeniul de aplicare și limitele produsului TIC certificat sunt specificate fără echivoc în certificatul EUCC sau în raportul de certificare, indicându-se dacă a fost certificat întregul produs TIC sau doar părți ale acestuia.

(3) Organismul de certificare furnizează solicitantului certificatul EUCC cel puțin în format electronic.

(4) Organismul de certificare întocmește un raport de certificare în conformitate cu anexa V pentru fiecare certificat EUCC pe care îl eliberează. Raportul de certificare se bazează pe raportul tehnic de evaluare emis de ITSEF. Raportul tehnic de evaluare și raportul de certificare indică criteriile și metodele specifice de evaluare menționate la articolul 7 utilizate pentru evaluare.

(5) Organismul de certificare furnizează autorității naționale de certificare a securității cibernetice și ENISA fiecare certificat EUCC și fiecare raport de certificare în format electronic.

Articolul 11

Marca și eticheta

(1) Titularul certificatului poate aplica o marcă și o etichetă pe un produs TIC certificat. Marca și eticheta demonstrează că produsul TIC a fost certificat în conformitate cu prezentul regulament. Marca și eticheta se aplică în conformitate cu prezentul articol și cu anexa IX.

(2) Marca și eticheta se aplică în mod vizibil, lizibil și indelebil pe produsul TIC certificat sau pe plăcuța cu date a acestuia. Dacă acest lucru nu este posibil sau nu se justifică dată fiind natura produsului, marca se aplică pe ambalaj și pe documentele însoțitoare. În cazul în care produsul TIC certificat este livrat sub formă de software, marca și eticheta apar în mod vizibil, lizibil și indelebil în documentația însoțitoare sau această documentație este pusă la dispoziția utilizatorilor ușor și direct prin intermediul unui site web.

(3) Marca și eticheta respectă dispozițiile anexei IX și conțin:

(a) nivelul de asigurare și nivelul AVA_VAN al produsului TIC certificat;

(b) identificarea unică a certificatului, constând în:

1. denumirea sistemului;
2. titlul și numărul de referință al acreditării organismului de certificare care a eliberat certificatul;
3. anul și luna eliberării;
4. numărul de identificare atribuit de organismul de certificare care a eliberat certificatul.

(4) Marca și eticheta sunt însoțite de un cod QR cu un link către un site web care conține cel puțin:

(a) informațiile privind valabilitatea certificatului;

(b) informațiile necesare privind certificarea, astfel cum sunt prevăzute în anexele V și VII;

(c) informațiile care trebuie puse la dispoziția publicului de către titularul certificatului în conformitate cu articolul 55 din Regulamentul (UE) 2019/881; și

(d) după caz, informații anterioare legate de certificarea sau certificările specifice ale produsului TIC, pentru a permite trasabilitatea.

Articolul 12

Perioada de valabilitate a certificatului EUCC

(1) Organismul de certificare stabilește o perioadă de valabilitate pentru fiecare certificat EUCC eliberat, în funcție de caracteristicile produsului TIC certificat.

(2) Perioada de valabilitate a certificatului EUCC nu poate depăși cinci ani.

(3) Prin derogare de la alineatul (2), perioada respectivă poate depăși cinci ani sub rezerva aprobării prealabile a autorității naționale de certificare a securității cibernetice. Autoritatea națională de certificare a securității cibernetice notifică Grupului european pentru certificarea securității cibernetice aprobarea acordată, fără întârzieri nejustificate.

Articolul 13

Revizuirea unui certificat EUCC

(1) La cererea titularului certificatului sau din alte motive justificate, organismul de certificare poate decide să revizuiască certificatul EUCC pentru un produs TIC. Revizuirea se efectuează în conformitate cu anexa IV. Organismul de certificare stabilește amploarea revizuirii. În cazul în care acest lucru este necesar pentru revizuire, organismul de certificare solicită unității ITSEF să efectueze o reevaluare a produsului TIC certificat.

(2) În urma rezultatelor revizuirii și, după caz, ale reevaluării, organismul de certificare:

(a) confirmă certificatul EUCC;

(b) retrage certificatul EUCC în conformitate cu articolul 14;

(c) retrage certificatul EUCC în conformitate cu articolul 14 și eliberează un nou certificat EUCC cu o sferă de aplicare identică și cu o perioadă de valabilitate prelungită; sau

(d) retrage certificatul EUCC în conformitate cu articolul 14 și eliberează un nou certificat EUCC cu o sferă de aplicare diferită.

(3) Organismul de certificare poate decide să suspende, fără întârzieri nejustificate, certificatul EUCC în conformitate cu articolul 30, în așteptarea unor măsuri de remediere pe care trebuie să le ia titularul certificatului EUCC.

Articolul 14

Retragerea unui certificat EUCC

(1) Fără a aduce atingere articolului 58 alineatul (8) litera (e) din Regulamentul (UE) 2019/881, certificatul EUCC trebuie retras de organismul de certificare care a eliberat respectivul certificat.

(2) Organismul de certificare menționat la alineatul (1) notifică retragerea certificatului autorității naționale de certificare a securității cibernetice. Aceasta informează și ENISA cu privire la această retragere, în vederea facilitării sarcinilor care îi revin acesteia în temeiul articolului 50 din Regulamentul (UE) 2019/881. Autoritatea națională de certificare a securității cibernetice informează celelalte autorități de supraveghere a pieței relevante.

(3) Titularul unui certificat EUCC poate solicita retragerea certificatului.

CAPITOLUL III

CERTIFICAREA PROFILURILOR DE PROTECȚIE

SECȚIUNEA I

STANDARDE ȘI CERINȚE SPECIFICE PENTRU EVALUARE

Articolul 15

Criterii și metode de evaluare

(1) Un profil de protecție trebuie evaluat cel puțin în conformitate cu următoarele elemente:

(a) elementele aplicabile ale standardelor menționate la articolul 3;

(b) nivelul de risc asociat utilizării preconizate a produselor TIC în cauză în conformitate cu articolul 52 din Regulamentul (UE) 2019/881 și funcțiile lor de securitate care sprijină obiectivele de securitate prevăzute la articolul 51 din respectivul regulament; și

(c) documentele ce reflectă stadiul actual al tehnologiei aplicabile enumerate în anexa I. Un profil de protecție acoperit de un domeniu tehnic trebuie certificat în raport cu cerințele stabilite în domeniul tehnic respectiv.

(2) În cazuri excepționale și justificate în mod corespunzător, un organism de evaluare a conformității poate certifica un profil de protecție fără a aplica documentele relevante ce reflectă stadiul actual al tehnologiei. În astfel de cazuri, organismul respectiv informează autoritatea națională de certificare a securității cibernetice de resort și furnizează o justificare privind certificarea fără aplicarea documentelor relevante ce reflectă stadiul actual al tehnologiei pe care o are în vedere, precum și metodologia de evaluare propusă. Autoritatea națională de certificare a securității cibernetice evaluează justificarea și, dacă acesta este întemeiată, aprobă neaplicarea documentelor relevante ce reflectă stadiul actual al tehnologiei și aprobă sau modifică, după caz, metodologia de evaluare care urmează să fie aplicată de organismul de evaluare a conformității. În așteptarea deciziei autorității naționale de certificare a securității cibernetice, organismul de evaluare a conformității nu eliberează niciun certificat pentru profilul de protecție. Autoritatea națională de certificare a securității cibernetice notifică autorizarea neaplicării documentelor relevante ce reflectă stadiul actual al tehnologiei, fără întârzieri nejustificate, Grupului european pentru certificarea securității cibernetice, care poate emite un aviz. Autoritatea națională de certificare a securității cibernetice ține seama în cea mai mare măsură de avizul Grupului european pentru certificarea securității cibernetice.

SECȚIUNEA II

ELIBERAREA, REÎNNOIREA ȘI RETRAGEREA CERTIFICATELOR EUCC PENTRU PROFILURILE DE PROTECȚIE

Articolul 16

Informații necesare pentru certificarea profilurilor de protecție

Un solicitant al unui certificat pentru un profil de protecție transmite sau pune în alt mod la dispoziția organismului de certificare și a unității ITSEF toate informațiile necesare pentru activitățile de certificare. Articolul 8 alineatele (2), (3), (4) și (7) se aplică mutatis mutandis.

Articolul 17

Eliberarea certificatelor EUCC pentru profilurile de protecție

(1) Solicitantul unui certificat furnizează organismului de certificare și unității ITSEF toate informațiile necesare, complete și corecte.

(2) Articolele 9 și 10 se aplică mutatis mutandis.

(3) ITSEF determină dacă un profil de protecție este complet, consecvent, solid din punct de vedere tehnic și eficace pentru utilizarea preconizată și pentru obiectivele de securitate ale categoriei de produse TIC acoperite de respectivul profil de protecție.

(4) Un profil de protecție trebuie să fie certificat exclusiv de către:

(a) o autoritate națională de certificare a securității cibernetice sau un alt organism public acreditat ca organism de certificare; sau

(b) un organism de certificare, cu aprobarea prealabilă a autorității naționale de certificare a securității cibernetice pentru fiecare profil de protecție în parte.

Articolul 18

Perioada de valabilitate a certificatelor EUCC pentru profilurile de protecție

(1) Organismul de certificare stabilește o perioadă de valabilitate pentru fiecare certificat EUCC.

(2) Perioada de valabilitate poate acoperi întreaga durată de viață a profilului de protecție în cauză.

Articolul 19

Revizuirea unui certificat EUCC pentru un profil de protecție

(1) La cererea titularului certificatului sau din alte motive justificate, organismul de certificare poate decide să revizuiască un certificat EUCC pentru un profil de protecție. Revizuirea se efectuează prin aplicarea condițiilor prevăzute la articolul 15. Organismul de certificare stabilește amploarea revizuirii. În cazul în care acest lucru este necesar pentru revizuire, organismul de certificare solicită unității ITSEF să efectueze o reevaluare a profilului de protecție certificat.

(2) În urma rezultatelor revizuirii și, după caz, ale reevaluării, organismul de certificare întreprinde una dintre următoarele acțiuni:

(a) confirmă certificatul EUCC;

(b) retrage certificatul EUCC în conformitate cu articolul 20;

(c) retrage certificatul EUCC în conformitate cu articolul 20 și eliberează un nou certificat EUCC cu o sferă de aplicare identică și cu o perioadă de valabilitate prelungită;

(d) retrage certificatul EUCC în conformitate cu articolul 20 și eliberează un nou certificat EUCC cu o sferă de aplicare diferită.

Articolul 20

Retragerea unui certificat EUCC pentru un profil de protecție

(1) Fără a aduce atingere articolului 58 alineatul (8) litera (e) din Regulamentul (UE) 2019/881, un certificat EUCC pentru un profil de protecție trebuie retras de organismul de certificare care a eliberat respectivul certificat. Articolul 14 se aplică mutatis mutandis.

(2) Un certificat pentru un profil de protecție eliberat în conformitate cu articolul 17 alineatul (4) litera (b) trebuie retras de autoritatea națională de certificare a securității cibernetice care a aprobat certificatul respectiv.

CAPITOLUL IV

ORGANISME DE EVALUARE A CONFORMITĂȚII

Articolul 21

Cerințe suplimentare sau specifice pentru un organism de certificare

(1) Un organism de certificare este autorizat de autoritatea națională de certificare a securității cibernetice să elibereze certificate EUCC pentru nivelul de asigurare „ridicat” în cazul în care demonstrează, pe lângă îndeplinirea cerințelor prevăzute la articolul 60 alineatul (1) și în anexa la Regulamentul (UE) 2019/881 privind acreditarea organismelor de evaluare a conformității, că:

(a) deține expertiza și competențele necesare pentru a lua decizia de certificare pentru nivelul de asigurare „ridicat”;

(b) își desfășoară activitățile de certificare în cooperare cu o unitate ITSEF autorizată în conformitate cu articolul 22; și

(c) dispune de competențele necesare și a instituit măsuri tehnice și operaționale adecvate pentru a proteja în mod eficace informațiile confidențiale și sensibile pentru nivelul de asigurare „ridicat”, în plus față de cerințele prevăzute la articolul 43.

(2) Autoritatea națională de certificare a securității cibernetice evaluează dacă un organism de certificare îndeplinește toate cerințele prevăzute la alineatul (1). Această evaluare include cel puțin interviuri structurate și o examinare a cel puțin unei certificări-pilot efectuate de organismul de certificare în conformitate cu prezentul regulament.

În evaluarea sa, autoritatea națională de certificare a securității cibernetice poate reutiliza orice dovadă adecvată dintr-o autorizare prealabilă sau din activități similare acordate în temeiul:

(a) prezentului regulament;

(b) unui alt sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 din Regulamentul (UE) 2019/881;

(c) unui sistem național dintre cele menționate la articolul 49 din prezentul regulament.

(3) Autoritatea națională de certificare a securității cibernetice întocmește un raport de autorizare care face obiectul unei evaluări *inter pares* în conformitate cu articolul 59 alineatul (3) litera (d) din Regulamentul (UE) 2019/881.

(4) Autoritatea națională de certificare a securității cibernetice precizează categoriile de produse TIC și profilurile de protecție la care se extinde autorizația. Autorizația este valabilă pentru o perioadă care nu depășește perioada de valabilitate a acreditării. Aceasta poate fi reînnoită la cerere, cu condiția ca organismul de certificare să îndeplinească în continuare cerințele prevăzute la prezentul articol. Pentru reînnoirea autorizației, nu sunt necesare evaluări-pilot.

(5) Autoritatea națională de certificare a securității cibernetice retrage autorizația organismului de certificare în cazul în care acesta nu mai îndeplinește condițiile prevăzute la prezentul articol. La retragerea autorizației, organismul de certificare încetează imediat să se declare drept organism de certificare autorizat.

Articolul 22

Cerințe suplimentare sau specifice pentru o unitate ITSEF

(1) O unitate ITSEF este autorizată de autoritatea națională de certificare a securității cibernetice să realizeze evaluarea produselor TIC care fac obiectul certificării pentru nivelul de asigurare „ridicat” în cazul în care demonstrează, pe lângă îndeplinirea cerințelor prevăzute la articolul 60 alineatul (1) și în anexa la Regulamentul (UE) 2019/881 privind acreditarea organismelor de evaluare a conformității, că respectă toate condițiile următoare:

(a) dispune de expertiza necesară pentru a efectua activitățile de evaluare în vederea determinării rezistenței la atacurile cibernetice de ultimă generație desfășurate de actori cu competențe și resurse semnificative;

(b) pentru domeniile tehnice și profilurile de protecție care fac parte din procesul TIC pentru respectivele produsele TIC, aceasta are:

1. expertiza necesară pentru efectuarea activităților de evaluare specifice necesare pentru a determina metodic, în mediul său operațional, rezistența unui obiect al evaluării împotriva atacatorilor calificați, pe baza unui atac potențial clasificat drept „moderat” sau „ridicat” potrivit standardelor menționate la articolul 3;

2. competențele tehnice specificate în documentele ce reflectă stadiul actual al tehnologiei enumerate în anexa I.

(c) dispune de competențele necesare și a instituit măsuri tehnice și operaționale adecvate pentru a proteja în mod eficace informațiile confidențiale și sensibile pentru nivelul de asigurare „ridicat”, în plus față de cerințele prevăzute la articolul 43.

(2) Autoritatea națională de certificare a securității cibernetice evaluează dacă ITSEF îndeplinește toate cerințele prevăzute la alineatul (1). Această evaluare include cel puțin interviuri structurate și o examinare a cel puțin unei evaluări-pilot efectuate de ITSEF în conformitate cu prezentul regulament.

(3) În evaluarea sa, autoritatea națională de certificare a securității cibernetice poate reutiliza orice dovadă adecvată dintr-o autorizare prealabilă sau din activități similare acordate în temeiul:

(a) prezentului regulament;

(b) unui alt sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 din Regulamentul (UE) 2019/881;

(c) unui sistem național dintre cele menționate la articolul 49 din prezentul regulament.

(4) Autoritatea națională de certificare a securității cibernetice întocmește un raport de autorizare care face obiectul unei evaluări *inter pares* în conformitate cu articolul 59 alineatul (3) litera (d) din Regulamentul (UE) 2019/881.

(5) Autoritatea națională de certificare a securității cibernetice precizează categoriile de produse TIC și profilurile de protecție la care se extinde autorizația. Autorizația este valabilă pentru o perioadă care nu depășește perioada de valabilitate a acreditării. Aceasta poate fi reînnoită la cerere, cu condiția ca ITSEF să îndeplinească în continuare cerințele prevăzute la prezentul articol. Pentru reînnoirea autorizației, nu ar trebui să fie necesare evaluări-pilot.

(6) Autoritatea națională de certificare a securității cibernetice retrage autorizația unității ITSEF în cazul în care aceasta nu mai îndeplinește condițiile prevăzute la prezentul articol. La retragerea autorizației, ITSEF încetează să se declare drept unitate ITSEF autorizată.

Articolul 23

Notificarea organismelor de certificare

(1) Autoritatea națională de certificare a securității cibernetice notifică Comisiei organismele de certificare de pe teritoriul său care au competența de a certifica nivelul de asigurare „substanțial” pe baza acreditării lor.

(2) Autoritatea națională de certificare a securității cibernetice notifică Comisiei organismele de certificare de pe teritoriul său care au competența de a certifica nivelul de asigurare „ridicat” pe baza acreditării lor și a deciziei de autorizare.

(3) Autoritatea națională de certificare a securității cibernetice furnizează cel puțin următoarele informații atunci când notifică Comisiei organismele de certificare:

(a) nivelul sau nivelurile de asigurare pentru care organismul de certificare este competent să elibereze certificate EUCC;

(b) următoarele informații referitoare la acreditare:

1. data acreditării;

2. numele și adresa organismului de certificare;

3. țara de înregistrare a organismului de certificare;

4. numărul de referință al acreditării;

5. sfera de aplicare și durata de valabilitate a acreditării;

6. adresa, locul și linkul către site-ul web relevant al organismului național de acreditare; și

(c) următoarele informații referitoare la autorizația pentru nivelul „ridicat”:

1. data autorizației;

2. numărul de referință al autorizației;

3. durata de valabilitate a autorizației;

4. sfera de aplicare a autorizației, inclusiv cel mai înalt nivel AVA_VAN și, după caz, domeniul tehnic acoperit.

(4) Autoritatea națională de certificare a securității cibernetice trimite ENISA o copie a notificării menționate la alineatele (1) și (2) în vederea publicării de informații exacte pe site-ul dedicat certificării securității cibernetice cu privire la eligibilitatea organismelor de certificare.

(5) Autoritatea națională de certificare a securității cibernetice examinează fără întârzieri nejustificate orice informație referitoare la modificarea statutului acreditării transmisă de organismul național de acreditare. În cazul în care acreditarea sau autorizația a fost retrasă, autoritatea națională de certificare a securității cibernetice informează Comisia în acest sens și poate transmite Comisiei o cerere în conformitate cu articolul 61 alineatul (4) din Regulamentul (UE) 2019/881.

Articolul 24

Notificarea unităților ITSEF

Obligațiile de notificare ale autorităților naționale de certificare a securității cibernetice prevăzute la articolul 23 se aplică și în cazul ITSEF. Notificarea include adresa ITSEF, acreditarea valabilă și, după caz, autorizația valabilă a acesteia.

CAPITOLUL V

MONITORIZARE, NECONFORMITATE ȘI NERESPECTAREA NORMELOR

SECȚIUNEA I

MONITORIZAREA CONFORMITĂȚII

Articolul 25

Activități de monitorizare desfășurate de autoritatea națională de certificare a securității cibernetice

(1) Fără a aduce atingere articolului 58 alineatul (7) din Regulamentul (UE) 2019/881, autoritatea națională de certificare a securității cibernetice monitorizează:

(a) respectarea de către organismul de certificare și ITSEF a obligațiilor care le revin în temeiul prezentului regulament și al Regulamentului (UE) 2019/881;

(b) respectarea titularilor unui certificat EUCC a obligațiilor care le revin în temeiul prezentului regulament și al Regulamentului (UE) 2019/881;

(c) conformitatea produselor TIC certificate cu cerințele stabilite în EUCC;

(d) conformitatea asigurării din certificatul EUCC care abordează evoluțiile în ceea ce privește amenințările cibernetice.

(2) Autoritatea națională de certificare a securității cibernetice își desfășoară activitățile de monitorizare în special pe baza următoarelor elemente:

(a) informații provenind de la organismele de certificare, organismele naționale de acreditare și autoritățile relevante de supraveghere a pieței;

(b) informații rezultate din auditurile și investigațiile proprii sau ale unei alte autorități;

(c) eșantionarea efectuată conform alineatului (3);

(d) reclamațiile primite.

(3) Autoritatea națională de certificare a securității cibernetice, în cooperare cu alte autorități de supraveghere a pieței, eșantionează anual cel puțin 4 % din certificatele EUCC, stabilite printr-o evaluare a riscurilor. La cerere și acționând în numele autorității naționale de certificare a securității cibernetice de resort, organismele de certificare și, dacă este necesar, ITSEF sprijină autoritatea respectivă în ceea ce privește monitorizarea conformității.

(4) Autoritatea națională de certificare a securității cibernetice selectează pe baza unor criterii obiective eșantionul de produse TIC certificate care urmează să fie verificate, criterii care includ:

(a) categoria de produse;

(b) nivelurile de asigurare ale produselor;

(c) titularul unui certificat;

(d) organismul de certificare și, după caz, unitatea ITSEF cu care s-a semnat un subcontract;

(e) orice alte informații aduse la cunoștința autorității.

(5) Autoritatea națională de certificare a securității cibernetice informează titularii certificatelor EUCC cu privire la produsele TIC selectate și la criteriile de selecție.

(6) Organismul de certificare care a certificat produsul TIC eșantionat efectuează, la cererea autorității naționale de certificare a securității cibernetice și cu sprijinul respectivei unități ITSEF, o examinare suplimentară în conformitate cu procedura prevăzută în anexa IV secțiunea IV.2 și informează autoritatea națională de certificare a securității cibernetice cu privire la rezultate.

(7) În cazul în care autoritatea națională de certificare a securității cibernetice are motive suficiente să creadă că un produs TIC certificat nu mai este conform cu prezentul regulament sau cu Regulamentul (UE) 2019/881, aceasta poate efectua investigații sau recurge la orice alte competențe de monitorizare prevăzute la articolul 58 alineatul (8) din Regulamentul (UE) 2019/881.

(8) Autoritatea națională de certificare a securității cibernetice informează organismul de certificare și unitatea ITSEF cu privire la investigațiile în curs privind produsele TIC selectate.

(9) În cazul în care constată că o investigație în curs se referă la produse TIC care sunt certificate de organisme de certificare stabilite în alte state membre, autoritatea națională de certificare a securității cibernetice informează autoritățile naționale de certificare a securității cibernetice din statele membre relevante cu privire la acest lucru pentru a colabora la investigații, dacă este necesar. Respectiva autoritate națională de certificare a securității cibernetice informează și Grupul european pentru certificarea securității cibernetice cu privire la investigațiile transfrontaliere și rezultatele ulterioare.

Articolul 26

Activitățile de monitorizare ale organismului de certificare

(1) Organismul de certificare monitorizează:

(a) respectarea de către titularii unui certificat a obligațiilor care le revin în temeiul prezentului regulament și al Regulamentului (UE) 2019/881 în ceea ce privește certificatul EUCC care a fost eliberat de organismul de certificare;

(b) conformitatea produselor TIC pe care le-a certificat cu cerințele de securitate proprii acestora;

(c) asigurarea care figurează în profilurile de protecție certificate.

(2) Organismul de certificare își desfășoară activitățile de monitorizare pe baza următoarelor elemente:

(a) informațiile furnizate pe baza angajamentelor solicitantului certificatului menționate la articolul 9 alineatul (2);

(b) informațiile rezultate din activitățile altor autorități de supraveghere a pieței relevante;

(c) reclamațiile primite;

(d) informațiile privind vulnerabilitățile care ar putea avea un impact asupra produselor TIC pe care le-a certificat.

(3) Autoritatea națională de certificare a securității cibernetice poate elabora norme pentru un dialog periodic între organismele de certificare și titularii de certificate EUCC pentru a verifica și a raporta cu privire la respectarea angajamentelor asumate în temeiul articolului 9 alineatul (2), fără a aduce atingere activităților legate de alte autorități de supraveghere a pieței relevante.

Articolul 27

Activități de monitorizare desfășurate de titularul certificatului

(1) Titularul unui certificat EUCC îndeplinește următoarele sarcini de monitorizare a conformității produsului TIC certificat cu propriile cerințe de securitate:

(a) monitorizarea informațiilor privind vulnerabilitățile produsului TIC certificat, inclusiv a dependențelor cunoscute, prin mijloace proprii, dar și având în vedere:

1. informație privind vulnerabilitățile publicată sau transmisă de către utilizatori sau cercetători din domeniul securității, astfel cum se menționează la articolul 55 alineatul (1) litera (c) din Regulamentul (UE) 2019/881;

2. informație transmisă din orice altă sursă;

(b) monitorizarea asigurării care figurează în certificatul EUCC.

(2) Titularul unui certificat EUCC lucrează în cooperare cu organismul de certificare, cu ITSEF și, după caz, cu autoritatea națională de certificare a securității cibernetice pentru a sprijini activitățile de monitorizare ale acestora.

SECȚIUNEA II

CONFORMITATE ȘI RESPECTAREA NORMELOR

Articolul 28

Consecințele neconformității unui produs TIC sau a unui profil de protecție certificat

(1) În cazul în care un produs TIC sau un profil de protecție certificat nu este conform cu cerințele prevăzute în prezentul regulament și în Regulamentul (UE) 2019/881, organismul de certificare informează titularul certificatului EUCC cu privire la neconformitatea identificată și solicită măsuri de remediere.

(2) În situația în care un caz de neconformitate cu dispozițiile prezentului regulament ar putea afecta conformitatea cu un alt act legislativ relevant al Uniunii, care prevede posibilitatea de a demonstra prezumția de conformitate cu cerințele actului legislativ respectiv prin utilizarea certificatului EUCC, organismul de certificare informează fără întârziere autoritatea națională de certificare a securității cibernetice în acest sens. Autoritatea națională de certificare a securității cibernetice notifică imediat cazul de neconformitate identificat autorității de supraveghere a pieței în a cărei sferă de competență intră respectivul actul legislativ relevant al Uniunii.

(3) La primirea informațiilor menționate la alineatul (1), titularul certificatului EUCC propune organismului de certificare, în termenul stabilit de acesta din urmă, care nu poate depăși 30 de zile, măsurile de remediere necesare pentru a corecta neconformitatea.

(4) Organismul de certificare poate suspenda certificatul EUCC în conformitate cu articolul 30 fără întârzieri nejustificate, în caz de urgență sau în cazul în care titularul certificatului EUCC nu cooperează în mod corespunzător cu organismul de certificare.

(5) Organismul de certificare efectuează o revizuire în conformitate cu articolele 13 și 19, evaluând dacă măsurile de remediere corectează neconformitatea.

(6) În cazul în care titularul certificatului EUCC nu propune măsuri de remediere adecvate în perioada menționată la alineatul (3), certificatul se suspendă în conformitate cu articolul 30 sau se retrage în conformitate cu articolul 14 sau 20.

(7) Prezentul articol nu se aplică în cazul vulnerabilităților care afectează un produs TIC certificat, care sunt gestionate în conformitate cu capitolul VI.

Articolul 29

Consecințele nerespectării obligațiilor de către titularul certificatului

(1) În cazul în care organismul de certificare constată că:

(a) titularul certificatului EUCC sau solicitantul unui certificat nu își respectă angajamentele și obligațiile prevăzute la articolul 9 alineatul (2), la articolul 17 alineatul (2) și la articolele 27 și 41 sau

(b) titularul certificatului EUCC nu respectă articolul 56 alineatul (8) din Regulamentul (UE) 2019/881 sau capitolul VI din prezentul regulament,

acesta stabilește o perioadă de maximum 30 de zile în care titularul certificatului EUCC trebuie să ia măsuri de remediere.

(2) În cazul în care titularul certificatului EUCC nu propune măsuri de remediere adecvate în perioada menționată la alineatul (1), certificatul se suspendă în conformitate cu articolul 30 sau se retrage în conformitate cu articolele 14 și 20.

(3) Încălcarea continuă sau recurentă de către titularul unui certificat EUCC a obligațiilor menționate la alineatul (1) duce la retragerea certificatului EUCC în conformitate cu articolul 14 sau 20.

(4) Organismul de certificare informează autoritatea națională de certificare a securității cibernetice cu privire la constatările menționate la alineatul (1). În cazul în care situația de neconformitate afectează conformitatea cu alte acte legislative relevante ale Uniunii, autoritatea națională de certificare a securității cibernetice notifică imediat situația de neconformitate identificată autorității de supraveghere a pieței în a cărei sferă de competență intră aceste alte acte legislative relevante ale Uniunii.

Articolul 30

Suspendarea certificatului EUCC

(1) În cazurile în care prezentul regulament se referă la suspendarea unui certificat EUCC, organismul de certificare suspendă certificatul EUCC în cauză pentru o perioadă corespunzătoare circumstanțelor care declanșează suspendarea, care nu poate depăși 42 de zile. Perioada de suspendare începe în ziua următoare datei deciziei organismului de certificare. Suspendarea nu afectează valabilitatea certificatului.

(2) Organismul de certificare notifică suspendarea certificatului titularului certificatului și autorității naționale de certificare a securității cibernetice fără întârzieri nejustificate și prezintă motivele suspendării, acțiunile care trebuie întreprinse și perioada de suspendare.

(3) Titularii certificatelor informează cumpărătorii produselor TIC în cauză cu privire la suspendare și la motivele furnizate de organismul de certificare privind suspendarea, cu excepția acelor informații a căror divulgare ar constitui un risc la adresa securității sau care conțin date sensibile. Aceste informații trebuie puse, de asemenea, la dispoziția publicului de către titularul certificatului.

(4) În cazul în care alte acte legislative relevante ale Uniunii prevăd o prezumție de conformitate pe baza certificatelor eliberate în temeiul dispozițiilor prezentului regulament, autoritatea națională de certificare a securității cibernetice notifică suspendarea autorității de supraveghere a pieței în a cărei sferă de competență intră aceste alte acte legislative relevante ale Uniunii.

(5) Suspendarea unui certificat trebuie notificată către ENISA în conformitate cu articolul 42 alineatul (3).

(6) În cazuri justificate în mod corespunzător, autoritatea națională de certificare a securității cibernetice poate autoriza o prelungire a perioadei de suspendare a certificatului EUCC. Durata totală a suspendării nu poate depăși un an.

Articolul 31

Consecințele nerespectării obligațiilor de către organismul de evaluare a conformității

(1) În cazul în care un organism de certificare nu își respectă obligațiile sau în cazul în care un anumit organism de certificare nu își face datoria în cazul identificării neconformității unei unități ITSEF, autoritatea națională de certificare a securității cibernetice trebuie, fără întârzieri nejustificate:

(a) să identifice, cu sprijinul unității ITSEF în cauză, certificatele EUCC care ar putea fi afectate;

(b) să solicite, dacă este necesar, ca unul sau mai multe produse TIC sau profiluri de protecție să fie evaluate fie de către unitatea ITSEF care a efectuat evaluarea, fie de orice altă unitate ITSEF acreditată și, după caz, autorizată, care poate fi mai în măsură din punct de vedere tehnic să sprijine identificarea respectivă;

(c) să analizeze impactul neconformității;

(d) să informeze titularul certificatului EUCC afectat de neconformitate.

(2) Pe baza măsurilor menționate la alineatul (1), organismul de certificare adoptă oricare dintre următoarele decizii cu privire la fiecare certificat EUCC afectat:

(a) menține certificatul EUCC fără modificări;

(b) retrage certificatul EUCC în conformitate cu articolul 14 sau 20 și, după caz, eliberează un nou certificat EUCC.

(3) Pe baza măsurilor menționate la alineatul (1), autoritatea națională de certificare a securității cibernetice:

(a) raportează organismului național de acreditare, dacă este necesar, neconformitatea organismului de certificare sau a unității ITSEF conexe;

(b) evaluează, dacă este cazul, impactul potențial asupra autorizației.

CAPITOLUL VI

GESTIONAREA ȘI DIVULGAREA VULNERABILITĂȚILOR

Articolul 32

Sfera de aplicare a gestionării vulnerabilităților

Prezentul capitol se aplică produselor TIC pentru care a fost eliberat un certificat EUCC.

SECȚIUNEA I

GESTIONAREA VULNERABILITĂȚILOR

Articolul 33

Proceduri de gestionare a vulnerabilităților

(1) Titularul unui certificat EUCC instituie și menține toate procedurile necesare de gestionare a vulnerabilităților în conformitate cu normele prevăzute în prezenta secțiune și, dacă este necesar, prin completare cu de procedurile prevăzute în EN ISO/IEC 30111.

(2) Titularul unui certificat EUCC utilizează și publică metode adecvate pentru a primi informații privind vulnerabilitățile legate de produsele sale din surse externe, inclusiv din partea utilizatorilor, a organismelor de certificare și a cercetătorilor din domeniul securității.

(3) În cazul în care detectează sau primește informații cu privire la o potențială vulnerabilitate care afectează un produs TIC certificat, titularul unui certificat EUCC înregistrează informația respectivă și efectuează o analiză a impactului vulnerabilității.

(4) Atunci când o potențială vulnerabilitate vizează un produs compozit, titularul certificatului EUCC informează titularul certificatelor EUCC dependente cu privire la respectiva vulnerabilitate.

(5) Ca răspuns la o cerere rezonabilă din partea organismului de certificare care a eliberat certificatul, titularul unui certificat EUCC transmite organismului de certificare respectiv toate informațiile relevante cu privire la potențialele vulnerabilități.

Articolul 34

Analiza impactului vulnerabilităților

(1) Analiza impactului vulnerabilităților se referă la obiectul evaluării și la declarațiile de asigurare cuprinse în certificat. Analiza impactului vulnerabilităților se efectuează într-un interval de timp adecvat în ceea ce privește riscul de exploatare și caracterul critic al vulnerabilității potențiale a produsului TIC certificat.

(2) Dacă este cazul, se efectuează un calcul al potențialului de atac în conformitate cu metodologia relevantă inclusă în standardele menționate la articolul 3 și în documentele relevante ce reflectă stadiul actual al tehnologiei enumerate în anexa I, pentru a determina în ce măsură vulnerabilitatea riscă să fie exploatată. Se ia în considerare nivelul AVA_VAN al certificatului EUCC.

Articolul 35

Raportul de analiză a impactului vulnerabilității

(1) Titularul întocmește un raport de analiză a impactului vulnerabilității în cazul în care analiza impactului arată că vulnerabilitatea are un impact probabil asupra conformității produsului TIC cu certificatul său.

(2) Raportul de analiză a impactului vulnerabilității conține o evaluare a următoarelor elemente:

(a) impactul vulnerabilității produsului TIC certificat;

(b) riscurile posibile asociate proximității sau posibilității unui atac;

(c) posibilitatea ca vulnerabilitatea să poată fi remediată;

(d) în cazul în care vulnerabilitatea poate fi remediată, posibilele soluționări ale vulnerabilității.

(3) Raportul de analiză a impactului vulnerabilității conține, după caz, detalii cu privire la mijloacele posibile de exploatare a vulnerabilității. Informațiile referitoare la mijloacele posibile de exploatare a vulnerabilității trebuie tratate în conformitate cu măsurile de securitate adecvate pentru a proteja confidențialitatea și pentru a asigura, dacă este necesar, distribuția limitată a acestora.

(4) Titularul certificatului EUCC transmite raportul de analiză a impactului vulnerabilității organismului de certificare sau autorității naționale de certificare a securității cibernetice în conformitate cu articolul 56 alineatul (8) din Regulamentul (UE) 2019/881, fără întârzieri nejustificate.

(5) În cazul în care raportul de analiză a impactului vulnerabilității stabilește că vulnerabilitatea nu este reziduală în sensul standardelor menționate la articolul 3 și că aceasta poate fi remediată, se aplică articolul 36.

(6) În cazul în care raportul de analiză a impactului vulnerabilității stabilește că vulnerabilitatea nu este reziduală și că nu poate fi remediată, certificatul EUCC se retrage în conformitate cu articolul 14.

(7) Titularul certificatului EUCC monitorizează orice vulnerabilitate reziduală pentru a se asigura că aceasta nu poate fi exploatată în cazul unor modificări ale mediului operațional.

Articolul 36

Remedierea vulnerabilității

Titularul certificatului EUCC prezintă organismului de certificare o propunere de măsuri de remediere adecvate. Organismul de certificare revizuiește certificatul în conformitate cu articolul 13. Sfera de aplicare a revizuirii este determinată de remedierea propusă a vulnerabilității.

SECȚIUNEA II

DIVULGAREA VULNERABILITĂȚILOR

Articolul 37

Informații puse la dispoziția autorității naționale de certificare a securității cibernetice

(1) Informațiile furnizate de organismul de certificare autorității naționale de certificare a securității cibernetice includ toate elementele necesare pentru ca autoritatea națională de certificare a securității cibernetice să înțeleagă impactul vulnerabilității, modificările care trebuie aduse produsului TIC și orice informații din partea organismului de certificare cu privire la implicațiile mai ample ale vulnerabilității pentru alte produse TIC certificate, dacă aceste informații sunt disponibile.

(2) Informațiile furnizate în conformitate cu alineatul (1) nu conțin detalii privind mijloacele de exploatare a vulnerabilității. Această dispoziție nu aduce atingere competențelor de investigare ale autorității naționale de certificare a securității cibernetice.

Articolul 38

Cooperarea cu alte autorități naționale de certificare a securității cibernetice

(1) Autoritatea națională de certificare a securității cibernetice pune informațiile relevante primite în conformitate cu articolul 37 la dispoziția altor autorități naționale de certificare a securității cibernetice și la dispoziția ENISA.

(2) Alte autorități naționale de certificare a securității cibernetice pot decide să analizeze mai în detaliu vulnerabilitatea sau, după informarea titularului certificatului EUCC, să solicite organismelor de certificare relevante să evalueze dacă vulnerabilitatea poate afecta alte produse TIC certificate.

Articolul 39

Publicarea vulnerabilității

La retragerea certificatului, titularul certificatului EUCC divulgă și înregistrează orice vulnerabilitate publică și remediată a produsului TIC în baza de date europeană a vulnerabilităților, instituită în conformitate cu articolul 12 din Directiva

(UE) 2022/2555 a Parlamentului European și a Consiliului ([5]), sau în alte registre online menționate la articolul 55 alineatul (1) litera (d) din Regulamentul (UE) 2019/881.

CAPITOLUL VII

PĂSTRAREA, DIVULGAREA ȘI PROTECȚIA INFORMAȚIILOR

Articolul 40

Păstrarea evidențelor de către organismele de certificare și ITSEF

(1) ITSEF și organismele de certificare mențin un sistem de evidență care conține toate documentele elaborate în legătură cu fiecare evaluare și certificare pe care o efectuează.

(2) Organismele de certificare și ITSEF stochează evidențele în mod securizat și le păstrează pe perioada necesară în sensul prezentului regulament și timp de cel puțin 5 ani după retragerea certificatului EUCC relevant. În cazul în care organismul de certificare a emis un nou certificat EUCC în conformitate cu articolul 13 alineatul (2) litera (c), acesta păstrează documentația aferentă certificatului EUCC retras împreună cu cea a noului certificat EUCC și pentru aceeași perioadă de timp ca pe aceasta din urmă.

Articolul 41

Informații puse la dispoziție de titularul certificatului

(1) Informațiile menționate la articolul 55 din Regulamentul (UE) 2019/881 sunt disponibile într-o limbă ușor accesibilă utilizatorilor.

(2) Titularul unui certificat EUCC stochează următoarele elemente în mod securizat pe perioada necesară în sensul prezentului regulament și timp de cel puțin 5 ani după retragerea certificatului EUCC relevant:

(a) evidențele informațiilor furnizate organismului de certificare și unității ITSEF în cursul procesului de certificare;

(b) specimenul produsului TIC certificat.

(3) În cazul în care organismul de certificare a emis un nou certificat EUCC în conformitate cu articolul 13 alineatul (2) litera (c), titularul păstrează documentația aferentă certificatului EUCC retras împreună cu cea a noului certificat EUCC și pentru aceeași perioadă de timp ca pe aceasta din urmă.

(4) La cererea organismului de certificare sau a autorității naționale de certificare a securității cibernetice, titularul certificatului EUCC pune la dispoziție evidențele și copiile menționate la alineatul (2).

Articolul 42

Informații care trebuie puse la dispoziție de ENISA

(1) ENISA publică următoarele informații pe site-ul web menționat la articolul 50 alineatul (1) din Regulamentul (UE) 2019/881:

(a) toate certificatele EUCC;

(b) informații privind statutul unui certificat EUCC, mai precis dacă acesta este în vigoare, suspendat, retras sau expirat;

(c) rapoarte de certificare corespunzătoare fiecărui certificat EUCC;

([5]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

(d) o listă a organismelor acreditate de evaluare a conformității;

(e) o listă a organismelor autorizate de evaluare a conformității;

(f) documentele ce reflectă stadiul actual al tehnologiei enumerate în anexa I;

(g) avizele Grupului european pentru certificarea securității cibernetice menționate la articolul 62 alineatul (4) litera (c) din Regulamentul (UE) 2019/881;

(h) rapoartele de evaluare colegială emise în conformitate cu articolul 47;

(2) Informațiile menționate la alineatul (1) trebuie să fie puse la dispoziție cel puțin în limba engleză.

(3) Organismele de certificare și, după caz, autoritățile naționale de certificare a securității cibernetice informează fără întârziere ENISA cu privire la deciziile lor care afectează conținutul sau statutul certificatului EUCC menționat la alineatul (1) litera (b).

(4) ENISA se asigură că informațiile publicate în conformitate cu alineatul (1) literele (a), (b) și (c) identifică în mod clar versiunile unui produs TIC certificat care fac obiectul certificatului EUCC.

Articolul 43

Protecția informațiilor

Organismele de evaluare a conformității, autoritățile naționale de certificare a securității cibernetice, ECCG, ENISA, Comisia și toate celelalte părți asigură securitatea și protecția secretelor de afaceri și a altor informații confidențiale, inclusiv a secretelor comerciale, precum și protecția drepturilor de proprietate intelectuală și iau măsurile tehnice și organizatorice necesare și adecvate în acest sens.

CAPITOLUL VIII

ACORDURI DE RECUNOAȘTERE RECIPROCĂ CU ȚĂRI TERȚE

Articolul 44

Condiții

(1) Țările terțe care doresc să își certifice produsele în conformitate cu prezentul regulament și care doresc ca o astfel de certificare să fie recunoscută în Uniune încheie un acord de recunoaștere reciprocă cu Uniunea.

(2) Acordul de recunoaștere reciprocă acoperă nivelurile de asigurare aplicabile pentru produsele TIC certificate și, după caz, profilurile de protecție.

(3) Acordurile de recunoaștere reciprocă menționate la alineatul (1) pot fi încheiate numai cu țări terțe care îndeplinesc următoarele condiții:

(a) dețin o autoritate care:

1. este un organism public și independent de entitățile pe care le supraveghează și le monitorizează în ceea ce privește structura organizațională și juridică, finanțarea financiară și procesul decizional;
2. dispune de competențe adecvate de monitorizare și supraveghere pentru a efectua investigații și este împuternicită să ia măsurile corective adecvate pentru a asigura conformitatea;
3. dispune de un sistem de sancțiuni eficace, proporțional și disuasiv pentru a asigura conformitatea;
4. a convenit să colaboreze cu Grupul european pentru certificarea securității cibernetice și cu ENISA pentru a face schimb de bune practici și de informații privind evoluțiile relevante în domeniul certificării securității cibernetice și a depune eforturi în vederea unei interpretări uniforme a criteriilor și metodelor de evaluare aplicabile în prezent, printre altele prin aplicarea unei documentații armonizate echivalente documentelor ce reflectă stadiul actual al tehnologiei enumerate în anexa I;

(b) dețin un organism de acreditare independent care efectuează acreditări utilizând standarde echivalente celor menționate în Regulamentul (CE) nr. 765/2008;

(c) își iau angajamentul ca procesele și procedurile de evaluare și certificare să se desfășoare cu profesionalismul corespunzător, ținând seama de respectarea standardelor internaționale menționate în prezentul regulament, mai precis la articolul 3;

(d) au capacitatea de a raporta vulnerabilitățile nedetectate anterior și dispun de o procedură consacrată și adecvată de gestionare și divulgare a vulnerabilităților;

(e) au instituit proceduri care permit depunerea și tratarea în mod eficace a plângerilor și oferă reclamantului căi de atac eficace;

(f) instituie un mecanism de cooperare cu alte organisme ale Uniunii și ale statelor membre care sunt relevante pentru certificarea securității cibernetice în temeiul prezentului regulament, inclusiv prin schimbul de informații cu privire la posibila neconformitate a certificatelor, prin monitorizarea evoluțiilor relevante în domeniul certificării și prin asigurarea unei abordări comune privind menținerea și revizuirea certificării.

(4) Pe lângă condițiile prevăzute la alineatul (3), acordul de recunoaștere reciprocă menționat la alineatul (1) care acoperă nivelul de asigurare „ridicat” poate fi încheiat cu țări terțe numai dacă sunt îndeplinite și următoarele condiții:

(a) țara terță deține o autoritate independentă și publică de certificare a securității cibernetice care efectuează sau deleagă activitățile de evaluare necesare pentru a permite certificarea pentru nivelul de asigurare „ridicat”, aceste activități fiind echivalente cu cerințele și procedurile prevăzute pentru autoritățile naționale de securitate cibernetică în prezentul regulament și în Regulamentul (UE) 2019/881;

(b) acordul de recunoaștere reciprocă instituie un mecanism comun echivalent evaluării colegiale pentru certificarea EUCC, pentru a consolida schimbul de practici și a soluționa în comun problemele din domeniul evaluării și certificării.

CAPITOLUL IX

EVALUAREA COLEGIALĂ A ORGANISMELOR DE CERTIFICARE

Articolul 45

Procedura evaluării colegiale

(1) Un organism de certificare care eliberează certificate EUCC pentru nivelul de asigurare „ridicat” trebuie să fie supus unei evaluări colegiale periodice și cel puțin o dată la 5 ani. Diferitele tipuri de evaluări colegiale sunt enumerate în anexa VI.

(2) Grupul european pentru certificarea securității cibernetice elaborează și menține un calendar al evaluărilor colegiale care să asigure respectarea acestei periodicități. Cu excepția cazurilor justificate în mod corespunzător, evaluările colegiale se efectuează la fața locului.

(3) Evaluarea colegială se poate baza pe dovezile colectate în cursul evaluărilor colegiale anterioare sau al procedurilor echivalente ale organismului de certificare supus evaluării colegiale ori ale autorității naționale de certificare a securității cibernetice, cu condiția ca:

(a) rezultatele să nu fie mai vechi de 5 ani;

(b) rezultatele să fie însoțite de o descriere a procedurilor de evaluare colegială stabilite pentru sistemul respectiv, în cazul în care acestea se referă la o evaluare colegială efectuată în cadrul unui alt sistem de certificare;

(c) raportul de evaluare colegială menționat la articolul 47 să specifice rezultatele care au fost reutilizate, cu sau fără o evaluare suplimentară.

(4) În cazul în care o evaluare colegială acoperă un domeniu tehnic, unitatea ITSEF în cauză trebuie, de asemenea, evaluată.

(5) Organismul de certificare supus evaluării colegiale și, dacă este necesar, autoritatea națională de certificare a securității cibernetice se asigură că toate informațiile relevante sunt puse la dispoziția echipei de evaluare colegială.

(6) Evaluarea colegială se efectuează de o echipă de evaluare colegială înființată în conformitate cu anexa VI.

Articolul 46

Etapele evaluării colegiale

(1) În cursul etapei pregătitoare, membrii echipei de evaluare colegială examinează documentația organismului de certificare în ceea ce privește politicile și procedurile acestuia, inclusiv utilizarea documentelor ce reflectă stadiul actual al tehnologiei.

(2) În timpul etapei vizitei la fața locului, echipa de evaluare colegială evaluează competența tehnică a organismului și, după caz, competența unei unități ITSEF care a efectuat cel puțin o evaluare a unui produs TIC supusă evaluării colegiale.

(3) Durata etapei vizitei la fața locului poate fi prelungită sau redusă în funcție factori precum posibilitatea de a reutiliza dovezile și rezultatele evaluării colegiale existente sau numărul de unități ITSEF și de domenii tehnice pentru care organismul de certificare eliberează certificate.

(4) Dacă este cazul, echipa de evaluare colegială stabilește competența tehnică a fiecărei unități ITSEF vizitând laboratorul sau laboratoarele sale tehnice și intervievând evaluatorii săi în ceea ce privește domeniul tehnic și metodele de atac specifice aferente.

(5) În etapa raportării, echipa de evaluare își înscrie constatările într-un raport de evaluare colegială care include un verdict și, după caz, o listă a neconformităților observate, fiecare încadrată în funcție de un nivel critic.

(6) Raportul de evaluare colegială trebuie discutat mai întâi cu organismul de certificare supus evaluării colegiale. În urma acestor discuții, organismul de certificare supus evaluării colegiale stabilește un calendar al măsurilor care trebuie luate pentru a aborda constatările.

Articolul 47

Raportul de evaluare colegială

(1) Echipa de evaluare colegială furnizează organismului de certificare supus evaluării colegiale un proiect al raportului de evaluare colegială.

(2) Organismul de certificare supus evaluării colegiale prezintă echipei de evaluare colegială observații cu privire la constatări și o listă de angajamente pentru remedierea deficiențelor identificate în proiectul raportului de evaluare colegială.

(3) Echipa de evaluare colegială prezintă Grupului european pentru certificarea securității cibernetice un raport final de evaluare colegială, care include, de asemenea, observațiile și angajamentele asumate de organismul de certificare supus evaluării colegiale. Echipa de evaluare colegială include, de asemenea, poziția sa cu privire la observații și la măsura în care angajamentele respective sunt suficiente pentru a remedia deficiențele identificate.

(4) În cazul în care în raportul de evaluare colegială sunt identificate neconformități, Grupul european pentru certificarea securității cibernetice poate stabili un termen adecvat pentru remedierea neconformităților de către organismul de certificare supus evaluării colegiale.

(5) Grupul european pentru certificarea securității cibernetice adoptă un aviz cu privire la raportul de evaluare colegială:

(a) în cazul în care raportul de evaluare colegială nu identifică neconformități sau în cazul în care neconformitățile au fost abordate în mod corespunzător de organismul de certificare supus evaluării colegiale, Grupul european pentru certificarea securității cibernetice poate emite un aviz pozitiv și toate documentele relevante se publică pe site-ul ENISA privind certificarea;

(b) în cazul în care organismul de certificare supus evaluării colegiale nu abordează neconformitățile în mod corespunzător în termenul stabilit, Grupul european pentru certificarea securității cibernetice poate emite un aviz negativ care se publică pe site-ul ENISA privind certificarea, împreună cu raportul de evaluare colegială și cu toate documentele relevante.

(6) Înainte de publicarea avizului, toate informațiile sensibile, datele cu caracter personal sau informațiile proprietare se elimină din documentele publicate.

CAPITOLUL X

MENȚINEREA SISTEMULUI

Articolul 48

Menținerea EUCC

(1) Comisia poate solicita Grupului european pentru certificarea securității cibernetice să adopte un aviz în vederea menținerii EUCC și să întreprindă lucrările pregătitoare necesare.

(2) Grupul european pentru certificarea securității cibernetice poate adopta un aviz pentru a aproba documentele ce reflectă stadiul actual al tehnologiei.

(3) Documentele ce reflectă stadiul actual al tehnologiei care au fost aprobate de Grupul european pentru certificarea securității cibernetice trebuie să fie publicate de ENISA.

CAPITOLUL XI

DISPOZIȚII FINALE

Articolul 49

Sistemele naționale acoperite de EUCC

(1) În conformitate cu articolul 57 alineatul (1) din Regulamentul (UE) 2019/881 și fără a aduce atingere articolul 57 alineatul (3) din regulamentul respectiv, toate sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC și procesele TIC care fac obiectul EUCC încetează să producă efecte la 12 luni de la intrarea în vigoare a prezentului regulament.

(2) Prin derogare de la articolul 50, o procedură de certificare poate fi inițiată în cadrul unui sistem național de certificare a securității cibernetice în termen de 12 luni de la intrarea în vigoare a prezentului regulament, cu condiția ca procedura de certificare să fie finalizată în termen de cel mult 24 de luni de la intrarea în vigoare a prezentului regulament.

(3) Certificatele eliberate în cadrul sistemelor naționale de certificare a securității cibernetice pot face obiectul unei revizuiri. Noile certificate care înlocuiesc certificatele revizuite se eliberează în conformitate cu prezentul regulament.

Articolul 50

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la 27 februarie 2025.

Capitolul IV și anexa V se aplică de la data intrării în vigoare a prezentului regulament.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 31 ianuarie 2024.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

Domenii tehnice și documente ce reflectă stadiul actual al tehnologiei

1. Domenii tehnice la nivelul AVA_VAN 4 sau 5:

   (a) documente referitoare la evaluarea armonizată a domeniului tehnic „Cartele inteligente și dispozitive similare”, mai precis următoarele documente, în versiunea care este în vigoare la [data intrării în vigoare]:

      (1) „Cerințe minime ale ITSEF privind evaluările de securitate ale cartelelor inteligente și dispozitivelor similare”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (2) „Cerințe minime de securitate *in situ*”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (3) „Aplicarea criteriilor comune circuitelor integrate”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (4) „Cerințe privind arhitectura de securitate (ADV_ARC) pentru cartele inteligente și dispozitive similare”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (5) „Certificarea produselor cu cartele inteligente «cu sursă deschisă»”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (6) „Evaluarea produselor compozite pentru cartele inteligente și dispozitive similare”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (7) „Aplicarea potențialului de atac asupra cartelelor inteligente”, document aprobat inițial de ECCG la 20 octombrie 2023;

   (b) documente referitoare la evaluarea armonizată a domeniului tehnic „Dispozitive hardware cu cutii de securitate”, în special următoarele documente, în versiunea care este în vigoare la [data intrării în vigoare]:

      (1) „Cerințe minime ale ITSEF privind evaluările de securitate ale dispozitivelor hardware cu cutii de securitate”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (2) „Cerințe minime de securitate *in situ*”, document aprobat inițial de ECCG la 20 octombrie 2023;

      (3) „Aplicarea potențialului de atac asupra dispozitivelor hardware cu cutii de securitate”, document aprobat inițial de ECCG la 20 octombrie 2023.

2. Documente ce reflectă stadiul actual al tehnologiei, în versiunea care este în vigoare la [data intrării în vigoare]:

   (a) document referitor la acreditarea armonizată a organismelor de evaluare a conformității: „Acreditarea unităților ITSEF pentru EUCC”, document aprobat inițial de ECCG la 20 octombrie 2023.

ANEXA II

Profiluri de protecție certificate la nivelul AVA_VAN 4 sau 5

1. Pentru categoria dispozitivelor calificate de creare a semnăturii și a sigiliului la distanță:

(1) EN 419241-2: 2019 – Sisteme fiabile de susținere a semnăturii prin server – Partea 2: Profil de protecție pentru QSCD pentru semnătura prin server;

(2) EN 419221-5:2018 - Profiluri de protecție pentru modulele criptografice ale prestatorilor de servicii de încredere - Partea 5: Modul criptografic pentru serviciile de încredere

2. Profilurile de protecție care au fost adoptate ca documente ce reflectă stadiul actual al tehnologiei:

[NECOMPLETAT]

ANEXA III

Profiluri de protecție recomandate (ilustrând domeniile tehnice din anexa I)

Profiluri de protecție (PP) utilizate în certificarea produselor TIC care se încadrează în categoria de produse TIC menționată mai jos:

(a) pentru categoria documentelor de călătorie cu citire optică:

(1) PP pentru un document de călătorie cu citire optică utilizând procedura standard de control cu PACE, BSI-CC-PP-0068-V2-2011-MA-01;

(2) PP pentru un document de călătorie cu citire optică utilizând „Aplicația OACI", controlul extins al accesului, BSI-CC-PP-0056-2009;

(3) PP pentru un document de călătorie cu citire optică utilizând „Aplicația OACI", controlul extins al accesului cu PACE, BSI-CC-PP-0056-V2-2012-MA-02;

(4) PP pentru un document de călătorie cu citire optică utilizând „Aplicația OACI", controlul de bază al accesului, BSI-CC-PP-0055-2009;

(b) pentru categoria dispozitivelor securizate de creare a semnăturii:

(1) EN 419211-1:2014 - Profiluri de protecție pentru dispozitive securizate de creare a semnăturii - Partea 1: Prezentare generală

(2) EN 419211-2:2013 - Profiluri de protecție pentru dispozitive securizate de creare a semnăturii - Partea 2: Dispozitiv cu generare de cheie;

(3) EN 419211-3:2013 - Profiluri de protecție pentru dispozitive securizate de creare a semnăturii - Partea 3: Dispozitiv cu import de cheie;

(4) EN 419211-4:2013 - Profiluri de protecție pentru dispozitive securizate de creare a semnăturii - Partea 4: Extensie pentru dispozitive cu generare de cheie și comunicație securizată cu aplicația de generare de certificate

(5) EN 419211-5:2013 - Profiluri de protecție pentru dispozitive securizate de creare a semnăturii - Partea 5: Extensie pentru dispozitive cu generare de cheie și comunicație sigură cu aplicația de creare a semnăturii;

(6) EN 419211-6:2014 - Profiluri de protecție pentru dispozitive securizate de creare a semnăturii - Partea 6: Extensie pentru dispozitive cu import de cheie și comunicație sigură cu aplicația de creare a semnăturii;

(c) pentru categoria tahografelor digitale:

(1) Tahograf digital – card de tahograf, astfel cum este menționat în Regulamentul de punere în aplicare (UE) 2016/799 al Comisiei din 18 martie 2016 de punere în aplicare a Regulamentului (UE) nr. 165/2014 (anexa 1C);

(2) Tahograf digital – unitate montată pe vehicul, astfel cum este menționată în anexa IB la Regulamentul (CE) nr. 1360/2002 al Comisiei, destinată instalării pe vehiculele de transport rutier;

(3) Tahograf digital – echipament GNSS extern, astfel cum este menționat în anexa 1C la Regulamentul de punere în aplicare (UE) 2016/799 al Comisiei din 18 martie 2016 de punere în aplicare a Regulamentului (UE) nr. 165/2014 al Parlamentului European și al Consiliului;

(4) Tahograf digital – senzor de mișcare, astfel cum este menționat în anexa 1C la Regulamentul de punere în aplicare (UE) 2016/799 al Comisiei din 18 martie 2016 de punere în aplicare a Regulamentului (UE) nr. 165/2014 al Parlamentului European și al Consiliului;

(d) pentru categoria circuitelor integrate securizate, a cartelelor inteligente și a dispozitivelor conexe:

(1) Profilul de protecție pentru *Security IC Platform,* BSI-CC-PP-0084-2014;

(2) *Java Card System - Open Configuration*, V3.0.5 BSI-CC-PP-0099-2017;

(3) *Java Card System - Closed Configuration,* BSI-CC-PP-0101-2017;

(4) Profilul de protecție pentru *PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16*, ANSSI-CC-PP-2015/07;

(5) *Universal SIM card*, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

(6) Cardul inteligent universal integrat (eUICC) pentru dispozitive de tip mașină-la-mașină, BSI-CC-PP-0089-2015;

(e) pentru categoria punctelor de interacțiune (de plată) și a terminalelor de plată:

(1) Punctul de interacțiune „POI-CHIP-ONLY”, ANSSI-CC-PP-2015/01;

(2) Punctul de interacțiune „POI-CHIP-ONLY and Open Protocol Package”, ANSSI-CC-PP-2015/02;

(3) Punctul de interacțiune „POI-COMPREHENSIVE”, ANSSI-CC-PP-2015/03;

(4) Punctul de interacțiune „POI-COMPREHENSIVE and Open Protocol Package”, ANSSI-CC-PP-2015/04;

(5) Punctul de interacțiune „POI-PED-ONLY”, ANSSI-CC-PP-2015/05;

(6) Punctul de interacțiune „POI-PED-ONLY and Open Protocol Package”, ANSSI-CC-PP-2015/06;

(f) pentru categoria dispozitivelor hardware cu cutii de securitate:

(1) Modul criptografic pentru operațiunile cu semnături CSP cu copie de rezervă – PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

(2) Modul criptografic pentru operațiunile de generare de cheie CSP – PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

(3) Modul criptografic pentru operațiunile cu semnături CSP fără copie de rezervă – PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10;

ANEXA IV

Continuitatea asigurării și revizuirea certificatelor

IV.1 **Continuitatea asigurării: sfera de aplicare**

1. Următoarele cerințe privind asigurarea continuității se aplică activităților de menținere a certificării legate de următoarele aspecte:

   (a) o reevaluare în cazul în care un produs TIC certificat nemodificat îndeplinește în continuare cerințele de securitate;

   (b) o evaluare a impactului modificărilor aduse unui produs TIC în ceea ce privește certificarea acestuia;

   (c) dacă este inclusă în certificare, aplicarea de corecții în conformitate cu un proces evaluat de gestionare a corecțiilor;

   (d) dacă este inclusă, revizuirea gestionării ciclului de viață sau a proceselor de producție ale titularului certificatului.

2. Titularul unui certificat EUCC poate solicita revizuirea certificatului în următoarele cazuri:

   (a) certificatul EUCC urmează să expire în termen de nouă luni;

   (b) a avut loc o modificare fie a produsului TIC certificat, fie a unui alt factor care ar putea avea un impact asupra funcționalității sale de securitate;

   (c) titularul certificatului solicită ca evaluarea vulnerabilității să se efectueze din nou pentru a reconfirma nivelul de asigurare al certificatului EUCC asociat rezistenței produsului TIC la atacurile cibernetice actuale.

IV.2 **Reevaluarea**

1. În cazul în care este necesar să se evalueze impactul evoluțiilor amenințărilor din mediul unui produs TIC certificat nemodificat, se transmite organismului de certificare o cerere de reevaluare.

2. Reevaluarea se efectuează de către unitatea ITSEF care a fost implicată în evaluarea anterioară, prin reutilizarea tuturor rezultatelor sale care se aplică în continuare. Evaluarea se concentrează pe activitățile de asigurare care ar putea fi afectate de evoluțiile amenințărilor din mediul produsului TIC certificat, în special familia AVA_VAN relevantă și, în plus, familia ciclului de viață al asigurării, în cazul căreia se colectează din nou suficiente dovezi cu privire la menținerea mediului de dezvoltare.

3. Unitatea ITSEF descrie modificările și detaliază rezultatele reevaluării, împreună cu o actualizare a raportului tehnic de evaluare anterior.

4. Organismul de certificare examinează raportul tehnic de evaluare actualizat și întocmește un raport de reevaluare. Statutul certificatului inițial se modifică apoi în conformitate cu articolul 13.

5. Raportul de reevaluare și certificatul actualizat sunt puse la dispoziția autorității naționale de certificare a securității cibernetice și a ENISA în vederea publicării pe site-ul de certificare a securității cibernetice al acesteia din urmă.

IV.3 **Modificarea unui produs TIC certificat**

1. În cazul în care un produs TIC certificat a făcut obiectul unor modificări, titularul certificatului care dorește să mențină certificatul furnizează organismului de certificare un raport de analiză a impactului.

2. Raportul de analiză a impactului conține următoarele elemente:

   (a) o introducere care să conțină informațiile necesare pentru identificarea raportului de analiză a impactului și a obiectului evaluării care face obiectul modificărilor;

(b) descrierea modificărilor aduse produsului;

(c) identificarea elementelor de probă ale dezvoltatorului în cauză;

(d) o descriere a modificărilor elementelor de probă ale dezvoltatorului;

(e) constatările și concluziile privind impactul fiecărei modificări asupra nivelului de asigurare.

3. Organismul de certificare examinează modificările descrise în raportul de analiză a impactului pentru a valida impactul acestora asupra nivelului de asigurare al obiectului evaluării certificat, astfel cum este propus în concluziile raportului de analiză a impactului.

4. În urma examinării, organismul de certificare stabilește amploarea unei modificări ca fiind minoră sau majoră, în funcție de impactul acesteia.

5. În cazul în care modificările au fost confirmate de organismul de certificare ca fiind minore, se eliberează un nou certificat pentru produsul TIC modificat și se întocmește un raport de menținere a raportului de certificare inițial, în următoarele condiții:

(a) raportul de menținere este inclus ca subset al raportului de analiză a impactului, cu următoarele secțiuni:

(1) introducere;

(2) descrierea modificărilor;

(3) elementele de probă ale dezvoltatorului în cauză;

(b) data de valabilitate a noului certificat nu depășește data certificatului inițial.

6. Noul certificat – care include raportul de menținere – se pune la dispoziția ENISA în vederea publicării pe site-ul acesteia de certificare a securității cibernetice.

7. În cazul în care modificările au fost confirmate ca fiind majore, se efectuează o reevaluare în contextul evaluării anterioare, în care sunt reutilizate rezultatele evaluării anterioare care sunt în continuare valabile.

8. După finalizarea evaluării obiectului evaluării modificat, unitatea ITSEF întocmește un nou raport tehnic de evaluare. Organismul de certificare examinează raportul tehnic de evaluare actualizat și, dacă este cazul, întocmește un nou certificat împreună cu un nou raport de certificare.

9. Noul certificat și noul raport de certificare se transmit ENISA spre publicare.

IV.4 **Gestionarea corecțiilor**

1. Procedura de gestionare a corecțiilor prevede un proces structurat de actualizare a produselor TIC certificate. Procedura de gestionare a corecțiilor – inclusiv mecanismul încorporat în produsul TIC de către solicitantul certificării – poate fi utilizată după certificarea produsului TIC sub responsabilitatea organismului de evaluare a conformității.

2. Solicitantul certificării poate include în certificarea produsului TIC un mecanism de corecție ca parte a unei proceduri de gestionare certificate încorporate în produsul TIC dacă este îndeplinită una dintre următoarele condiții:

(a) funcționalitățile vizate de corecție se află în afara sferei obiectului evaluării produsului TIC certificat;

(b) corecția se referă la o modificare minoră prestabilită a produsului TIC certificat;

(c) corecția se referă la o vulnerabilitate confirmată cu efecte critice asupra securității produsului TIC certificat.

3. În cazul în care corecția se referă la o modificare majoră a obiectului evaluării produsului TIC certificat în ceea ce privește o vulnerabilitate nedetectată anterior care nu are efecte critice asupra securității produsului TIC, se aplică dispozițiile articolului 13.

4. Procedura de gestionare a corecțiilor pentru un produs TIC va fi compusă din următoarele elemente:

   (a) procesul de dezvoltare și implementare a corecției pentru produsul TIC;

   (b) mecanismul și funcțiile tehnice pentru adoptarea corecției la nivelul produsului TIC;

   (c) un set de activități de evaluare legate de eficacitatea și performanța mecanismului tehnic.

5. În timpul certificării produsului TIC:

   (a) solicitantul certificării produsului TIC furnizează descrierea procedurii de gestionare a corecțiilor;

   (b) ITSEF verifică următoarele elemente:

      (1) dacă dezvoltatorul a încorporat mecanismele de corecție în produsul TIC în conformitate cu procedura de gestionare a corecțiilor care a fost supusă certificării;

      (2) dacă limitele obiectului evaluării sunt separate astfel încât modificările aduse proceselor separate să nu afecteze securitatea obiectului evaluării;

      (3) dacă mecanismul tehnic de corecție funcționează în conformitate cu dispozițiile prezentei secțiuni și cu informațiile furnizate de solicitant;

   (c) dacă organismul de certificare include în raportul de certificare rezultatul procedurii evaluate de gestionare a corecțiilor.

6. Titularul certificatului poate aplica produsului TIC certificat în cauză corecția obținută în conformitate cu procedura certificată de gestionare a corecțiilor și ia următoarele măsuri în termen de 5 zile lucrătoare în următoarele cazuri:

   (a) în cazul menționat la punctul 2 litera (a), acesta raportează respectiva corecție organismului de certificare, care nu modifică certificatul EUCC în cauză;

   (b) în cazul menționat la punctul 2 litera (b), acesta transmite unității ITSEF respectiva corecție spre reexaminare. După primirea corecției, ITSEF informează organismul de certificare, iar acesta ia măsurile corespunzătoare cu privire la eliberarea unei noi versiuni a certificatului EUCC corespunzător și la actualizarea raportului de certificare;

   (c) în cazul menționat la punctul 2 litera (c), acesta transmite respectiva corecție unității ITSEF pentru reevaluarea necesară, dar poate implementa corecția în paralel. ITSEF informează organismul de certificare, după care acesta începe activitățile de certificare corespunzătoare.

ANEXA V

Conținutul raportului de certificare

V.1 **Raportul de certificare**

1. Pe baza rapoartelor tehnice de evaluare furnizate de ITSEF, organismul de certificare întocmește un raport de certificare care urmează să fie publicat împreună cu certificatul EUCC aferent.

2. Raportul de certificare este sursa informațiilor detaliate și practice cu privire la produsul TIC sau la categoria de produse TIC și cu privire la implementarea securizată a produsului TIC și, prin urmare, trebuie să includă toate informațiile care sunt relevante pentru utilizatori și pentru părțile interesate și care sunt publice și pot fi comunicate. Informațiile care sunt publice și pot fi comunicate pot fi menționate în raportul de certificare.

3. Raportul de certificare trebuie să conțină cel puțin următoarele secțiuni:

   (a) rezumatul;

   (b) identificarea produsului TIC sau a categoriei de produse TIC pentru profilurile de protecție;

   (c) serviciile de securitate;

   (d) ipotezele și clarificarea sferei de aplicare;

   (e) informații privind arhitectura informatică;

   (f) informații suplimentare în materie de securitate cibernetică, dacă este cazul;

   (g) testarea produselor TIC, dacă a fost efectuată;

   (h) dacă este cazul, o identificare a proceselor de gestionare a ciclului de viață și a instalațiilor de producție ale titularului certificatului;

   (i) rezultatele evaluării și informații privind certificatul;

   (j) rezumatul obiectivului de securitate al produsului TIC supus certificării;

   (k) atunci când este disponibilă, marca sau eticheta asociată sistemului;

   (l) bibliografie.

4. Rezumatul este un rezumat succint al întregului raport de certificare. Rezumatul oferă o imagine de ansamblu clară și concisă a rezultatelor evaluării și include următoarele informații:

   (a) denumirea produsului TIC evaluat, enumerarea componentelor produsului care fac parte din evaluare și versiunea produsului TIC;

   (b) denumirea unității ITSEF care a efectuat evaluarea și, după caz, lista subcontractanților;

   (c) data finalizării evaluării;

   (d) o trimitere la raportul tehnic de evaluare întocmit de ITSEF;

   (e) scurtă descriere a rezultatelor raportului de certificare, inclusiv:

      (1) versiunea și, dacă este cazul, ediția criteriilor comune aplicate evaluării;

      (2) pachetul aferent asigurării și componentele asigurării securității din criteriile comune, inclusiv nivelul AVA_VAN aplicat în timpul evaluării și nivelul de asigurare corespunzător, astfel cum se prevede la articolul 52 din Regulamentul (UE) 2019/881, la care se referă certificatul EUCC;

      (3) funcționalitatea de securitate a produsului TIC evaluat;

      (4) un rezumat al amenințărilor și al politicilor de securitate organizațională abordate de produsul TIC evaluat;

(5) cerințe de configurare speciale;

(6) ipoteze privind mediul de operare;

(7) dacă este cazul, prezența unei proceduri aprobate de gestionare a corecțiilor în conformitate cu anexa IV secțiunea IV.4;

(8) mesaj(e) de declinare a responsabilității.

5. Produsul TIC evaluat trebuie identificat în mod clar, inclusiv cu ajutorul următoarelor informații:

(a) denumirea produsului TIC evaluat;

(b) o enumerare a componentelor produsului TIC care fac parte din evaluare;

(c) numărul versiunii componentelor produsului TIC;

(d) identificarea cerințelor suplimentare pentru mediul de operare al produsului TIC certificat;

(e) numele și datele de contact ale titularului certificatului EUCC;

(f) dacă este cazul, procedura de gestionare a corecțiilor inclusă în certificat;

(g) link către site-ul web al titularului certificatului EUCC în care sunt furnizate informații suplimentare în materie de securitate cibernetică pentru produsul TIC certificat în conformitate cu articolul 55 din Regulamentul (UE) 2019/881.

6. Informațiile incluse în prezenta secțiune trebuie să fie cât mai exacte posibil, pentru a asigura o reprezentare completă și exactă a produsului TIC, care să poată fi reutilizată în viitoarele evaluări.

7. Secțiunea privind politica de securitate conține descrierea politicii de securitate a produsului TIC și a politicilor sau normelor pe care produsul TIC evaluat trebuie să le aplice sau să le respecte. Aceasta include o referință și o descriere a următoarelor politici:

(a) politica titularului certificatului de gestionare a vulnerabilităților;

(b) politica titularului certificatului privind continuitatea asigurării;

8. Dacă este cazul, politica poate include condițiile legate de utilizarea unei proceduri de gestionare a corecțiilor pe parcursul perioadei de valabilitate a certificatului.

9. Secțiunea privind ipotezele și clarificarea sferei de aplicare conține informații exhaustive cu privire la circumstanțele și obiectivele legate de utilizarea preconizată a produsului, astfel cum se menționează la articolul 7 alineatul (1) litera (c). Informațiile includ:

(a) ipoteze privind utilizarea și implementarea produsului TIC sub forma unor cerințe minime, cum ar fi cerințele de instalare și configurare corespunzătoare și cerințele de hardware care sunt îndeplinite;

(b) ipoteze privind mediul necesar pentru funcționarea conformă a produsului TIC;

10. Informațiile enumerate la punctul 9 trebuie să fie cât mai ușor de înțeles, pentru a permite utilizatorilor produsului TIC certificat să ia decizii în cunoștință de cauză cu privire la riscurile asociate utilizării acestuia.

11. Secțiunea privind informațiile legate de arhitectura informatică include o descriere detaliată a produsului TIC și a principalelor sale componente în conformitate cu designul subsistemelor ADV_TDS din criteriile comune.

12. Se furnizează o listă completă a informațiilor suplimentare privind securitatea cibernetică referitoare la produsul TIC în conformitate cu articolul 55 din Regulamentul (UE) 2019/881. Toate documentele relevante se indică prin numerele versiunilor.

13. Secțiunea privind testarea produselor TIC include următoarele informații:

(a) denumirea și punctul de contact ale autorității sau ale organismului care a eliberat certificatul, inclusiv ale autorității naționale de certificare a securității cibernetice de resort;

(b) numele unității ITSEF care a efectuat evaluarea, dacă este diferită de organismul de certificare;

(c) o identificare a componentelor de asigurare utilizate în standardele menționate la articolul 3;

(d) versiunea documentului ce reflectă stadiul actual al tehnologiei și criteriile suplimentare de evaluare a securității utilizate în evaluare;

(e) setările și configurația complete și precise ale produsului TIC în timpul evaluării, inclusiv notele operaționale și observațiile, dacă sunt disponibile;

(f) orice profil de protecție care a fost utilizat, inclusiv următoarele informații:

(1) autorul profilului de protecție;

(2) denumirea și identificatorul profilului de protecție;

(3) identificatorul certificatului profilului de protecție;

(4) denumirea și datele de contact ale organismului de certificare și ale unității ITSEF implicate în evaluarea profilului de protecție;

(5) pachetul (pachetele) aferent(e) asigurării necesar(e) pentru un produs care respectă profilul de protecție.

14. Rezultatele evaluării și informațiile privind secțiunea certificatului includ următoarele informații:

(a) confirmarea nivelului de asigurare atins, astfel cum se menționează la articolul 4 din prezentul regulament și la articolul 52 din Regulamentul (UE) 2019/881;

(b) cerințele de asigurare din standardele menționate la articolul 3 pe care produsul TIC sau profilul de protecție le îndeplinește efectiv, inclusiv nivelul AVA_VAN;

(c) descrierea detaliată a cerințelor de asigurare, precum și detalii privind modul în care produsul îndeplinește fiecare cerință;

(d) data eliberării și perioada de valabilitate a certificatului;

(e) identificatorul unic al certificatului.

15. Obiectivul de securitate trebuie să fie inclus în raportul de certificare sau menționat și rezumat în raportul de certificare și furnizat împreună cu raportul de certificare în scopul publicării.

16. Obiectivul de securitate poate fi sanitizat în conformitate cu secțiunea VI.2.

17. Marca sau eticheta asociată EUCC poate fi încorporată în raportul de certificare în conformitate cu normele și procedurile prevăzute la articolul 11.

18. Secțiunea bibliografică include trimiteri la toate documentele utilizate pentru întocmirea raportului de certificare. Informațiile respective includ cel puțin următoarele:

(a) criteriile de evaluare a securității, documentele ce reflectă stadiul actual al tehnologiei și specificațiile relevante suplimentare utilizate, precum și versiunea acestora;

(b) raportul tehnic de evaluare;

(c) raportul tehnic de evaluare pentru evaluarea compozită, dacă este cazul;

(d) documentația tehnică de referință;

(e) documentația dezvoltatorului utilizată în cadrul evaluării.

19. Pentru a garanta reproductibilitatea evaluării, toate documentele la care se face referire trebuie să fie identificate în mod unic cu ajutorul datei exacte a publicării și al numărului exact al versiunii.

V.2 **Sanitizarea unui obiectiv de securitate pentru publicare**

1. Obiectivul de securitate care trebuie inclus sau la care trebuie să se facă trimitere în raportul de certificare în temeiul secțiunii VI.1 punctul 1 poate fi sanitizat prin eliminarea sau parafrazarea informațiilor tehnice proprietare.

2. Obiectivul de securitate sanitizat astfel obținut trebuie să fie o reprezentare reală a versiunii sale originale complete. Aceasta înseamnă că obiectivul de securitate sanitizat nu poate omite informații necesare pentru a înțelege proprietățile de securitate ale obiectului evaluării și sfera de aplicare a evaluării.

3. Conținutul obiectivului de securitate sanitizat trebuie să respecte următoarele cerințe minime:
   (a) introducerea sa nu trebuie sanitizată, deoarece în general nu include informații proprietare;
   (b) obiectivul de securitate sanitizat trebuie să aibă un identificator unic diferit de versiunea sa originală completă;
   (c) descrierea obiectului evaluării poate fi redusă, deoarece poate include informații proprietare și informații detaliate cu privire la designul obiectului evaluării, care nu ar trebui publicate;
   (d) descrierea mediului de securitate al obiectului evaluării (ipoteze, amenințări, politici de securitate organizațională) nu se reduce, în măsura în care informațiile respective sunt necesare pentru înțelegerea sferei de aplicare a evaluării;
   (e) obiectivele de securitate nu se reduc, deoarece toate informațiile trebuie făcute publice pentru a se înțelege finalitatea obiectivului de securitate și a obiectului evaluării;
   (f) toate cerințele de securitate trebuie făcute publice. Notele de aplicare pot oferi informații cu privire la modul în care cerințele funcționale ale criteriilor comune menționate la articolul 3 au fost utilizate pentru a înțelege obiectivul de securitate;
   (g) specificarea rezumatului obiectului evaluării include toate funcțiile de securitate ale obiectului evaluării, dar informațiile proprietare suplimentare pot fi sanitizate;
   (h) se includ trimiteri la profilurile de protecție aplicate obiectului evaluării;
   (i) justificarea poate fi sanitizată pentru a elimina informațiile proprietare.

4. Chiar dacă obiectivul de securitate sanitizat nu este evaluat în mod oficial în conformitate cu standardele de evaluare menționate la articolul 3, organismul de certificare se asigură că acesta este conform cu obiectivul de securitate complet și evaluat și face trimitere în raportul de certificare atât la obiectivul de securitate complet, cât și la obiectivul de securitate sanitizat.

ANEXA VI

Sfera de aplicare și componența echipei în ceea ce privește evaluările colegiale

VI.1 **Sfera de aplicare a evaluării colegiale**

1. Sunt acoperite următoarele tipuri de evaluări colegiale:

   (a) tipul 1 – atunci când un organism de certificare desfășoară activități de certificare pentru nivelul AVA_VAN.3;

   (b) tipul 2 – atunci când un organism de certificare desfășoară activități de certificare legate de un domeniu tehnic dintre cele enumerate ca documente ce reflectă stadiul actual al tehnologiei în anexa I;

   (c) tipul 3 – atunci când un organism de certificare desfășoară activități de certificare peste nivelul AVA_VAN.3 utilizând un profil de protecție dintre cele enumerate ca documente ce reflectă stadiul actual al tehnologiei în anexa II sau III.

2. Organismul de certificare supus evaluării colegiale prezintă lista produselor TIC certificate care pot fi eligibile pentru revizuirea de către echipa de evaluare colegială, în conformitate cu următoarele norme:

   (a) produsele eligibile acoperă sfera de aplicare tehnică a autorizării organismului de certificare, iar cel puțin două evaluări diferite ale produselor cu nivelul de asigurare „ridicat” vor fi analizate prin intermediul evaluării colegiale, precum și un profil de protecție, în cazul în care organismul de certificare a eliberat un certificat pentru nivelul de asigurare „ridicat”;

   (b) pentru o evaluare colegială de tip 2, organismul de certificare prezintă cel puțin un produs pentru fiecare domeniu tehnic și pentru fiecare unitate ITSEF vizată;

   (c) pentru o evaluare colegială de tip 3, cel puțin un produs eligibil trebuie evaluat în conformitate cu profilul de protecție aplicabil și relevant.

VI.2 **Echipa de evaluare colegială**

1. Echipa de evaluare este formată din cel puțin doi experți selectați din organisme de certificare diferite și din state membre diferite care eliberează certificate pentru nivelul de asigurare „ridicat”. Experții ar trebui să demonstreze că dețin competențele relevante în ceea ce privește standardele menționate la articolul 3 și documentele ce reflectă stadiul actual al tehnologiei care fac obiectul evaluării colegiale.

2. În cazul delegării atribuției de eliberare a certificatelor sau în cazul aprobării prealabile, astfel cum se menționează la articolul 56 alineatul (6) din Regulamentul (UE) 2019/881, un expert din partea autorității naționale de certificare a securității cibernetice aflate în legătură cu organismul de certificare în cauză trebuie, de asemenea, să facă parte din echipa de experți selectați în conformitate cu alineatul (1) din prezenta secțiune.

3. Pentru o evaluare colegială de tip 2, membrii echipei trebuie să fie selectați dintre membrii organismelor de certificare autorizate pentru domeniul tehnic în cauză.

4. Fiecare membru al echipei de evaluare trebuie să aibă cel puțin doi ani de experiență în desfășurarea activităților de certificare în cadrul unui organism de certificare;

5. Pentru o evaluare colegială de tip 2 sau 3, fiecare membru al echipei de evaluare trebuie să aibă cel puțin doi ani de experiență în desfășurarea activităților de certificare pentru domeniul tehnic sau profilul de protecție relevant, să aibă cunoștințe de specialitate dovedite și să fi participat la autorizarea unei unități ITSEF.

6. Autoritatea națională de certificare a securității cibernetice care monitorizează și supraveghează organismul de certificare supus evaluării colegiale și cel puțin o autoritate națională de certificare a securității cibernetice al cărei organism de certificare nu face obiectul evaluării colegiale participă la evaluarea colegială în calitate de observatori. ENISA poate participa, de asemenea, la evaluarea colegială în calitate de observator.

7. Organismul de certificare supus evaluării colegiale este informat cu privire la componența echipei de evaluare colegială. În cazuri justificate, acesta poate contesta componența echipei de evaluare colegială și poate solicita revizuirea acesteia.

ANEXA VII

Conținutul unui certificat EUCC

Certificatul EUCC conține cel puțin:

(a) un identificator unic stabilit de organismul de certificare care eliberează certificatul;

(b) informații referitoare la produsul TIC certificat sau la profilul de protecție și la titularul certificatului, inclusiv:

(1) denumirea produsului TIC sau a profilului de protecție și, după caz, a obiectului evaluării;

(2) tipul de produs TIC sau de profil de protecție și, după caz, tipul de obiect al evaluării;

(3) versiunea produsului TIC sau a profilului de protecție;

(4) numele, adresa și datele de contact ale titularului certificatului;

(5) linkul către site-ul web al titularului certificatului care conține informațiile suplimentare în materie de securitate cibernetică menționate la articolul 55 din Regulamentul (UE) 2019/881;

(c) informații referitoare la evaluarea și certificarea produsului TIC sau a profilului de protecție, inclusiv:

(1) numele, adresa și datele de contact ale organismului de certificare care a eliberat certificatul;

(2) în cazul în care este diferită de organismul de certificare, numele unității ITSEF care a efectuat evaluarea;

(3) denumirea autorității naționale de certificare a securității cibernetice de resort;

(4) o trimitere la prezentul regulament;

(5) o trimitere la raportul de certificare asociat certificatului menționat în anexa V;

(6) nivelul de asigurare aplicabil în conformitate cu articolul 4;

(7) o trimitere la versiunea standardelor utilizate pentru evaluare menționate la articolul 3;

(8) identificarea nivelului de asigurare sau a pachetului specificat în standardele menționate la articolul 3 și în conformitate cu anexa VIII, inclusiv componentele de asigurare utilizate și nivelul AVA_VAN vizat;

(9) după caz, o trimitere la unul sau mai multe profiluri de protecție cu care este conform produsul TIC sau profilul de protecție;

(10) data eliberării;

(11) perioada de valabilitate a certificatului;

(d) marca și eticheta asociate certificatului în conformitate cu articolul 11.

ANEXA VIII

Declarația privind pachetul aferent asigurării

1. Contrar definițiilor din criteriile comune, o augmentare:

(a) nu se indică prin semnul „+”;

(b) se detaliază printr-o listă a tuturor componentelor vizate;

(c) se prezintă în detaliu în raportul de certificare.

2. Nivelul de asigurare confirmat într-un certificat EUCC poate fi completat de nivelul de asigurare al evaluării specificat la articolul 3 din prezentul regulament.

3. În cazul în care nivelul de asigurare confirmat într-un certificat EUCC nu se referă la o augmentare, certificatul EUCC indică unul dintre următoarele pachete:

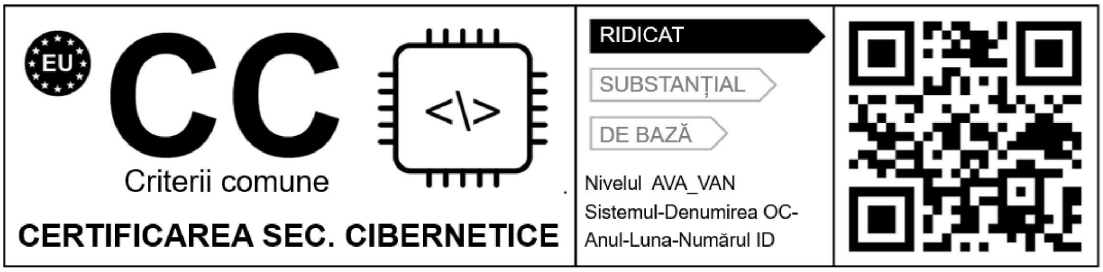
(a) „pachetul specific aferent asigurării”;

(b) „pachetul aferent asigurării care este conform cu un profil de protecție”, în cazul în care se face trimitere la un profil de protecție fără un nivel de asigurare a evaluării.

ANEXA IX

Marca și eticheta

1. Forma mărcii și a etichetei:



2. În caz de micșorare sau de mărire a mărcii și a etichetei, trebuie respectate proporțiile care rezultă din reprezentarea grafică de mai sus.

3. În cazul în care sunt prezente fizic, marca și eticheta trebuie să aibă o înălțime de cel puțin 5 mm.