REGOLAMENTO DI ESECUZIONE (UE) 2024/482 DELLA COMMISSIONE

del 31 gennaio 2024

recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») ([1]), in particolare l'articolo 49, paragrafo 7,

considerando quanto segue:

(1) Il presente regolamento specifica i ruoli, le norme e gli obblighi, nonché la struttura del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (*European Common Criteria-based cybersecurity certification* – EUCC) in conformità del quadro europeo di certificazione della cibersicurezza di cui al regolamento (UE) 2019/881. L'EUCC si fonda sull'accordo sul reciproco riconoscimento (ARR) dei certificati di valutazione della sicurezza delle tecnologie dell'informazione del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione ([2]) (*Senior Officials Group – Information Systems Security*, SOG-IS) e si basa sui criteri comuni, comprese le procedure e i documenti del gruppo.

(2) Il sistema dovrebbe basarsi su norme internazionali consolidate. I criteri comuni (*Common Criteria*) sono una norma internazionale per la valutazione della sicurezza delle informazioni pubblicata, ad esempio, come ISO/IEC 15408 *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*. Essa si basa sulla valutazione da parte di terzi e prevede sette livelli di garanzia della valutazione (*Evaluation Assurance Level* – EAL). I criteri comuni sono accompagnati dalla metodologia comune di valutazione (*Common Evaluation Methodology*), pubblicata, ad esempio come ISO/IEC 18045 - *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation*. Le specifiche e i documenti che applicano le disposizioni del presente regolamento possono riferirsi a una norma disponibile al pubblico che rispecchia la norma utilizzata per la certificazione nel quadro del presente regolamento, ad esempio i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione (*Common Criteria for Information Technology Security Evaluation*) e la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione (*Common Methodology for Information Technology Security Evaluation*).

(3) L'EUCC utilizza la famiglia di valutazione delle vulnerabilità dei criteri comuni (AVA_VAN), componenti da 1 a 5. I cinque componenti forniscono tutti i determinanti e tutte le dipendenze principali per l'analisi delle vulnerabilità dei prodotti TIC. Dal momento che corrispondono ai livelli di affidabilità del presente regolamento, i componenti consentono di compiere una scelta consapevole in merito all'affidabilità sulla base delle valutazioni dei requisiti di sicurezza e del rischio associato all'uso previsto del prodotto TIC che sono state effettuate. Il richiedente di un certificato EUCC dovrebbe fornire la documentazione relativa all'uso previsto del prodotto TIC e l'analisi dei livelli di rischio associati a tale uso per consentire all'organismo di valutazione della conformità di valutare l'idoneità del livello di affidabilità selezionato. Se le attività di valutazione e certificazione sono svolte dallo stesso organismo di valutazione della conformità, il richiedente dovrebbe presentare le informazioni richieste un'unica volta.

(4) Un settore tecnico costituisce un quadro di riferimento in cui rientra un gruppo di prodotti TIC con funzionalità di sicurezza specifiche e simili in grado di attenuare gli attacchi e nell'ambito del quale le caratteristiche sono comuni a un determinato livello di affidabilità. Esso indica nei documenti sullo stato dell'arte i requisiti di sicurezza specifici, nonché i metodi, le tecniche e gli strumenti di valutazione supplementari applicabili alla certificazione dei prodotti TIC che rientrano in tale settore tecnico. Pertanto promuove anche l'armonizzazione della valutazione dei prodotti

([1]) GU L 151 del 7.6.2019, pag. 15.

([2]) Accordo sul reciproco riconoscimento dei certificati di valutazione della sicurezza delle tecnologie dell'informazione, versione 3.0 del gennaio 2010, disponibile su sogis.eu, approvato dal gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione della Commissione europea in risposta al punto 3 della raccomandazione 95/144/CE del Consiglio, del 7 aprile 1995, su criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione (GU L 93 del 26.4.1995, pag. 27).

TIC contemplati. Attualmente sono ampiamente utilizzati due settori tecnici per la certificazione ai livelli AVA_VAN.4 e AVA_VAN.5. Il primo è quello relativo a «smart card e dispositivi analoghi» in cui porzioni significative della funzionalità di sicurezza richiesta dipendono da elementi hardware specifici, personalizzati e spesso separabili (ad esempio hardware per smart card, circuiti integrati, prodotti compositi per smart card, *Trusted Platform Modules* utilizzati nel *trusted computing* o carte tachigrafiche digitali). Il secondo è quello dei «dispositivi hardware con box di sicurezza» in cui porzioni significative della funzionalità di sicurezza richiesta dipendono da un involucro fisico hardware (denominato «box di sicurezza») progettato per resistere agli attacchi diretti (ad esempio terminali di pagamento, tachigrafi, contatori intelligenti, terminali di controllo degli accessi e moduli di sicurezza hardware).

(5) Al momento della richiesta di certificazione il richiedente dovrebbe mettere in relazione le proprie motivazioni per la selezione di un livello di affidabilità con gli obiettivi stabiliti nell'articolo 51 del regolamento (UE) 2019/881 e con la selezione dei componenti dal catalogo dei requisiti funzionali di sicurezza e dei requisiti di garanzia della sicurezza contenuto nei criteri comuni. Gli organismi di certificazione dovrebbero valutare l'adeguatezza del livello di affidabilità selezionato e garantire che esso sia commisurato al livello di rischio associato all'uso previsto del prodotto TIC.

(6) Nell'ambito dei criteri comuni la certificazione è effettuata rispetto a un traguardo di sicurezza che comprende una definizione del problema di sicurezza del prodotto TIC, nonché gli obiettivi di sicurezza che affrontano tale problema. Il problema di sicurezza fornisce dettagli sull'uso previsto del prodotto TIC e sui rischi associati a tale uso. Un insieme selezionato di requisiti di sicurezza risponde sia al problema sia agli obiettivi di sicurezza di un prodotto TIC.

(7) I profili di protezione sono uno strumento efficace per determinare a priori i criteri comuni applicabili a una determinata categoria di prodotti TIC e pertanto costituiscono anche un elemento essenziale nel processo di certificazione dei prodotti TIC contemplati dal profilo di protezione. Il profilo di protezione è utilizzato ai fini della valutazione dei futuri traguardi di sicurezza che rientrano nella categoria di prodotti TIC a cui si rivolge. I profili di protezione semplificano e migliorano ulteriormente l'efficienza del processo di certificazione dei prodotti TIC e aiutano gli utenti a specificare in modo corretto ed efficace le funzionalità degli stessi. I profili di protezione dovrebbero quindi essere considerati parte integrante del processo TIC che porta alla certificazione dei prodotti TIC.

(8) Affinché possano esercitare il proprio ruolo nel processo TIC a sostegno dello sviluppo e della messa a disposizione di un prodotto TIC certificato, i profili di protezione dovrebbero anch'essi poter essere certificati indipendentemente dalla certificazione del prodotto TIC specifico che vi rientra. È quindi essenziale che ai profili di protezione sia applicato almeno lo stesso livello di controllo previsto per i traguardi di sicurezza al fine di garantire un elevato livello di cibersicurezza. I profili di protezione dovrebbero essere valutati e certificati separatamente dal relativo prodotto TIC e unicamente applicando la classe di affidabilità per i profili di protezione (APE) e, ove applicabile, per le configurazioni dei profili di protezione (ACE) di cui ai criteri comuni e alla metodologia comune di valutazione. In considerazione del loro importante e delicato ruolo di riferimento nella certificazione dei prodotti TIC, tali profili dovrebbero essere certificati solo dagli enti pubblici o da un organismo di certificazione che ha ricevuto la previa approvazione dell'autorità nazionale di certificazione della cibersicurezza per tale profilo di protezione specifico. Dato il loro ruolo fondamentale per la certificazione al livello di affidabilità «elevato», in particolare al di fuori dei settori tecnici, i profili di protezione dovrebbero essere elaborati come documenti sullo stato dell'arte che dovrebbero essere approvati dal gruppo europeo per la certificazione della cibersicurezza (*European Cybersecurity Certification Group*, ECCG).

(9) Le autorità nazionali di certificazione della cibersicurezza dovrebbero includere i profili di protezione certificati nel monitoraggio della conformità e della compliance nell'ambito dell'EUCC. Se le metodologie, gli strumenti e le competenze applicati agli approcci di valutazione dei prodotti TIC sono disponibili per profili di protezione certificati specifici, i settori tecnici possono basarsi su tali profili di protezione specifici.

(10) Al fine di garantire un elevato livello di fiducia e affidabilità dei prodotti TIC certificati, a norma del presente regolamento non dovrebbe essere consentita l'autovalutazione. Dovrebbe essere consentita solo la valutazione di conformità da parte di terzi effettuata dalle strutture di valutazione della sicurezza delle tecnologie dell'informazione (*Information Technology Security Evaluation Facilities* – ITSEF) e dagli organismi di certificazione.

(11) La comunità SOG-IS ha fornito interpretazioni e approcci comuni per l'applicazione dei criteri comuni e della metodologia comune di valutazione nella certificazione, in particolare per il livello di affidabilità «elevato» perseguito dai settori tecnici «smart card e dispositivi simili» e «dispositivi hardware con box di sicurezza». Il riutilizzo di tali documenti di sostegno nel sistema EUCC garantisce una transizione agevole dai sistemi SOG-IS attuati a livello nazionale al sistema EUCC armonizzato. Pertanto il presente regolamento dovrebbe includere metodologie di valutazione armonizzate di rilevanza generale per tutte le attività di certificazione. Inoltre la Commissione dovrebbe poter richiedere al gruppo europeo per la certificazione della cibersicurezza di adottare un parere che approvi e raccomandi l'applicazione delle metodologie di valutazione specificate nei documenti sullo stato dell'arte per la certificazione del prodotto TIC o del profilo di protezione nell'ambito del sistema EUCC. Nell'allegato I del presente regolamento figurano pertanto i documenti sullo stato dell'arte per le attività di valutazione svolte dagli organismi di valutazione della conformità. Il gruppo europeo per la certificazione della cibersicurezza dovrebbe approvare e tenere aggiornati i documenti sullo stato dell'arte. Nell'ambito della certificazione è opportuno ricorrere a tali documenti. Un organismo di valutazione della conformità può non ricorrere a tali documenti solo in casi eccezionali e debitamente giustificati e a determinate condizioni, in particolare previa approvazione dell'autorità nazionale di certificazione della cibersicurezza.

(12) La certificazione dei prodotti TIC al livello AVA_VAN 4 o 5 dovrebbe essere possibile solo a determinate condizioni e qualora sia disponibile una metodologia di valutazione specifica. La metodologia di valutazione specifica può essere contenuta in documenti sullo stato dell'arte pertinenti per il settore tecnico in questione o in profili di protezione specifici adottati come documenti sullo stato dell'arte che sono pertinenti per la categoria di prodotti in questione. La certificazione a tali livelli di affidabilità dovrebbe essere possibile solo in casi eccezionali e debitamente giustificati e a determinate condizioni, in particolare previa approvazione dell'autorità nazionale di certificazione della cibersicurezza, anche della metodologia di valutazione applicabile. Tali casi eccezionali e debitamente giustificati possono verificarsi qualora la legislazione dell'Unione o nazionale richieda la certificazione di un prodotto TIC al livello AVA_VAN 4 o 5. Analogamente, i profili di protezione possono essere certificati senza che siano applicati i documenti sullo stato dell'arte pertinenti in casi eccezionali e debitamente giustificati e a determinate condizioni, in particolare previa approvazione dell'autorità nazionale di certificazione della cibersicurezza, anche della metodologia di valutazione applicabile.

(13) I marchi e le etichette utilizzati nel quadro dell'EUCC hanno lo scopo di dimostrare visibilmente agli utenti l'affidabilità del prodotto TIC certificato e a consentire loro di compiere una scelta consapevole quando acquistano prodotti TIC. L'uso di marchi ed etichette dovrebbe essere soggetto anche alle norme e alle condizioni stabilite dalla norma ISO/IEC 17065 e, ove applicabile, dalla norma ISO/IEC 17030 con i relativi orientamenti.

(14) Gli organismi di certificazione dovrebbero decidere in merito alla durata della validità dei certificati tenendo conto del ciclo di vita del prodotto TIC in questione. Tale durata non dovrebbe superare i cinque anni. Le autorità nazionali di certificazione della cibersicurezza dovrebbero adoperarsi per armonizzare la durata della validità nell'Unione.

(15) Se l'ambito di applicazione di un certificato EUCC esistente è ridotto, il certificato deve essere revocato e dovrebbe essere rilasciato un nuovo certificato con il nuovo ambito di applicazione in modo da garantire che gli utenti siano chiaramente informati in merito all'attuale ambito di applicazione e al livello di affidabilità del certificato di un determinato prodotto TIC.

(16) La certificazione dei profili di protezione si differenzia da quella dei prodotti TIC in quanto riguarda un processo TIC. Dal momento che un profilo di protezione riguarda una categoria di prodotti TIC, la sua valutazione e certificazione non possono essere effettuate sulla base di un singolo prodotto TIC. Poiché un profilo di protezione unifica i requisiti generali di sicurezza relativi a una categoria di prodotti TIC ed è indipendente dalla manifestazione del prodotto TIC da parte del suo fornitore, il periodo di validità di un certificato EUCC per un profilo di protezione dovrebbe in linea di principio essere di almeno cinque anni e dovrebbe poter essere prorogato per tutto il ciclo di vita del profilo di protezione.

(17) Per organismo di valutazione della conformità si intende un organismo che svolge attività di valutazione della conformità, fra cui tarature, prove, certificazioni e ispezioni. Al fine di garantire una qualità elevata dei servizi, nel presente regolamento si specifica che le attività di prova, da un lato, e le attività di certificazione e ispezione, dall'altro, dovrebbero essere svolte da soggetti che operano in modo indipendente l'uno dall'altro, ossia, rispettivamente, dalle strutture di valutazione della sicurezza delle tecnologie dell'informazione (ITSEF) e dagli organismi di certificazione. Entrambi i tipi di organismi di valutazione della conformità dovrebbero essere accreditati e, in determinate situazioni, autorizzati.

(18) Un organismo di certificazione dovrebbe essere accreditato in conformità della norma ISO/IEC 17065 dall'organismo nazionale di accreditamento per i livelli di affidabilità «sostanziale» ed «elevato». Oltre all'accreditamento conformemente al regolamento (UE) 2019/881, in combinato disposto con il regolamento (CE) n. 765/2008, gli organismi di valutazione della conformità dovrebbero soddisfare requisiti specifici al fine di garantire di possedere la competenza tecnica per valutare i requisiti di cibersicurezza nell'ambito del livello di affidabilità «elevato» dell'EUCC, e ciò è confermato mediante un'«autorizzazione». Al fine di sostenere il processo di autorizzazione l'ENISA, previa approvazione da parte del gruppo europeo per la certificazione della cibersicurezza, dovrebbe elaborare e pubblicare i pertinenti documenti sullo stato dell'arte.

(19) La competenza tecnica di un'ITSEF dovrebbe essere valutata attraverso l'accreditamento del laboratorio di prova in conformità della norma ISO/IEC 17025 e integrata dalla norma ISO/IEC 23532-1 per l'intera serie di attività di valutazione pertinenti al livello di affidabilità e specificate nella norma ISO/IEC 18045 congiuntamente alla norma ISO/IEC 15408. Sia l'organismo di certificazione che l'ITSEF dovrebbero istituire e mantenere in essere un adeguato sistema di gestione delle competenze del personale basato sulla norma ISO/IEC 19896-1 per gli elementi e i livelli di competenza e per la valutazione della competenza. Per quanto riguarda il livello di conoscenza, competenze, esperienza e istruzione, i requisiti applicabili per i valutatori dovrebbero essere tratti dalla norma ISO/IEC 19896-3. È opportuno dimostrare le disposizioni e le misure equivalenti che trattano gli scostamenti da tali sistemi di gestione delle competenze in linea con gli obiettivi del sistema.

(20) Per essere autorizzata, l'ITSEF dovrebbe dimostrare di essere in grado di determinare l'assenza di vulnerabilità note, l'attuazione corretta e coerente delle funzionalità di sicurezza avanzate per la tecnologia specifica in questione e la resistenza agli attacchi commessi da soggetti qualificati del prodotto TIC oggetto degli attacchi. Inoltre, per le autorizzazioni nel settore tecnico «smart card e dispositivi simili», l'ITSEF dovrebbe anche dimostrare di possedere le capacità tecniche necessarie per lo svolgimento delle attività di valutazione e dei relativi compiti, come definito nel documento di sostegno *Minimum ITSEF requirements for security evaluations of smart cards and similar devices* ([3]) nell'ambito dei criteri comuni. Per l'autorizzazione nel settore tecnico «dispositivi hardware con box di sicurezza», l'ITSEF dovrebbe altresì dimostrare di possedere i requisiti tecnici minimi necessari per lo svolgimento delle attività di valutazione e dei relativi compiti per quanto riguarda i dispositivi hardware con box di sicurezza, come raccomandato dall'ECCG. Nel contesto dei requisiti minimi l'ITSEF dovrebbe essere in grado di condurre i diversi tipi di attacchi indicati nel documento di sostegno *Application of Attack Potential to Hardware Devices with Security Boxes* nell'ambito dei criteri comuni. Tali capacità comprendono le conoscenze e le competenze del valutatore, nonché gli strumenti e i metodi di valutazione necessari per determinare e valutare i diversi tipi di attacchi.

(21) L'autorità nazionale di certificazione della cibersicurezza dovrebbe monitorare il rispetto, da parte degli organismi di certificazione, delle ITSEF e dei titolari di certificati, degli obblighi derivanti dal presente regolamento e dal regolamento (UE) 2019/881. A tal fine dovrebbe utilizzare qualsiasi fonte di informazione appropriata, comprese le informazioni ricevute dai partecipanti al processo di certificazione e quelle raccolte nell'ambito delle proprie indagini.

(22) Gli organismi di certificazione dovrebbero collaborare con le autorità di vigilanza del mercato competenti e tenere conto di tutte le informazioni sulle vulnerabilità che potrebbero essere pertinenti per i prodotti TIC per i quali hanno rilasciato i certificati. Gli organismi di certificazione dovrebbero monitorare i profili di protezione che hanno certificato per verificare se i requisiti di sicurezza stabiliti per una categoria di prodotti TIC continuino a tenere conto degli ultimi sviluppi del panorama delle minacce.

(23) A sostegno del monitoraggio della compliance le autorità nazionali di certificazione della cibersicurezza dovrebbero cooperare con le autorità di vigilanza del mercato competenti in conformità dell'articolo 58 del regolamento (UE) 2019/881 e del regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio ([4]). Gli operatori economici dell'Unione sono tenuti a condividere le informazioni e a collaborare con le autorità di vigilanza del mercato a norma dell'articolo 4, paragrafo 3, del regolamento (UE) 2019/1020.

([3]) *Joint Interpretation Library, Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices*, versione 2.1 del febbraio 2020, disponibile sul sito web sogis.eu.

([4]) Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011 (GU L 169 del 25.6.2019, pag. 1).

(24) Gli organismi di certificazione dovrebbero monitorare la compliance dei titolari di un certificato e la conformità di tutti i certificati rilasciati nell'ambito dell'EUCC. Il monitoraggio dovrebbe garantire che tutte le relazioni di valutazione fornite da un'ITSEF e le conclusioni in esse contenute, nonché i criteri e i metodi di valutazione, siano applicati in modo coerente e corretto in tutte le attività di certificazione.

(25) Qualora siano rilevati potenziali problemi di non compliance che riguardano un prodotto TIC certificato, è importante garantire una risposta proporzionata. I certificati possono quindi essere sospesi. La sospensione dovrebbe comportare alcune limitazioni per quanto riguarda la promozione e l'uso del prodotto TIC in questione, ma non incidere sulla validità del certificato. La sospensione dovrebbe essere notificata agli acquirenti dei prodotti TIC in questione da parte del titolare del certificato UE, mentre le autorità di vigilanza del mercato competenti dovrebbero essere informate al riguardo dall'autorità nazionale di certificazione della cibersicurezza competente. Per informare il pubblico, l'ENISA dovrebbe pubblicare le informazioni sulla sospensione su un sito web apposito.

(26) Il titolare di un certificato EUCC dovrebbe attuare le procedure di gestione delle vulnerabilità necessarie e garantire che tali procedure siano integrate all'interno della propria organizzazione. Qualora venga a conoscenza di una potenziale vulnerabilità, il titolare del certificato EUCC dovrebbe eseguire un'analisi dell'impatto della vulnerabilità. Se quest'ultima conferma che la vulnerabilità può essere sfruttata, il titolare del certificato dovrebbe inviare una relazione della valutazione all'organismo di certificazione, che a sua volta dovrebbe informare l'autorità nazionale di certificazione della cibersicurezza. La relazione dovrebbe fornire informazioni in merito all'impatto della vulnerabilità, alle modifiche o alle soluzioni correttive necessarie, comprese le possibili implicazioni più ampie della vulnerabilità, nonché alle soluzioni correttive per altri prodotti. La norma EN ISO/IEC 29147 dovrebbe integrare, ove necessario, la procedura per la divulgazione delle vulnerabilità.

(27) Ai fini della certificazione, gli organismi di valutazione della conformità e le autorità nazionali di certificazione della cibersicurezza ottengono dati riservati e sensibili e segreti aziendali, anche relativi alla proprietà intellettuale o al monitoraggio della compliance, che richiedono un'adeguata protezione. Essi dovrebbero pertanto possedere le competenze e le conoscenze tecniche necessarie e istituire sistemi per la protezione delle informazioni. I requisiti e le condizioni per la protezione delle informazioni dovrebbero essere soddisfatti sia per l'accreditamento che per l'autorizzazione.

(28) L'ENISA dovrebbe fornire l'elenco dei profili di protezione certificati sul suo sito web relativo alla certificazione della cibersicurezza e indicarne lo stato in conformità del regolamento (UE) 2019/881.

(29) Il presente regolamento stabilisce le condizioni per gli accordi sul reciproco riconoscimento con i paesi terzi. Tali accordi possono essere bilaterali o multilaterali e dovrebbero sostituire accordi analoghi attualmente in vigore. Al fine di facilitare un'agevole transizione verso tali accordi sul reciproco riconoscimento, per un periodo limitato gli Stati membri possono mantenere gli accordi di cooperazione esistenti con paesi terzi.

(30) Gli organismi di certificazione che rilasciano certificati EUCC di livello di affidabilità «elevato», nonché le relative ITSEF associate, dovrebbero essere sottoposti a valutazioni inter pares. L'obiettivo delle valutazioni inter pares dovrebbe essere quello di determinare se la costituzione e le procedure di un organismo di certificazione oggetto di valutazione inter pares continuino a rispettare i requisiti del sistema EUCC. Tali valutazioni inter pares sono diverse dalle valutazioni inter pares tra le autorità nazionali di certificazione della cibersicurezza di cui all'articolo 59 del regolamento (UE) 2019/881. Le valutazioni inter pares dovrebbero accertare che gli organismi di certificazione lavorino in modo armonizzato e producano la stessa qualità di certificati, nonché individuare qualsiasi potenziale punto di forza o punto debole nelle prestazioni degli organismi di certificazione, anche ai fini dello scambio delle migliori pratiche. Poiché esistono diversi tipi di organismi di certificazione, è opportuno consentire diversi tipi di valutazioni inter pares. Nei casi più complessi, come nel caso di organismi di certificazione che rilasciano certificati per livelli AVA_VAN differenti, è possibile utilizzare diversi tipi di valutazione inter pares purché siano soddisfatti tutti i requisiti.

(31) Il gruppo europeo per la certificazione della cibersicurezza dovrebbe svolgere un ruolo importante nel mantenimento del sistema. Ciò dovrebbe essere realizzato, tra l'altro, attraverso la cooperazione con il settore privato e la creazione di sottogruppi specializzati, nonché i lavori preparatori e l'assistenza pertinenti richiesti dalla Commissione. Il gruppo europeo per la certificazione della cibersicurezza svolge un ruolo importante nell'approvazione dei documenti sullo stato dell'arte. Nell'approvazione e nell'adozione dei documenti sullo stato dell'arte è opportuno tenere debitamente conto degli elementi di cui all'articolo 54, paragrafo 1, lettera c), del

regolamento (UE) 2019/881. I settori tecnici e i documenti sullo stato dell'arte dovrebbero essere pubblicati nell'allegato I del presente regolamento. I profili di protezione che sono stati adottati come documenti sullo stato dell'arte dovrebbero essere pubblicati nell'allegato II. Al fine di garantire la dinamicità di tali allegati, la Commissione può modificarli conformemente alla procedura di cui all'articolo 66, paragrafo 2, del regolamento (UE) 2019/881 e tenendo conto del parere del gruppo europeo per la certificazione della cibersicurezza. L'allegato III contiene i profili di protezione raccomandati, che al momento dell'entrata in vigore del presente regolamento non sono documenti sullo stato dell'arte. Tali profili dovrebbero essere pubblicati sul sito web dell'ENISA di cui all'articolo 50, paragrafo 1, del regolamento (UE) 2019/881.

(32) Il presente regolamento dovrebbe iniziare ad applicarsi 12 mesi dopo la sua entrata in vigore. I requisiti del capo IV e dell'allegato V non richiedono un periodo di transizione e dovrebbero pertanto applicarsi a partire dall'entrata in vigore del presente regolamento.

(33) Le misure previste dal presente regolamento sono conformi al parere del comitato europeo per la certificazione della cibersicurezza istituito dall'articolo 66 del regolamento (UE) 2019/881,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

Il presente regolamento istituisce il sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

Il presente regolamento si applica a tutti i prodotti delle tecnologie dell'informazione e della comunicazione (TIC), compresa la relativa documentazione, che sono presentati ai fini della certificazione nel quadro dell'EUCC, nonché a tutti i profili di protezione che sono presentati ai fini della certificazione come parte del processo TIC alla base della certificazione dei prodotti TIC.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

(1) «criteri comuni»: i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione quali definiti nella norma ISO/IEC 15408;

(2) «metodologia comune di valutazione»: la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione quale definita nella norma ISO/IEC 18045;

(3) «oggetto della valutazione»: un prodotto TIC o una sua parte, o un profilo di protezione come parte di un processo TIC, sottoposto a valutazione di cibersicurezza allo scopo di ricevere la certificazione EUCC;

(4) «traguardo di sicurezza»: una dichiarazione dei requisiti di sicurezza dipendenti dall'implementazione per uno specifico prodotto TIC;

(5) «profilo di protezione»: un processo TIC che stabilisce i requisiti di sicurezza per una categoria specifica di prodotti TIC, che affronta le esigenze di sicurezza indipendenti dall'implementazione e che può essere utilizzato per valutare i prodotti TIC rientranti in tale categoria specifica ai fini della loro certificazione;

(6) «relazione tecnica di valutazione»: un documento prodotto da un'ITSEF per presentare i risultati, i verdetti e le giustificazioni ottenuti durante la valutazione di un prodotto TIC o di un profilo di protezione in conformità delle norme e degli obblighi stabiliti nel presente regolamento;

(7) «ITSEF»: una struttura di valutazione della sicurezza delle tecnologie dell'informazione, che è un organismo di valutazione della conformità quale definito nell'articolo 2, punto 13), del regolamento (CE) n. 765/2008, che svolge attività di valutazione;

(8) «livello AVA_VAN»: un livello di analisi della vulnerabilità dell'affidabilità che indica il grado delle attività di valutazione della cibersicurezza svolte per determinare il livello di resistenza rispetto alla potenziale possibilità di sfruttare i difetti o i punti deboli dell'oggetto della valutazione nel suo ambiente operativo, come stabilito nei criteri comuni;

(9) «certificato EUCC»: un certificato di cibersicurezza rilasciato nell'ambito dell'EUCC per prodotti TIC o per profili di protezione che possono essere utilizzati esclusivamente nel processo TIC di certificazione dei prodotti TIC;

(10) «prodotto composito»: un prodotto TIC che è valutato insieme a un altro prodotto TIC sottostante che ha già ricevuto un certificato EUCC e dalla cui funzionalità di sicurezza dipende il prodotto TIC composito;

(11) «autorità nazionale di certificazione della cibersicurezza»: un'autorità designata da uno Stato membro a norma dell'articolo 58, paragrafo 1, del regolamento (UE) 2019/881;

(12) «organismo di certificazione»: un organismo di valutazione della conformità quale definito nell'articolo 2, punto 13), del regolamento (CE) n. 765/2008, che svolge attività di certificazione;

(13) «settore tecnico»: un quadro tecnico comune relativo a una particolare tecnologia per la certificazione armonizzata con una serie di requisiti di sicurezza caratteristici;

(14) «documento sullo stato dell'arte»: documento in cui sono specificati i metodi, le tecniche e gli strumenti di valutazione che si applicano alla certificazione dei prodotti TIC, o ai requisiti di sicurezza di una categoria generica di prodotti TIC, o a qualsiasi altro requisito necessario per la certificazione, al fine di armonizzare la valutazione, in particolare dei settori tecnici o dei profili di protezione;

(15) «autorità di vigilanza del mercato»: un'autorità quale definita nell'articolo 3, punto 4), del regolamento (UE) 2019/1020.

Articolo 3

Norme di valutazione

Alle valutazioni effettuate nell'ambito del sistema EUCC si applicano le norme seguenti:

(a) i criteri comuni;

(b) la metodologia comune di valutazione.

Articolo 4

Livelli di affidabilità

1. Gli organismi di certificazione rilasciano certificati EUCC con un livello di affidabilità «sostanziale» o «elevato».

2. I certificati EUCC al livello di affidabilità «sostanziale» corrispondono ai certificati relativi al livello AVA_VAN 1 o 2.

3. I certificati EUCC al livello di affidabilità «elevato» corrispondono ai certificati relativi al livello AVA_VAN 3, 4 o 5.

4. Il livello di affidabilità confermato in un certificato EUCC distingue tra l'uso conforme e l'uso aumentato dei componenti dell'affidabilità specificati nei criteri comuni in conformità dell'allegato VIII.

5. Gli organismi di valutazione della conformità applicano le componenti dell'affidabilità da cui dipende il livello AVA_VAN selezionato in conformità delle norme di cui all'articolo 3.

Articolo 5

Metodi di certificazione dei prodotti TIC

1. La certificazione di un prodotto TIC è effettuata rispetto al suo traguardo di sicurezza:

(a) come definito dal richiedente; oppure

(b) integrando un profilo di protezione certificato come parte del processo TIC, qualora il prodotto TIC rientri nella categoria di prodotti TIC contemplata da tale profilo di protezione.

2. I profili di protezione sono certificati al solo scopo di certificare i prodotti TIC che rientrano nella categoria specifica di prodotti TIC contemplata dal profilo di protezione.

Articolo 6

Autovalutazione della conformità

Non è consentita l'autovalutazione della conformità ai sensi dell'articolo 53 del regolamento (UE) 2019/881.

CAPO II

CERTIFICAZIONE DEI PRODOTTI TIC

SEZIONE I

Norme e requisiti specifici per la valutazione

Articolo 7

Criteri e metodi di valutazione dei prodotti TIC

1. Un prodotto TIC presentato ai fini della certificazione è valutato almeno conformemente a quanto segue:

(a) gli elementi applicabili delle norme di cui all'articolo 3;

(b) le classi dei requisiti di garanzia della sicurezza per la valutazione della vulnerabilità e le prove funzionali indipendenti, come stabilito nelle norme di valutazione di cui all'articolo 3;

(c) il livello di rischio associato all'uso previsto dei prodotti TIC in questione a norma dell'articolo 52 del regolamento (UE) 2019/881 e le loro funzioni di sicurezza a sostegno degli obiettivi di sicurezza di cui all'articolo 51 del medesimo regolamento;

(d) i documenti sullo stato dell'arte applicabili di cui all'allegato I; e

(e) i profili di protezione certificati applicabili di cui all'allegato II.

2. In casi eccezionali e debitamente giustificati, un organismo di valutazione della conformità può chiedere di non applicare il pertinente documento sullo stato dell'arte. In tali casi l'organismo di valutazione della conformità informa l'autorità nazionale di certificazione della cibersicurezza fornendo una giustificazione debitamente motivata della propria richiesta. L'autorità nazionale di certificazione della cibersicurezza valuta se l'eccezione sia giustificata e, in caso

affermativo, la approva. In attesa della decisione dell'autorità nazionale di certificazione della cibersicurezza, l'organismo di valutazione della conformità non rilascia alcun certificato. L'autorità nazionale di certificazione della cibersicurezza notifica senza indebito ritardo l'eccezione approvata al gruppo europeo per la certificazione della cibersicurezza, che può formulare un parere. L'autorità nazionale di certificazione della cibersicurezza tiene nella massima considerazione il parere del gruppo europeo per la certificazione della cibersicurezza.

3. La certificazione dei prodotti TIC al livello AVA_VAN 4 o 5 è possibile solo negli scenari seguenti:

(a) se rientra in uno dei settori tecnici di cui all'allegato I, il prodotto TIC è valutato conformemente ai documenti sullo stato dell'arte applicabili di tali settori tecnici;

(b) se rientra in una categoria di prodotti TIC contemplati da un profilo di protezione certificato che comprende il livello AVA_VAN 4 o 5 e che figura nell'allegato II come profilo di protezione avanzato, il prodotto TIC è valutato conformemente alla metodologia di valutazione specificata per tale profilo di protezione;

(c) se le lettere a) e b) del presente paragrafo non sono applicabili e se l'inclusione di un settore tecnico nell'allegato I o di un profilo di protezione certificato nell'allegato II è improbabile nel prossimo futuro, e solo in casi eccezionali e debitamente giustificati, alle condizioni di cui al paragrafo 4.

4. Qualora ritenga di trovarsi di fronte a un caso eccezionale e debitamente giustificato di cui al paragrafo 3, lettera c), l'organismo di valutazione della conformità notifica la certificazione prevista all'autorità nazionale di certificazione della cibersicurezza fornendo una giustificazione e una proposta di metodologia di valutazione. L'autorità nazionale di certificazione della cibersicurezza valuta se l'eccezione sia giustificata e, in caso affermativo, approva o modifica la metodologia di valutazione che dovrà essere applicata dall'organismo di valutazione della conformità. In attesa della decisione dell'autorità nazionale di certificazione della cibersicurezza, l'organismo di valutazione della conformità non rilascia alcun certificato. L'autorità nazionale di certificazione della cibersicurezza segnala senza indebito ritardo la certificazione prevista al gruppo europeo per la certificazione della cibersicurezza, che può formulare un parere. L'autorità nazionale di certificazione della cibersicurezza tiene nella massima considerazione il parere del gruppo europeo per la certificazione della cibersicurezza.

5. Nel caso di un prodotto TIC sottoposto a una valutazione di prodotto composito conformemente ai pertinenti documenti sullo stato dell'arte, l'ITSEF che ha effettuato la valutazione del prodotto TIC sottostante condivide le informazioni pertinenti con l'ITSEF che effettua la valutazione del prodotto TIC composito.

SEZIONE II

Rilascio, rinnovo e revoca dei certificati EUCC

Articolo 8

Informazioni necessarie per la certificazione

1. Il richiedente la certificazione nel quadro dell'EUCC fornisce o mette altrimenti a disposizione dell'organismo di certificazione e dell'ITSEF tutte le informazioni necessarie per le attività di certificazione.

2. Le informazioni di cui al paragrafo 1 comprendono tutti gli elementi di prova pertinenti in conformità delle sezioni relative alle «Azioni dello sviluppatore» nel formato appropriato, come indicato nelle sezioni «Contenuto e presentazione dell'elemento di prova» dei criteri comuni e della metodologia comune di valutazione per il livello di affidabilità selezionato e i requisiti di garanzia della sicurezza associati. Gli elementi di prova includono, se necessario, dettagli sul prodotto TIC e sul suo codice sorgente in conformità del presente regolamento, fatte salve le salvaguardie contro la divulgazione non autorizzata.

3. I richiedenti la certificazione possono fornire all'organismo di certificazione e all'ITSEF risultati della valutazione adeguati provenienti da una precedente certificazione a norma:

(a) del presente regolamento;

(b) di un altro sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881;

(c) di un sistema nazionale di cui all'articolo 49 del presente regolamento.

4. Se i risultati della valutazione sono pertinenti ai suoi compiti, l'ITSEF può riutilizzarli, a condizione che siano conformi ai requisiti applicabili e che la loro autenticità sia confermata.

5. Se l'organismo di certificazione consente di sottoporre il prodotto a una certificazione di prodotto composito, il richiedente la certificazione mette a disposizione dell'organismo di certificazione e dell'ITSEF tutti gli elementi necessari, se del caso, in conformità del documento sullo stato dell'arte.

6. I richiedenti la certificazione forniscono inoltre all'organismo di certificazione e all'ITSEF le informazioni seguenti:

(a) il link al proprio sito web contenente le informazioni supplementari sulla cibersicurezza di cui all'articolo 55 del regolamento (UE) 2019/881;

(b) una descrizione delle procedure di gestione e divulgazione delle vulnerabilità del richiedente.

7. Tutta la documentazione pertinente di cui al presente articolo è conservata dall'organismo di certificazione, dall'ITSEF e dal richiedente per un periodo di cinque anni dopo la scadenza del certificato.

Articolo 9

Condizioni per il rilascio di un certificato EUCC

1. Gli organismi di certificazione rilasciano un certificato EUCC se sono soddisfatte tutte le condizioni seguenti:

(a) la categoria di prodotto TIC rientra nell'ambito di applicazione dell'accreditamento, ed eventualmente dell'autorizzazione, dell'organismo di certificazione e dell'ITSEF coinvolti nella certificazione;

(b) il richiedente la certificazione ha firmato una dichiarazione con cui si assume tutti gli impegni di cui al paragrafo 2;

(c) l'ITSEF ha concluso la valutazione senza obiezioni in conformità delle norme, dei criteri e dei metodi di valutazione di cui agli articoli 3 e 7;

(d) l'organismo di certificazione ha concluso il riesame dei risultati della valutazione senza obiezioni;

(e) l'organismo di certificazione ha verificato che le relazioni tecniche di valutazione fornite dall'ITSEF siano coerenti con gli elementi di prova forniti e che le norme, i criteri e i metodi di valutazione di cui agli articoli 3 e 7 siano stati applicati correttamente.

2. Il richiedente la certificazione si assume gli impegni seguenti:

(a) presentazione all'organismo di certificazione e all'ITSEF di tutte le informazioni necessarie, complete e corrette, e di ulteriori informazioni necessarie, se richiesto;

(b) astensione dalla promozione del prodotto TIC come certificato nel quadro dell'EUCC prima che il certificato EUCC sia stato rilasciato;

(c) promozione del prodotto TIC come certificato solo in relazione all'ambito di applicazione stabilito nel certificato EUCC;

(d) cessazione immediata della promozione del prodotto TIC come certificato in caso di sospensione, revoca o scadenza del certificato EUCC;

(e) garanzia che i prodotti TIC venduti facendo riferimento al certificato EUCC siano esattamente identici al prodotto TIC oggetto della certificazione;

(f) rispetto delle norme di utilizzo del marchio e dell'etichetta stabilite per il certificato EUCC in conformità dell'articolo 11.

3. Nel caso di un prodotto TIC sottoposto a una certificazione di prodotto composito conformemente ai pertinenti documenti sullo stato dell'arte, l'organismo di certificazione che ha effettuato la certificazione del prodotto TIC sottostante condivide le informazioni pertinenti con l'organismo di certificazione che effettua la certificazione del prodotto TIC composito.

Articolo 10

Contenuto e formato del certificato EUCC

1. Il certificato EUCC contiene almeno le informazioni di cui all'allegato VII.

2. Nel certificato EUCC o nella relazione di certificazione sono specificati in modo inequivocabile l'ambito e i limiti del prodotto TIC certificato, ed è indicato se la certificazione riguarda l'intero prodotto TIC o solo alcune sue parti.

3. L'organismo di certificazione fornisce al richiedente il certificato EUCC almeno in formato elettronico.

4. L'organismo di certificazione elabora una relazione di certificazione in conformità dell'allegato V per ciascun certificato EUCC rilasciato. La relazione di certificazione si basa sulla relazione tecnica di valutazione redatta dall'ITSEF. La relazione tecnica di valutazione e la relazione di certificazione indicano i criteri e i metodi di valutazione specifici di cui all'articolo 7 utilizzati per la valutazione.

5. L'organismo di certificazione fornisce all'autorità nazionale di certificazione della cibersicurezza e all'ENISA tutti i certificati EUCC e tutte le relazioni di certificazione in formato elettronico.

Articolo 11

Marchio ed etichetta

1. Il titolare di un certificato può apporre un marchio e un'etichetta su un prodotto TIC certificato. Il marchio e l'etichetta dimostrano che il prodotto TIC è stato certificato in conformità del presente regolamento. Essi sono apposti in conformità del presente articolo e dell'allegato IX.

2. Il marchio e l'etichetta sono apposti in modo visibile, leggibile e indelebile sul prodotto TIC certificato o sulla sua targhetta identificativa. Qualora ciò sia impossibile o difficilmente realizzabile a causa della natura del prodotto, essi sono apposti sull'imballaggio o sui documenti di accompagnamento. Se il prodotto TIC certificato è fornito sotto forma di software, il marchio e l'etichetta figurano in modo visibile, leggibile e indelebile sui documenti di accompagnamento, o tali documenti sono resi facilmente e direttamente accessibili agli utenti attraverso un sito web.

3. Il marchio e l'etichetta sono conformi al quanto disposto nell'allegato IX e contengono:

(a) il livello di affidabilità e il livello AVA_VAN del prodotto TIC certificato;

(b) l'identificatore unico del certificato, costituito dagli elementi seguenti:

  (1) denominazione del sistema;

  (2) denominazione e numero di riferimento dell'accreditamento dell'organismo di certificazione che ha rilasciato il certificato;

  (3) anno e mese di rilascio;

  (4) numero di identificazione assegnato dall'organismo di certificazione che ha rilasciato il certificato.

4. Il marchio e l'etichetta sono accompagnati da un codice QR con un link a un sito web contenente almeno:

(a) le informazioni sulla validità del certificato;

(b) le informazioni necessarie sulla certificazione, di cui agli allegati V e VII;

(c) le informazioni che il titolare del certificato deve rendere pubblicamente disponibili conformemente all'articolo 55 del regolamento (UE) 2019/881; nonché

(d) se del caso, le informazioni storiche relative alla certificazione o alle certificazioni specifiche del prodotto TIC per consentire la tracciabilità.

Articolo 12

Periodo di validità del certificato EUCC

1. L'organismo di certificazione stabilisce un periodo di validità per ciascun certificato EUCC rilasciato tenendo conto delle caratteristiche del prodotto TIC certificato.

2. Il periodo di validità del certificato EUCC non supera i cinque anni.

3. In deroga al paragrafo 2 tale periodo può superare i cinque anni, previa approvazione da parte dell'autorità nazionale di certificazione della cibersicurezza. L'autorità nazionale di certificazione della cibersicurezza notifica al gruppo europeo per la certificazione della cibersicurezza l'approvazione concessa senza indebito ritardo.

Articolo 13

Riesame del certificato EUCC

1. Su richiesta del titolare del certificato o per altri motivi giustificati, l'organismo di certificazione può decidere di riesaminare il certificato EUCC per un prodotto TIC. Il riesame è effettuato conformemente all'allegato IV. L'organismo di certificazione determina la portata del riesame. Se necessario per il riesame, l'organismo di certificazione chiede all'ITSEF di effettuare una nuova valutazione del prodotto TIC certificato.

2. A seguito dei risultati del riesame e, se del caso, della nuova valutazione, l'organismo di certificazione:

(a) conferma il certificato EUCC;

(b) revoca il certificato EUCC in conformità dell'articolo 14;

(c) revoca il certificato EUCC in conformità dell'articolo 14 e rilascia un nuovo certificato EUCC con un ambito di applicazione identico e un periodo di validità prorogato; oppure

(d) revoca il certificato EUCC in conformità dell'articolo 14 e rilascia un nuovo certificato EUCC con un ambito di applicazione diverso.

3. L'organismo di certificazione può decidere di sospendere, senza indebito ritardo, il certificato EUCC in conformità dell'articolo 30, in attesa di una misura correttiva da parte del titolare del certificato EUCC.

Articolo 14

Revoca del certificato EUCC

1. Fatto salvo l'articolo 58, paragrafo 8, lettera e), del regolamento (UE) 2019/881, un certificato EUCC è revocato dall'organismo di certificazione che lo ha rilasciato.

2. L'organismo di certificazione di cui al paragrafo 1 notifica la revoca del certificato all'autorità nazionale di certificazione della cibersicurezza. Tale notifica è trasmessa anche all'ENISA al fine di facilitare l'esecuzione dei suoi compiti a norma dell'articolo 50 del regolamento (UE) 2019/881. L'autorità nazionale di certificazione della cibersicurezza informa le altre autorità di vigilanza del mercato competenti.

3. Il titolare di un certificato EUCC può richiedere la revoca del certificato.

CAPO III

CERTIFICAZIONE DEI PROFILI DI PROTEZIONE

SEZIONE I

Norme e requisiti specifici per la valutazione

Articolo 15

Criteri e metodi di valutazione

1. Un profilo di protezione è valutato quanto meno conformemente a quanto segue:

(a) gli elementi applicabili delle norme di cui all'articolo 3;

(b) il livello di rischio associato all'uso previsto dei prodotti TIC in questione a norma dell'articolo 52 del regolamento (UE) 2019/881 e le loro funzioni di sicurezza a sostegno degli obiettivi di sicurezza di cui all'articolo 51 del medesimo regolamento; e

(c) i pertinenti documenti sullo stato dell'arte di cui all'allegato I. Un profilo di protezione contemplato da un settore tecnico è certificato rispetto ai requisiti stabiliti in tale settore tecnico.

2. In casi eccezionali e debitamente giustificati, un organismo di valutazione della conformità può certificare un profilo di protezione senza applicare i pertinenti documenti sullo stato dell'arte. In tali casi informa l'autorità nazionale di certificazione della cibersicurezza competente e fornisce una giustificazione per la prevista certificazione senza l'applicazione dei pertinenti documenti sullo stato dell'arte, nonché una proposta di metodologia di valutazione. L'autorità nazionale di certificazione della cibersicurezza valuta la giustificazione e, qualora la ritenga valida, approva la mancata applicazione dei pertinenti documenti sullo stato dell'arte e approva o modifica, se del caso, la metodologia di valutazione che dovrà essere applicata dall'organismo di valutazione della conformità. In attesa della decisione dell'autorità nazionale di certificazione della cibersicurezza, l'organismo di valutazione della conformità non rilascia alcun certificato per il profilo di protezione. L'autorità nazionale di certificazione della cibersicurezza notifica senza indebito ritardo l'autorizzazione della mancata applicazione dei pertinenti documenti sullo stato dell'arte al gruppo europeo per la certificazione della cibersicurezza, che può formulare un parere. L'autorità nazionale di certificazione della cibersicurezza tiene nella massima considerazione il parere del gruppo europeo per la certificazione della cibersicurezza.

SEZIONE II

Rilascio, rinnovo e revoca dei certificati EUCC per i profili di protezione

Articolo 16

Informazioni necessarie per la certificazione dei profili di protezione

Il richiedente la certificazione di un profilo di protezione fornisce o mette altrimenti a disposizione dell'organismo di certificazione e dell'ITSEF tutte le informazioni necessarie per le attività di certificazione. Si applicano, mutatis mutandis, le disposizioni dell'articolo 8, paragrafi 2, 3, 4 e 7.

Articolo 17

Rilascio di certificati EUCC per i profili di protezione

1. Il richiedente la certificazione fornisce all'organismo di certificazione e all'ITSEF tutte le informazioni necessarie, complete e corrette.

2. Gli articoli 9 e 10 si applicano mutatis mutandis.

3. L'ITSEF valuta se un profilo di protezione è completo, coerente, tecnicamente valido ed efficace per l'uso previsto e gli obiettivi di sicurezza della categoria di prodotti TIC da esso contemplati.

4. Un profilo di protezione è certificato unicamente:

(a) da un'autorità nazionale di certificazione della cibersicurezza o da un altro organismo pubblico accreditato come organismo di certificazione; oppure

(b) da un organismo di certificazione, previa approvazione dell'autorità nazionale di certificazione della cibersicurezza per ogni singolo profilo di protezione.

Articolo 18

Periodo di validità del certificato EUCC per i profili di protezione

1. L'organismo di certificazione stabilisce un periodo di validità per ciascun certificato EUCC.

2. Il periodo di validità può durare fino al termine del ciclo di vita del profilo di protezione in questione.

Articolo 19

Riesame del certificato EUCC per i profili di protezione

1. Su richiesta del titolare del certificato o per altri motivi giustificati, l'organismo di certificazione può decidere di riesaminare un certificato EUCC per un profilo di protezione. Il riesame è effettuato applicando le condizioni di cui all'articolo 15. L'organismo di certificazione determina la portata del riesame. Se necessario per il riesame, l'organismo di certificazione chiede all'ITSEF di effettuare una nuova valutazione del profilo di protezione certificato.

2. A seguito dei risultati del riesame e, se del caso, della nuova valutazione, l'organismo di certificazione procede in uno dei modi seguenti:

(a) conferma il certificato EUCC;

(b) revoca il certificato EUCC in conformità dell'articolo 20;

(c) revoca il certificato EUCC in conformità dell'articolo 20 e rilascia un nuovo certificato EUCC con un ambito di applicazione identico e un periodo di validità prorogato;

(d) revoca il certificato EUCC in conformità dell'articolo 20 e rilascia un nuovo certificato EUCC con un ambito di applicazione diverso.

Articolo 20

Revoca del certificato EUCC per un profilo di protezione

1. Fatto salvo l'articolo 58, paragrafo 8, lettera e), del regolamento (UE) 2019/881, un certificato EUCC per un profilo di protezione è revocato dall'organismo di certificazione che lo ha rilasciato. L'articolo 14 si applica mutatis mutandis.

2. Un certificato per un profilo di protezione rilasciato conformemente all'articolo 17, paragrafo 4, lettera b), è revocato dall'autorità nazionale di certificazione della cibersicurezza che lo ha approvato.

CAPO IV

ORGANISMI DI VALUTAZIONE DELLA CONFORMITÀ

Articolo 21

Requisiti specifici o supplementari per un organismo di certificazione

1. Un organismo di certificazione è autorizzato dall'autorità nazionale di certificazione della cibersicurezza a rilasciare certificati EUCC di livello di affidabilità «elevato» se, oltre a soddisfare i requisiti di cui all'articolo 60, paragrafo 1, e all'allegato del regolamento (UE) 2019/881 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità, dimostra:

(a) di possedere le conoscenze e le competenze necessarie per la decisione relativa alla certificazione del livello di affidabilità «elevato»;

(b) di svolgere le proprie attività di certificazione in collaborazione con un'ITSEF autorizzata in conformità dell'articolo 22; e

(c) di possedere le competenze richieste e di aver adottato misure tecniche e operative adeguate per proteggere efficacemente le informazioni riservate e sensibili per il livello di affidabilità «elevato», oltre a soddisfare i requisiti di cui all'articolo 43.

2. L'autorità nazionale di certificazione della cibersicurezza valuta se un organismo di certificazione soddisfa tutti i requisiti di cui al paragrafo 1. Tale valutazione comprende almeno interviste strutturate e un riesame di almeno una certificazione pilota effettuata dall'organismo di certificazione in conformità del presente regolamento.

Nella sua valutazione, l'autorità nazionale di certificazione della cibersicurezza può riutilizzare elementi di prova adeguati provenienti da una precedente autorizzazione o da attività analoghe concesse a norma:

(a) del presente regolamento;

(b) di un altro sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881;

(c) di un sistema nazionale di cui all'articolo 49 del presente regolamento.

3. L'autorità nazionale di certificazione della cibersicurezza elabora una relazione di autorizzazione soggetta a valutazione inter pares in conformità dell'articolo 59, paragrafo 3, lettera d), del regolamento (UE) 2019/881.

4. L'autorità nazionale di certificazione della cibersicurezza specifica le categorie di prodotti TIC e i profili di protezione a cui si estende l'autorizzazione. L'autorizzazione è valida per un periodo non superiore alla validità dell'accreditamento. Tale autorizzazione può essere rinnovata su richiesta, a condizione che l'organismo di certificazione continui a soddisfare i requisiti di cui al presente articolo. Per il rinnovo dell'autorizzazione non sono richieste valutazioni pilota.

5. L'autorità nazionale di certificazione della cibersicurezza revoca l'autorizzazione dell'organismo di certificazione se quest'ultimo non soddisfa più le condizioni di cui al presente articolo. In caso di revoca dell'autorizzazione, l'organismo di certificazione cessa immediatamente di presentarsi come organismo di certificazione autorizzato.

Articolo 22

Requisiti specifici o supplementari per un ITSEF

1. Un'ITSEF è autorizzata dall'autorità nazionale di certificazione della cibersicurezza a effettuare la valutazione dei prodotti TIC soggetti a certificazione con il livello di affidabilità «elevato» se, oltre a soddisfare i requisiti di cui all'articolo 60, paragrafo 1, e all'allegato del regolamento (UE) 2019/881 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità, dimostra di rispettare tutte le condizioni seguenti:

(a) possesso delle competenze necessarie per svolgere le attività di valutazione al fine di determinare la resistenza agli attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative;

(b) per quanto riguarda i settori tecnici e i profili di protezione, che fanno parte del processo TIC per tali prodotti TIC:

(1) possesso delle competenze per svolgere le attività di valutazione specifiche necessarie a determinare metodicamente la resistenza di un oggetto della valutazione agli attacchi commessi da soggetti qualificati nel suo ambiente operativo, ipotizzando un potenziale di attacco «moderato» o «elevato», come stabilito nelle norme di cui all'articolo 3;

(2) possesso delle competenze tecniche specificate nei documenti sullo stato dell'arte di cui all'allegato I;

(c) possesso delle competenze richieste e adozione di misure tecniche e operative adeguate per proteggere efficacemente le informazioni riservate e sensibili per il livello di affidabilità «elevato», oltre al soddisfacimento dei requisiti di cui all'articolo 43.

2. L'autorità nazionale di certificazione della cibersicurezza valuta se un'ITSEF soddisfa tutti i requisiti di cui al paragrafo 1. Tale valutazione comprende quanto meno interviste strutturate e un riesame di almeno una valutazione pilota effettuata dall'ITSEF in conformità del presente regolamento.

3. Nella sua valutazione, l'autorità nazionale di certificazione della cibersicurezza può riutilizzare elementi di prova adeguati provenienti da una precedente autorizzazione o da attività analoghe concesse a norma:

(a) del presente regolamento;

(b) di un altro sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881;

(c) di un sistema nazionale di cui all'articolo 49 del presente regolamento.

4. L'autorità nazionale di certificazione della cibersicurezza elabora una relazione di autorizzazione soggetta a valutazione inter pares in conformità dell'articolo 59, paragrafo 3, lettera d), del regolamento (UE) 2019/881.

5. L'autorità nazionale di certificazione della cibersicurezza specifica le categorie di prodotti TIC e i profili di protezione a cui si estende l'autorizzazione. L'autorizzazione è valida per un periodo non superiore alla validità dell'accreditamento. Tale autorizzazione può essere rinnovata su richiesta, a condizione che l'ITSEF continui a soddisfare i requisiti di cui al presente articolo. Per il rinnovo dell'autorizzazione non devono essere richieste valutazioni pilota.

6. L'autorità nazionale di certificazione della cibersicurezza revoca l'autorizzazione dell'ITSEF se quest'ultima non soddisfa più le condizioni di cui al presente articolo. In caso di revoca dell'autorizzazione, l'ITSEF cessa di presentarsi come un'ITSEF autorizzata.

Articolo 23

Notifica degli organismi di certificazione

1. L'autorità nazionale di certificazione della cibersicurezza notifica alla Commissione gli organismi di certificazione presenti sul suo territorio che sono competenti a certificare al livello di affidabilità «sostanziale» in base al loro accreditamento.

2. L'autorità nazionale di certificazione della cibersicurezza notifica alla Commissione gli organismi di certificazione presenti sul suo territorio che sono competenti a certificare al livello di affidabilità «elevato» in base al loro accreditamento e alla decisione di autorizzazione.

3. All'atto della notifica alla Commissione degli organismi di certificazione, l'autorità nazionale di certificazione della cibersicurezza fornisce almeno le informazioni seguenti:

(a) il livello o i livelli di affidabilità per i quali l'organismo di certificazione è competente a rilasciare certificati EUCC;

(b) le informazioni relative all'accreditamento indicate di seguito:

(1) la data dell'accreditamento;

(2) il nome e l'indirizzo dell'organismo di certificazione;

(3) il paese di registrazione dell'organismo di certificazione,

(4) il numero di riferimento dell'accreditamento;

(5) l'ambito di applicazione e la durata di validità dell'accreditamento;

(6) l'indirizzo, la sede e il link al pertinente sito web dell'organismo nazionale di accreditamento; e

(c) le informazioni relative all'autorizzazione per il livello «elevato» indicate di seguito:

(1) la data dell'autorizzazione:

(2) il numero di riferimento dell'autorizzazione;

(3) la durata di validità dell'autorizzazione;

(4) l'ambito di applicazione dell'autorizzazione, compreso il livello AVA_VAN più elevato e, se del caso, il settore tecnico contemplato.

4. L'autorità nazionale di certificazione della cibersicurezza invia una copia della notifica di cui ai paragrafi 1 e 2 all'ENISA per la pubblicazione di informazioni accurate in merito all'ammissibilità degli organismi di certificazione sul sito web relativo alla certificazione della cibersicurezza.

5. L'autorità nazionale di certificazione della cibersicurezza esamina senza indebito ritardo qualsiasi informazione relativa a una modifica dello stato dell'accreditamento fornita dall'organismo nazionale di accreditamento. Se l'accreditamento o l'autorizzazione sono stati revocati, l'autorità nazionale di certificazione della cibersicurezza ne informa la Commissione e può presentare a quest'ultima una richiesta conformemente all'articolo 61, paragrafo 4, del regolamento (UE) 2019/881.

Articolo 24

Notifica dell'ITSEF

Gli obblighi di notifica delle autorità nazionali di certificazione della cibersicurezza di cui all'articolo 23 si applicano anche alle ITSEF. La notifica include l'indirizzo dell'ITSEF, l'accreditamento valido e, se del caso, l'autorizzazione valida di tale ITSEF.

CAPO V

MONITORAGGIO, NON CONFORMITÀ E NON COMPLIANCE

SEZIONE I

Monitoraggio della compliance

Articolo 25

Attività di monitoraggio da parte dell'autorità nazionale di certificazione della cibersicurezza

1. Fatto salvo l'articolo 58, paragrafo 7, del regolamento (UE) 2019/881, l'autorità nazionale di certificazione della cibersicurezza controlla:

(a) il rispetto, da parte dell'organismo di certificazione e dell'ITSEF, degli obblighi a essi incombenti a norma del presente regolamento e del regolamento (UE) 2019/881;

(b) il rispetto, da parte dei titolari di un certificato EUCC, degli obblighi a essi incombenti a norma del presente regolamento e del regolamento (UE) 2019/881;

(c) il rispetto, da parte dei prodotti TIC certificati, dei requisiti stabiliti nell'EUCC;

(d) il livello di affidabilità espresso nel certificato EUCC in relazione all'evoluzione del panorama delle minacce.

2. L'autorità nazionale di certificazione della cibersicurezza svolge le sue attività di monitoraggio in particolare sulla base:

(a) delle informazioni provenienti dagli organismi di certificazione, dagli organismi nazionali di accreditamento e dalle autorità di vigilanza del mercato competenti;

(b) delle informazioni derivanti da audit e indagini propri o di altre autorità;

(c) del campionamento effettuato in conformità del paragrafo 3;

(d) dei reclami ricevuti.

3. L'autorità nazionale di certificazione della cibersicurezza, in collaborazione con altre autorità di vigilanza del mercato, campiona annualmente almeno il 4 % dei certificati EUCC, in base a una valutazione dei rischi. Su richiesta e per conto dell'autorità nazionale di certificazione della cibersicurezza competente, gli organismi di certificazione e, se necessario, l'ITSEF assistono tale autorità nel monitoraggio della compliance.

4. L'autorità nazionale di certificazione della cibersicurezza seleziona il campione di prodotti TIC certificati da controllare utilizzando criteri oggettivi tra cui:

(a) la categoria di prodotti;

(b) i livelli di affidabilità dei prodotti;

(c) il titolare di un certificato;

(d) l'organismo di certificazione e, se del caso, l'ITSEF a cui sono state subappaltate le attività;

(e) qualsiasi altra informazione portata all'attenzione dell'autorità.

5. L'autorità nazionale di certificazione della cibersicurezza informa i titolari del certificato EUCC in merito ai prodotti TIC selezionati e ai criteri di selezione.

6. Su richiesta dell'autorità nazionale di certificazione della cibersicurezza, e con l'assistenza della rispettiva ITSEF, l'organismo di certificazione che ha certificato il prodotto TIC oggetto di campionamento procede a un riesame supplementare in conformità della procedura di cui all'allegato IV, sezione IV.2, e informa l'autorità nazionale di certificazione della cibersicurezza in merito ai risultati.

7. Qualora abbia motivi sufficienti per ritenere che un prodotto TIC certificato non sia più conforme al presente regolamento o al regolamento (UE) 2019/881, l'autorità nazionale di certificazione della cibersicurezza può svolgere indagini o avvalersi di qualsiasi altro potere di monitoraggio di cui all'articolo 58, paragrafo 8, del regolamento (UE) 2019/881.

8. L'autorità nazionale di certificazione della cibersicurezza informa l'organismo di certificazione e l'ITSEF in questione delle indagini in corso relative ai prodotti TIC selezionati.

9. Se rileva che un'indagine in corso riguarda prodotti TIC certificati da organismi di certificazione stabiliti in altri Stati membri, l'autorità nazionale di certificazione della cibersicurezza ne informa le autorità nazionali di certificazione della cibersicurezza degli Stati membri interessati ai fini della collaborazione alle indagini, se del caso. Tale autorità nazionale di certificazione della cibersicurezza informa inoltre il gruppo europeo per la certificazione della cibersicurezza in merito alle indagini transfrontaliere e ai relativi risultati.

Articolo 26

Attività di monitoraggio da parte dell'organismo di certificazione

1. L'organismo di certificazione monitora:

(a) il rispetto, da parte dei titolari di un certificato, degli obblighi a essi incombenti a norma del presente regolamento e del regolamento (UE) 2019/881 per quanto riguarda il certificato EUCC rilasciato dall'organismo di certificazione;

(b) il rispetto, da parte dei prodotti TIC che ha certificato, dei rispettivi requisiti di sicurezza;

(c) il livello di affidabilità espresso nei profili di protezione certificati.

2. L'organismo di certificazione svolge le proprie attività di monitoraggio sulla base:

(a) delle informazioni fornite in base agli impegni del richiedente la certificazione di cui all'articolo 9, paragrafo 2;

(b) delle informazioni derivanti dalle attività di altre autorità di vigilanza del mercato competenti;

(c) dei reclami ricevuti;

(d) delle informazioni sulle vulnerabilità che potrebbero avere un impatto sui prodotti TIC che ha certificato.

3. L'autorità nazionale di certificazione della cibersicurezza può elaborare norme volte a promuovere un dialogo periodico tra gli organismi di certificazione e i titolari di certificati EUCC al fine di verificare il rispetto degli impegni assunti a norma dell'articolo 9, paragrafo 2, e riferire in merito, fatte salve le attività connesse ad altre autorità di vigilanza del mercato competenti.

Articolo 27

Attività di monitoraggio da parte del titolare del certificato

1. Al fine di monitorare la conformità del prodotto TIC certificato ai suoi requisiti di sicurezza, il titolare di un certificato EUCC svolge i compiti seguenti:

(a) monitoraggio delle informazioni sulle vulnerabilità relative al prodotto TIC certificato, comprese le dipendenze note, con mezzi propri ma anche in considerazione di:

  (1) una pubblicazione o una presentazione di informazioni sulle vulnerabilità da parte di un utente o di un ricercatore nel settore della sicurezza di cui all'articolo 55, paragrafo 1, lettera c), del regolamento (UE) 2019/881;

  (2) informazioni presentate da qualsiasi altra fonte;

(b) monitoraggio del livello di affidabilità espresso nel certificato EUCC.

2. Il titolare di un certificato EUCC collabora con l'organismo di certificazione, l'ITSEF e, se del caso, l'autorità nazionale di certificazione della cibersicurezza per sostenere le loro attività di monitoraggio.

SEZIONE II

Conformità e compliance

Articolo 28

Conseguenze della non conformità di un prodotto TIC certificato o di un profilo di protezione

1. Se un prodotto TIC certificato o un profilo di protezione certificato non è conforme ai requisiti stabiliti nel presente regolamento e nel regolamento (UE) 2019/881, l'organismo di certificazione informa il titolare del certificato EUCC della non conformità individuata e richiede misure correttive.

2. Qualora un caso di non conformità alle disposizioni del presente regolamento possa influire sul rispetto di altre normative pertinenti dell'Unione, che prevedono la possibilità di dimostrare la presunzione di conformità ai requisiti imposti da tali atti giuridici utilizzando il certificato EUCC, l'organismo di certificazione ne informa senza indugio l'autorità nazionale di certificazione della cibersicurezza. L'autorità nazionale di certificazione della cibersicurezza notifica immediatamente il caso di non conformità individuato all'autorità di vigilanza del mercato responsabile di tali altre normative pertinenti dell'Unione.

3. Al ricevimento delle informazioni di cui al paragrafo 1 il titolare del certificato EUCC propone all'organismo di certificazione, entro il termine stabilito da quest'ultimo, che non può superare i 30 giorni, la misura correttiva necessaria per sanare la non conformità.

4. L'organismo di certificazione può sospendere senza indebito ritardo il certificato EUCC in conformità dell'articolo 30 in caso di emergenza o se il titolare del certificato EUCC non collabora debitamente con l'organismo di certificazione.

5. L'organismo di certificazione effettua un riesame in conformità degli articoli 13 e 19, valutando se la misura correttiva sani la non conformità.

6. Se il titolare del certificato EUCC non propone una misura correttiva adeguata durante il periodo di cui al paragrafo 3, il certificato è sospeso in conformità dell'articolo 30 o revocato in conformità dell'articolo 14 o 20.

7. Il presente articolo non si applica ai casi di vulnerabilità che interessano un prodotto TIC certificato, che saranno trattati in conformità del capo VI.

Articolo 29

Conseguenze della non compliance da parte del titolare del certificato

1. Se constata che:

(a) il titolare del certificato EUCC o il richiedente la certificazione non rispettano gli impegni e gli obblighi di cui all'articolo 9, paragrafo 2, all'articolo 17, paragrafo 2, e agli articoli 27 e 41; oppure

(b) il titolare del certificato EUCC non rispetta quanto stabilito dall'articolo 56, paragrafo 8, del regolamento (UE) 2019/881 o dal capo VI del presente regolamento,

l'organismo di certificazione fissa un termine non superiore a 30 giorni entro il quale il titolare del certificato EUCC adotta misure correttive.

2. Se il titolare del certificato EUCC non propone misure correttive adeguate durante il periodo di cui al paragrafo 1, il certificato è sospeso in conformità dell'articolo 30 o revocato in conformità degli articoli 14 e 20.

3. La violazione continuata o ricorrente da parte del titolare del certificato EUCC degli obblighi di cui al paragrafo 1 fa scattare la revoca del certificato EUCC in conformità dell'articolo 14 o dell'articolo 20.

4. L'organismo di certificazione informa l'autorità nazionale di certificazione della cibersicurezza in merito alle constatazioni di cui al paragrafo 1. Se il caso di non compliance incide sul rispetto di altre normative pertinenti dell'Unione, l'autorità nazionale di certificazione della cibersicurezza notifica immediatamente all'autorità di vigilanza del mercato responsabile di tali altre normative il caso di non compliance individuato.

Articolo 30

Sospensione del certificato EUCC

1. Laddove il presente regolamento faccia riferimento alla sospensione di un certificato EUCC, l'organismo di certificazione sospende il certificato EUCC in questione per un periodo adeguato alle circostanze che hanno determinato la sospensione, che non supera i 42 giorni. Il periodo di sospensione decorre dal giorno successivo a quello in cui l'organismo di certificazione ha adottato la decisione. La sospensione non pregiudica la validità del certificato.

2. L'organismo di certificazione notifica la sospensione al titolare del certificato e all'autorità nazionale di certificazione della cibersicurezza senza indebito ritardo e indica i motivi della sospensione, le misure da intraprendere e il periodo di sospensione.

3. I titolari della certificazione informano gli acquirenti dei prodotti TIC in questione in merito alla sospensione e alla relativa motivazione fornita dall'organismo di certificazione, ad eccezione di quelle parti la cui condivisione costituirebbe un rischio per la sicurezza o che contengono informazioni sensibili. Tali informazioni sono rese pubbliche anche dal titolare del certificato.

4. Qualora altre normative pertinenti dell'Unione prevedano una presunzione di conformità basata su certificati rilasciati a norma delle disposizioni del presente regolamento, l'autorità nazionale di certificazione della cibersicurezza informa l'autorità di vigilanza del mercato responsabile di tali normative in merito alla sospensione.

5. La sospensione di un certificato è notificata all'ENISA in conformità dell'articolo 42, paragrafo 3.

6. In casi debitamente giustificati l'autorità nazionale di certificazione della cibersicurezza può autorizzare una proroga del periodo di sospensione di un certificato EUCC. Il periodo complessivo di sospensione non può superare un anno.

Articolo 31

Conseguenze della non compliance da parte dell'organismo di valutazione della conformità

1. In caso di mancato rispetto dei propri obblighi da parte di un organismo di certificazione o da parte dell'organismo di certificazione competente, qualora sia individuata una non compliance da parte di un'ITSEF, l'autorità nazionale di certificazione della cibersicurezza, senza indebito ritardo:

(a) identifica con il sostegno dell'ITSEF in questione i certificati EUCC potenzialmente interessati;

(b) richiede, se necessario, l'esecuzione di attività di valutazione su uno o più prodotti TIC o profili di protezione da parte dell'ITSEF che ha effettuato la valutazione o di qualsiasi altra ITSEF accreditata e, se del caso, autorizzata che possa trovarsi in una posizione tecnica migliore per sostenere tale identificazione;

(c) analizza gli impatti della non compliance;

(d) informa il titolare del certificato EUCC interessato dalla non compliance.

2. Sulla base delle misure di cui al paragrafo 1, l'organismo di certificazione adotta, in relazione a ciascun certificato EUCC interessato, una delle decisioni indicate di seguito:

(a) mantenere il certificato EUCC inalterato;

(b) revocare il certificato EUCC in conformità dell'articolo 14 o dell'articolo 20 e, se del caso, rilasciare un nuovo certificato EUCC.

3. Sulla base delle misure di cui al paragrafo 1 l'autorità nazionale di certificazione della cibersicurezza:

(a) segnala, se necessario, la non compliance dell'organismo di certificazione o della relativa ITSEF all'organismo nazionale di accreditamento;

(b) valuta, se del caso, il potenziale impatto sull'autorizzazione.

CAPO VI

GESTIONE E DIVULGAZIONE DELLE VULNERABILITÀ

Articolo 32

Ambito della gestione delle vulnerabilità

Il presente capo si applica ai prodotti TIC per i quali è stato rilasciato un certificato EUCC.

SEZIONE I

Gestione delle vulnerabilità

Articolo 33

Procedure di gestione delle vulnerabilità

1. Il titolare di un certificato EUCC istituisce e mantiene in essere tutte le procedure di gestione delle vulnerabilità necessarie in conformità delle norme di cui alla presente sezione e, se necessario, le integra con le procedure stabilite nella norma EN ISO/IEC 30111.

2. Il titolare di un certificato EUCC mantiene in essere e pubblica metodi appropriati per ricevere informazioni sulle vulnerabilità relative ai propri prodotti trasmesse da fonti esterne, compresi gli utenti, gli organismi di certificazione e i ricercatori nel settore della sicurezza.

3. Qualora rilevi una potenziale vulnerabilità che interessa un suo prodotto TIC certificato o riceva informazioni in merito, il titolare di un certificato EUCC registra tali informazioni ed effettua un'analisi dell'impatto delle vulnerabilità.

4. Se una potenziale vulnerabilità interessa un prodotto composito, il titolare del certificato EUCC ne informa il titolare dei certificati EUCC da esso dipendenti.

5. In risposta a una richiesta ragionevole dell'organismo di certificazione che ha rilasciato il certificato, il titolare di un certificato EUCC trasmette a tale organismo tutte le informazioni pertinenti sulle potenziali vulnerabilità.

Articolo 34

Analisi dell'impatto delle vulnerabilità

1. L'analisi dell'impatto delle vulnerabilità si riferisce all'oggetto della valutazione e alle dichiarazioni di affidabilità contenute nel certificato. L'analisi dell'impatto delle vulnerabilità è effettuata in un intervallo di tempo adeguato in relazione alla sfruttabilità e alla criticità della potenziale vulnerabilità del prodotto TIC certificato.

2. Se del caso, è effettuato un calcolo del potenziale di attacco in conformità della metodologia pertinente inclusa nelle norme di cui all'articolo 3 e dei documenti sullo stato dell'arte pertinenti di cui all'allegato I, al fine di determinare la sfruttabilità della vulnerabilità. Si tiene conto del livello AVA_VAN del certificato EUCC.

Articolo 35

Relazione sull'analisi dell'impatto delle vulnerabilità

1. Se dall'analisi dell'impatto emerge un probabile impatto della vulnerabilità sulla conformità del prodotto TIC al relativo certificato, il titolare elabora una relazione sull'analisi dell'impatto delle vulnerabilità.

2. La relazione sull'analisi dell'impatto delle vulnerabilità contiene una valutazione degli elementi seguenti:

(a) l'impatto della vulnerabilità sul prodotto TIC certificato;

(b) i possibili rischi associati alla prossimità o alla disponibilità di un attacco;

(c) la possibilità di risolvere la vulnerabilità;

(d) laddove la vulnerabilità possa essere risolta, le possibili modalità di risoluzione.

3. La relazione sull'analisi dell'impatto delle vulnerabilità contiene, se del caso, dettagli sulle possibili modalità di sfruttamento della vulnerabilità. Le informazioni relative alle possibili modalità di sfruttamento della vulnerabilità sono trattate conformemente a misure di sicurezza adeguate per proteggerne la riservatezza e garantirne, se necessario, una diffusione limitata.

4. In conformità dell'articolo 56, paragrafo 8, del regolamento (UE) 2019/881, il titolare di un certificato EUCC trasmette senza indebito ritardo una relazione sull'analisi dell'impatto delle vulnerabilità all'organismo di certificazione o all'autorità nazionale di certificazione della cibersicurezza.

5. Se dalla relazione sull'analisi dell'impatto delle vulnerabilità emerge che la vulnerabilità non è residua ai sensi delle norme di cui all'articolo 3 e che può essere risolta, si applica l'articolo 36.

6. Se dalla relazione sull'analisi dell'impatto delle vulnerabilità emerge che la vulnerabilità non è residua e che non può essere risolta, il certificato EUCC è revocato in conformità dell'articolo 14.

7. Il titolare del certificato EUCC monitora le eventuali vulnerabilità residue per garantire che non possano essere sfruttate in caso di modifiche dell'ambiente operativo.

Articolo 36

Risoluzione delle vulnerabilità

Il titolare di un certificato EUCC trasmette all'organismo di certificazione una proposta contenente una misura correttiva adeguata. L'organismo di certificazione riesamina il certificato in conformità dell'articolo 13. L'ambito di applicazione del riesame è determinato in base alla proposta di risoluzione della vulnerabilità.

SEZIONE II

Divulgazione delle vulnerabilità

Articolo 37

Informazioni condivise con l'autorità nazionale di certificazione della cibersicurezza

1. Le informazioni fornite dall'organismo di certificazione all'autorità nazionale di certificazione della cibersicurezza includono tutti gli elementi necessari a quest'ultima per comprendere l'impatto della vulnerabilità, le modifiche da apportare al prodotto TIC e, se disponibili, le eventuali informazioni da parte dell'organismo di certificazione sulle implicazioni più ampie della vulnerabilità per altri prodotti TIC certificati.

2. Le informazioni fornite in conformità del paragrafo 1 non contengono dettagli sulle modalità di sfruttamento della vulnerabilità. La presente disposizione lascia impregiudicati i poteri di indagine dell'autorità nazionale di certificazione della cibersicurezza.

Articolo 38

Cooperazione con altre autorità nazionali di certificazione della cibersicurezza

1. L'autorità nazionale di certificazione della cibersicurezza condivide le informazioni pertinenti ricevute in conformità dell'articolo 37 con le altre autorità nazionali di certificazione della cibersicurezza e con l'ENISA.

2. Altre autorità nazionali di certificazione della cibersicurezza possono decidere di analizzare ulteriormente la vulnerabilità o, dopo aver informato il titolare del certificato EUCC, chiedere agli organismi di certificazione competenti di valutare se la vulnerabilità possa interessare altri prodotti TIC certificati.

Articolo 39

Pubblicazione della vulnerabilità

In caso di revoca di un certificato, il titolare del certificato EUCC divulga e registra qualsiasi vulnerabilità del prodotto TIC pubblicamente nota e risolta nella banca dati europea delle vulnerabilità, istituita in conformità dell'articolo 12 della

direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([5]), o in altri archivi online di cui all'articolo 55, paragrafo 1, lettera d), del regolamento (UE) 2019/881.

CAPO VII

CONSERVAZIONE, DIVULGAZIONE E PROTEZIONE DELLE INFORMAZIONI

Articolo 40

Conservazione dei registri da parte degli organismi di certificazione e dell'ITSEF

1. L'ITSEF e gli organismi di certificazione mantengono un sistema di registri in cui sono contenuti tutti i documenti prodotti in relazione a ciascuna valutazione e certificazione da essi effettuata.

2. Gli organismi di certificazione e l'ITSEF archiviano i registri in modo sicuro e li conservano per il periodo necessario ai fini del presente regolamento e per almeno cinque anni dopo la revoca del relativo certificato EUCC. Qualora abbia rilasciato un nuovo certificato EUCC in conformità dell'articolo 13, paragrafo 2, lettera c), l'organismo di certificazione conserva la documentazione relativa al certificato EUCC revocato insieme a quella relativa al nuovo certificato EUCC, per lo stesso periodo di tempo.

Articolo 41

Informazioni messe a disposizione dal titolare di un certificato

1. Le informazioni di cui all'articolo 55 del regolamento (UE) 2019/881 sono disponibili in un linguaggio facilmente comprensibile dagli utenti.

2. Il titolare di un certificato EUCC archivia in modo sicuro per il periodo necessario ai fini del presente regolamento e per almeno cinque anni dopo la revoca del relativo certificato EUCC:

(a) i registri delle informazioni fornite all'organismo di certificazione e all'ITSEF durante il processo di certificazione;

(b) un esemplare del prodotto TIC certificato.

3. Qualora l'organismo di certificazione abbia rilasciato un nuovo certificato EUCC in conformità dell'articolo 13, paragrafo 2, lettera c), il titolare conserva la documentazione relativa al certificato EUCC revocato insieme a quella relativa al nuovo certificato EUCC, per lo stesso periodo di tempo.

4. Su richiesta dell'organismo di certificazione o dell'autorità nazionale di certificazione della cibersicurezza, il titolare di un certificato EUCC mette a disposizione i registri e le copie di cui al paragrafo 2.

Articolo 42

Informazioni che l'ENISA deve mettere a disposizione

1. L'ENISA pubblica sul sito web di cui all'articolo 50, paragrafo 1, del regolamento (UE) 2019/881, le informazioni seguenti:

(a) tutti i certificati EUCC;

(b) le informazioni sullo stato dei certificati EUCC, in particolare se sono in vigore, sospesi, revocati o scaduti;

(c) le relazioni di certificazione corrispondenti a ciascun certificato EUCC;

([5]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).

(d) un elenco degli organismi di valutazione della conformità accreditati;

(e) un elenco degli organismi di valutazione della conformità autorizzati;

(f) i documenti sullo stato dell'arte di cui all'allegato I;

(g) i pareri del gruppo europeo per la certificazione della cibersicurezza di cui all'articolo 62, paragrafo 4, lettera c), del regolamento (UE) 2019/881;

(h) le relazioni di valutazione inter pares emesse in conformità dell'articolo 47.

2. Le informazioni di cui al paragrafo 1 sono messe a disposizione almeno in inglese.

3. Gli organismi di certificazione e, se del caso, le autorità nazionali di certificazione della cibersicurezza informano senza indugio l'ENISA in merito alle loro decisioni che incidono sul contenuto o sullo stato di un certificato EUCC di cui al paragrafo 1, lettera b).

4. L'ENISA garantisce che le informazioni pubblicate in conformità del paragrafo 1, lettere a), b) e c), identifichino chiaramente le versioni di un prodotto TIC certificato che sono contemplate da un certificato EUCC.

Articolo 43

Protezione delle informazioni

Gli organismi di valutazione della conformità, le autorità nazionali di certificazione della cibersicurezza, l'ECCG, l'ENISA, la Commissione e tutte le altre parti garantiscono la sicurezza e la protezione dei segreti aziendali e di altre informazioni riservate, compresi i segreti commerciali, nonché la salvaguardia dei diritti di proprietà intellettuale, e adottano le misure tecniche e organizzative necessarie e appropriate.

CAPO VIII

ACCORDI SUL RECIPROCO RICONOSCIMENTO CON I PAESI TERZI

Articolo 44

Condizioni

1. I paesi terzi che intendono certificare i propri prodotti in conformità del presente regolamento e che desiderano che tale certificazione sia riconosciuta all'interno dell'Unione concludono un accordo sul reciproco riconoscimento con l'Unione.

2. L'accordo sul reciproco riconoscimento riguarda i livelli di affidabilità applicabili ai prodotti TIC certificati e, se del caso, i profili di protezione.

3. Gli accordi sul reciproco riconoscimento di cui al paragrafo 1 possono essere conclusi solo con i paesi terzi che soddisfano le condizioni seguenti:

(a) dispongono di un'autorità che:

(1) è un ente pubblico, indipendente dagli enti che vigila e monitora in termini di struttura organizzativa e giuridica, finanziamento e processo decisionale;

(2) dispone di adeguati poteri di monitoraggio e vigilanza per svolgere indagini e ha il potere di adottare misure correttive adeguate per garantire la compliance;

(3) dispone di un sistema sanzionatorio efficace, proporzionato e dissuasivo per garantire la compliance;

(4) accetta di collaborare con il gruppo europeo per la certificazione della cibersicurezza e con l'ENISA al fine di scambiare le migliori pratiche e informazioni sugli sviluppi pertinenti nel campo della certificazione della cibersicurezza e di lavorare a un'interpretazione uniforme dei criteri e dei metodi di valutazione attualmente applicabili, tra l'altro applicando una documentazione armonizzata equivalente ai documenti sullo stato dell'arte elencati di cui all'allegato I;

(b) dispongono di un organismo di accreditamento indipendente che effettua accreditamenti utilizzando norme equivalenti a quelle di cui al regolamento (CE) n. 765/2008;

(c) si impegnano affinché i processi e le procedure di valutazione e certificazione siano svolti in modo debitamente professionale, tenendo conto del rispetto delle norme internazionali di cui al presente regolamento, in particolare all'articolo 3;

(d) sono in grado di segnalare le vulnerabilità non rilevate in precedenza e dispongono di una procedura consolidata e adeguata di gestione e divulgazione delle vulnerabilità;

(e) dispongono di procedure consolidate che consentono loro di presentare e trattare efficacemente i reclami e di fornire effettivi mezzi di ricorso giurisdizionale al reclamante;

(f) istituiscono un meccanismo di cooperazione con gli altri organismi dell'Unione e degli Stati membri competenti per la certificazione della cibersicurezza a norma del presente regolamento, compresa la condivisione di informazioni sull'eventuale non compliance dei certificati, il monitoraggio degli sviluppi pertinenti nel campo della certificazione e la garanzia di un approccio comune al mantenimento e al riesame delle certificazioni.

4. Oltre alle condizioni di cui al paragrafo 3, è possibile concludere un accordo sul reciproco riconoscimento di cui al paragrafo 1 relativo al livello di affidabilità «elevato» con i paesi terzi solo se sono soddisfatte anche le condizioni seguenti:

(a) il paese terzo dispone di un'autorità pubblica e indipendente di certificazione della cibersicurezza che svolge o delega le attività di valutazione necessarie per consentire la certificazione al livello di affidabilità «elevato», che sono equivalenti ai requisiti e alle procedure stabiliti per le autorità nazionali di cibersicurezza nel presente regolamento e nel regolamento (UE) 2019/881;

(b) l'accordo sul reciproco riconoscimento stabilisce un meccanismo congiunto equivalente alla valutazione inter pares per la certificazione EUCC al fine di migliorare lo scambio di pratiche e risolvere congiuntamente i problemi nell'ambito della valutazione e della certificazione.

CAPO IX

VALUTAZIONE INTER PARES DEGLI ORGANISMI DI CERTIFICAZIONE

Articolo 45

Procedura di valutazione inter pares

1. Un organismo di certificazione che rilascia certificati EUCC per il livello di affidabilità «elevato» si sottopone a una valutazione inter pares su base periodica e almeno ogni cinque anni. I diversi tipi di valutazione inter pares figurano nell'allegato VI.

2. Il gruppo europeo per la certificazione della cibersicurezza elabora e mantiene un calendario di valutazioni inter pares che garantisce il rispetto di tale periodicità. Salvo casi debitamente giustificati, le valutazioni inter pares sono effettuate in loco.

3. La valutazione inter pares può basarsi su elementi di prova raccolti nel corso di precedenti valutazioni inter pares o procedure equivalenti dell'organismo di certificazione oggetto di valutazione inter pares o dell'autorità nazionale di certificazione della cibersicurezza, a condizione che:

(a) i risultati non risalgano a oltre cinque anni prima;

(b) qualora si riferiscano a una valutazione inter pares effettuata nell'ambito di un sistema di certificazione diverso, i risultati siano accompagnati da una descrizione delle procedure di valutazione inter pares stabilite per tale sistema;

(c) la relazione di valutazione inter pares di cui all'articolo 47 specifichi quali risultati sono stati riutilizzati con o senza ulteriore valutazione.

4. Qualora la valutazione inter pares riguardi un settore tecnico, è valutata anche l'ITSEF interessata.

5. L'organismo di certificazione oggetto di valutazione inter pares e, se necessario, l'autorità nazionale di certificazione della cibersicurezza assicurano che tutte le informazioni pertinenti siano messe a disposizione del gruppo di valutazione inter pares.

6. La valutazione inter pares è effettuata da un gruppo di valutazione inter pares istituito in conformità dell'allegato VI.

Articolo 46

Fasi della valutazione inter pares

1. Durante la fase preparatoria i membri del gruppo di valutazione inter pares esaminano la documentazione dell'organismo di certificazione riguardante le sue politiche e procedure, compreso l'uso dei documenti sullo stato dell'arte.

2. Durante la fase di visita in loco il gruppo di valutazione inter pares valuta la competenza tecnica dell'organismo e, se del caso, la competenza di un'ITSEF che ha effettuato almeno una valutazione dei prodotti TIC oggetto della valutazione inter pares.

3. La durata della fase di visita in loco può essere prolungata o ridotta in base a fattori quali la possibilità di riutilizzare elementi di prova e risultati di una valutazione inter pares esistente o il numero di settori tecnici e ITSEF per cui l'organismo di certificazione rilascia i certificati.

4. Se applicabile, il gruppo di valutazione inter pares determina la competenza tecnica di ciascuna ITSEF visitando il suo laboratorio o i suoi laboratori tecnici e intervistandone i valutatori per quanto riguarda il settore tecnico e i relativi metodi di attacco specifici.

5. Nella fase di stesura della relazione il gruppo di valutazione documenta i propri risultati in una relazione di valutazione inter pares che include un verdetto e, se del caso, un elenco delle non conformità osservate, ciascuna classificata in base a un livello di criticità.

6. La relazione di valutazione inter pares deve essere innanzitutto discussa con l'organismo di certificazione oggetto di valutazione inter pares. A seguito di tali discussioni, l'organismo di certificazione oggetto di valutazione inter pares stabilisce un calendario delle misure da adottare per tenere conto dei risultati emersi.

Articolo 47

Relazione di valutazione inter pares

1. Il gruppo di valutazione inter pares fornisce all'organismo di certificazione oggetto di valutazione inter pares un progetto di relazione di valutazione inter pares.

2. L'organismo di certificazione oggetto di valutazione inter pares trasmette al gruppo di valutazione inter pares i commenti relativi ai risultati e un elenco degli impegni assunti per far fronte alle carenze individuate nel progetto di relazione di valutazione inter pares.

3. Il gruppo di valutazione inter pares trasmette al gruppo europeo per la certificazione della cibersicurezza una relazione finale di valutazione inter pares, che comprende anche i commenti e gli impegni assunti da parte dall'organismo di certificazione oggetto di valutazione inter pares. Il gruppo di valutazione inter pares indica anche la propria posizione in merito ai commenti e se ritiene che tali impegni siano sufficienti a colmare le carenze individuate.

4. Qualora nella relazione di valutazione inter pares siano individuate non conformità, il gruppo europeo per la certificazione della cibersicurezza può stabilire un termine adeguato entro il quale l'organismo di certificazione oggetto di valutazione inter pares deve far fronte a tali non conformità.

5. Il gruppo europeo per la certificazione della cibersicurezza adotta un parere sulla relazione di valutazione inter pares:

(a) se nella relazione di valutazione inter pares non sono state individuate non conformità o se l'organismo di certificazione oggetto di valutazione inter pares le ha affrontate adeguatamente, il gruppo europeo per la certificazione della cibersicurezza può formulare un parere positivo e tutti i documenti pertinenti sono pubblicati sul sito web dell'ENISA relativo alla certificazione;

(b) se l'organismo di certificazione oggetto di valutazione inter pares non affronta adeguatamente le non conformità entro il termine stabilito, il gruppo europeo per la certificazione della cibersicurezza può formulare un parere negativo che è pubblicato sul sito web dell'ENISA relativo alla certificazione, insieme alla relazione di valutazione inter pares e a tutti i documenti pertinenti.

6. Prima della pubblicazione del parere, tutte le informazioni sensibili, personali o proprietarie sono rimosse dai documenti pubblicati.

CAPO X

MANTENIMENTO DEL SISTEMA

Articolo 48

Mantenimento dell'EUCC

1. La Commissione può chiedere al gruppo europeo per la certificazione della cibersicurezza di adottare un parere al fine di mantenere l'EUCC e di intraprendere i lavori preparatori necessari.

2. Il gruppo europeo per la certificazione della cibersicurezza può adottare un parere per approvare documenti sullo stato dell'arte.

3. I documenti sullo stato dell'arte che sono stati approvati dal gruppo europeo per la certificazione della cibersicurezza sono pubblicati dall'ENISA.

CAPO XI

DISPOSIZIONI FINALI

Articolo 49

Sistemi nazionali contemplati dall'EUCC

1. In conformità dell'articolo 57, paragrafo 1, del regolamento (UE) 2019/881 e fatto salvo l'articolo 57, paragrafo 3, di tale regolamento, tutti i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e i processi TIC contemplati dall'EUCC cessano di produrre effetti a decorrere da 12 mesi dopo l'entrata in vigore del presente regolamento.

2. In deroga all'articolo 50 una procedura di certificazione può essere avviata nell'ambito di un sistema nazionale di certificazione della cibersicurezza entro 12 mesi dall'entrata in vigore del presente regolamento a condizione che sia ultimata entro 24 mesi dall'entrata in vigore del presente regolamento.

3. I certificati rilasciati nell'ambito dei sistemi nazionali di certificazione della cibersicurezza possono essere soggetti a riesame. I nuovi certificati che sostituiscono i certificati oggetto di riesame sono rilasciati conformemente al presente regolamento.

Articolo 50

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere dal 27 febbraio 2025.

Il capo IV e l'allegato V si applicano a partire dalla data di entrata in vigore del presente regolamento.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 31 gennaio 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

Tettori tecnici e documenti sullo stato dell'arte

1. Settori tecnici al livello AVA_VAN 4 o 5:

   (a) documenti relativi alla valutazione armonizzata del settore tecnico «smart card e dispositivi simili» e in particolare i seguenti documenti, nelle rispettive versioni in vigore il [data di entrata in vigore]:

      (1) «*Minimum ITSEF requirements for security evaluations of smart cards and similar devices*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (2) «*Minimum Site Security Requirements*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (3) «*Application of Common Criteria to integrated circuits*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (4) «*Security Architecture requirements (ADV_ARC) for smart cards and similar devices*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (5) «*Certification of "open" smart card products*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (6) «*Composite product evaluation for smart cards and similar devices*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (7) «*Application of Attack Potential to Smartcards*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

   (b) documenti relativi alla valutazione armonizzata del settore tecnico «dispositivi hardware con box di sicurezza» e in particolare i seguenti documenti, nelle rispettive versioni in vigore il [data di entrata in vigore]:

      (1) «*Minimum ITSEF requirements for security evaluations of hardware devices with security boxes*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (2) «*Minimum Site Security Requirements*», inizialmente approvato dall'ECCG il 20 ottobre 2023;

      (3) «*Application of Attack Potential to hardware devices with security boxes*», inizialmente approvato dall'ECCG il 20 ottobre 2023.

2. Documenti sullo stato dell'arte nelle rispettive versioni in vigore il [data di entrata in vigore]:

   (a) documento relativo all'accreditamento armonizzato degli organismi di valutazione della conformità: «*Accreditation of ITSEFs for the EUCC*», inizialmente approvato dall'ECCG il 20 ottobre 2023.

ALLEGATO II

Profili di protezione certificati al livello AVA_VAN 4 o 5

1. Per la categoria dei dispositivi qualificati per la creazione di firme e sigilli a distanza:

(1) EN 419241-2:2019 – Sistemi affidabili che supportano la firma lato server – Parte 2: profili di protezione per QSCD per la firma lato server;

(2) EN 419221-5:2018 – Profili di protezione per moduli crittografici TSP – Parte 5: moduli crittografici per servizi fiduciari.

2. Profili di protezione che sono stati adottati come documenti sullo stato dell'arte:

[BLANK]

ALLEGATO III

Profili di protezione raccomandati (che illustrano i settori tecnici di cua all'allegato I)

Profili di protezione utilizzati per la certificazione di prodotti TIC che rientrano nella categoria di prodotti TIC indicata di seguito:

(a) per la categoria dei documenti di viaggio a lettura ottica:

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

(2) *PP for a Machine Readable Travel Document with «ICAO Application» Extended Access Control,* BSI-CC-PP-0056-2009;

(3) *PP for a Machine Readable Travel Document with «ICAO Application» Extended Access Control with PACE,* BSI-CC-PP-0056-V2-2012-MA-02;

(4) *PP for a Machine Readable Travel Document with «ICAO Application» Basic Access Control,* BSI-CC-PP-0055-2009;

(b) per la categoria dei dispositivi di creazione di firma sicura:

(1) EN 419211-1:2014 – Profili di protezione per dispositivi di creazione di firma sicura – Parte 1: visione d'insieme

(2) EN 419211-2:2013 – Profili di protezione per dispositivi di creazione di firma sicura – Parte 2: dispositivi con generatore di chiave;

(3) EN 419211-3:2013 – Profili di protezione per dispositivi di creazione di firma sicura – Parte 3: dispositivi con importazione di chiave;

(4) EN 419211-4:2013 – Profili di protezione per dispositivi di creazione di firma sicura – Parte 4: estensione per dispositivo con generatore di chiave e canale sicuro per applicazione di generazione di certificato;

(5) EN 419211-5:2013 – Profili di protezione per dispositivi di creazione di firma sicura – Parte 5: estensione per dispositivo con generatore di chiave e canale sicuro per applicazione di creazione di firma;

(6) EN 419211-6:2014 – Profili di protezione per dispositivi di creazione di firma sicura – Parte 6: estensione per il dispositivo con importazione di chiave e canale attendibile per applicazione di creazione di firma;

(c) per la categoria dei tachigrafi digitali:

(1) tachigrafo digitale – carta tachigrafica, come indicato nel regolamento di esecuzione (UE) 2016/799 della Commissione, del 18 marzo 2016, che applica il regolamento (UE) n. 165/2014 (allegato IC);

(2) tachigrafo digitale – unità elettronica di bordo di cui all'allegato IB del regolamento (CE) n. 1360/2002 della Commissione destinata al montaggio in veicoli per i trasporti stradali;

(3) tachigrafo digitale – dispositivo esterno del GNSS (EGF PP) di cui all'allegato IC del regolamento di esecuzione (UE) 2016/799 della Commissione, del 18 marzo 2016, che applica il regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio;

(4) tachigrafo digitale – sensore di movimento (MS PP) di cui all'allegato IC del regolamento di esecuzione (UE) 2016/799 della Commissione, del 18 marzo 2016, che applica il regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio;

(d) per la categoria dei circuiti integrati sicuri, delle smart card e dei relativi dispositivi:

(1) *Security IC Platform PP,* 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) *PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16,* ANSSI-CC-PP-2015/07;

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

(6) *Embedded UICC (eUICC) for Machine-to-Machine Devices*, BSI-CC-PP-0089-2015;

(e) per la categoria dei punti di interazione (di pagamento) e dei terminali di pagamento:

(1) punto di interazione «POI-CHIP-ONLY», ANSSI-CC-PP-2015/01;

(2) punto di interazione «POI-CHIP-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/02;

(3) punto di interazione «POI-COMPREHENSIVE», ANSSI-CC-PP-2015/03;

(4) punto di interazione «POI-COMPREHENSIVE and Open Protocol Package», ANSSI-CC-PP-2015/04;

(5) punto di interazione «POI-PED-ONLY», ANSSI-CC-PP-2015/05;

(6) punto di interazione «POI-PED-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/06;

(f) per la categoria dei dispositivi hardware con box di sicurezza:

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

(2) *Cryptographic Module for CSP key generation services* – PP CMCSOB, PP HSM CMCSOB 14167-3, ANSSI-CC-PP-2015/09;

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

ALLEGATO IV

CONTINUITÀ DELL'AFFIDABILITÀ E RIESAME DEI CERTIFICATI

IV.1 **Continuità dell'affidabilità: ambito di applicazione**

1. I seguenti requisiti per la continuità dell'affidabilità si applicano alle attività di mantenimento relative a quanto segue:

   (a) una nuova valutazione se un prodotto TIC certificato rimasto invariato soddisfa ancora i requisiti di sicurezza;

   (b) una valutazione dell'impatto delle modifiche apportate a un prodotto TIC certificato sulla sua certificazione;

   (c) se inclusa nella certificazione, l'applicazione di patch in conformità di un processo di gestione delle patch valutato;

   (d) se incluso, il riesame dei processi di produzione o di gestione del ciclo di vita del titolare del certificato.

2. Il titolare di un certificato EUCC può richiedere il riesame del certificato nei casi seguenti:

   (a) il certificato EUCC scadrà entro i successivi nove mesi;

   (b) si è verificata una modifica del prodotto TIC certificato o di un altro fattore che potrebbe avere un impatto sulla sua funzionalità di sicurezza;

   (c) il titolare del certificato richiede che sia effettuata nuovamente la valutazione delle vulnerabilità al fine di riconfermare l'affidabilità del certificato EUCC associata alla resistenza del prodotto TIC agli attuali attacchi informatici.

IV.2 **Nuova valutazione**

1. Qualora sia necessario valutare l'impatto dei cambiamenti nel panorama delle minacce di un prodotto TIC certificato rimasto invariato, è presentata all'organismo di certificazione una richiesta di nuova valutazione.

2. La nuova valutazione è effettuata dalla stessa ITSEF che ha partecipato alla valutazione precedente, che riutilizza tutti i risultati ancora validi. La valutazione si concentra sulle attività di garanzia dell'affidabilità che sono potenzialmente interessate dai cambiamenti nel panorama delle minacce del prodotto TIC certificato, in particolare la famiglia AVA_VAN pertinente, nonché la famiglia del ciclo di vita dell'affidabilità (*assurance lifecycle*, ALC) per le quali sono nuovamente raccolti elementi di prova sufficienti sulla manutenzione dell'ambiente di sviluppo.

3. L'ITSEF descrive i cambiamenti e presenta nel dettaglio i risultati della nuova valutazione con un aggiornamento della precedente relazione tecnica di valutazione.

4. L'organismo di certificazione esamina la relazione tecnica di valutazione aggiornata e redige una relazione di nuova valutazione. Lo stato del certificato iniziale è quindi modificato in conformità dell'articolo 13.

5. La relazione di nuova valutazione e il certificato aggiornato sono forniti all'autorità nazionale di certificazione della cibersicurezza e all'ENISA per la pubblicazione sul sito web relativo alla certificazione della cibersicurezza.

IV.3 **Modifiche di un prodotto TIC certificato**

1. Se un prodotto TIC certificato è stato soggetto a modifiche, il titolare del certificato che intende mantenerlo fornisce all'organismo di certificazione una relazione sull'analisi dell'impatto.

2. Nella relazione sull'analisi dell'impatto sono forniti gli elementi seguenti:

   (a) un'introduzione contenente le informazioni necessarie per identificare la relazione sull'analisi dell'impatto e l'oggetto della valutazione soggetto a modifiche;

(b) una descrizione delle modifiche apportate al prodotto;

(c) l'identificazione della *developer evidence* interessata;

(d) una descrizione delle modifiche della *developer evidence*;

(e) i risultati e le conclusioni in merito all'impatto sull'affidabilità per ciascuna modifica.

3. L'organismo di certificazione esamina le modifiche descritte nella relazione sull'analisi dell'impatto per convalidare il loro impatto sull'affidabilità dell'oggetto della valutazione certificato, come proposto nelle conclusioni di detta relazione.

4. A seguito dell'esame, l'organismo di certificazione stabilisce l'entità di una modifica definendola minore o maggiore in base al suo impatto.

5. Qualora l'organismo di certificazione abbia confermato che le modifiche sono di minore entità, è rilasciato un nuovo certificato per il prodotto TIC modificato ed è redatta una relazione di manutenzione in riferimento alla relazione di certificazione iniziale alle condizioni seguenti:

(a) la relazione di manutenzione è inclusa come sottoinsieme della relazione sull'analisi dell'impatto e contiene le sezioni seguenti:

(1) introduzione;

(2) descrizione delle modifiche;

(3) *developer evidence* interessata;

(b) la data di validità del nuovo certificato non supera quella del certificato iniziale.

6. Il nuovo certificato, compresa la relazione di manutenzione, è fornito all'ENISA per la pubblicazione sul sito web relativo alla certificazione della cibersicurezza.

7. Nel caso in cui sia stato confermato che le modifiche sono di maggiore entità, si procede a una nuova valutazione nel contesto della valutazione precedente e riutilizzando tutti i risultati della valutazione precedente ancora validi.

8. Al termine della valutazione dell'oggetto della valutazione modificato, l'ITSEF redige una nuova relazione tecnica di valutazione. L'organismo di certificazione esamina la relazione tecnica di valutazione aggiornata e, se del caso, redige un nuovo certificato con una nuova relazione di certificazione.

9. Il nuovo certificato e la nuova relazione di certificazione sono forniti all'ENISA per la pubblicazione.

IV.4 **Gestione delle patch**

1. Una procedura di gestione delle patch prevede un processo strutturato di aggiornamento di un prodotto TIC certificato. La procedura di gestione delle patch, compreso il meccanismo attuato nel prodotto TIC dal richiedente la certificazione, può essere utilizzata dopo la certificazione del prodotto TIC sotto la responsabilità dell'organismo di valutazione della conformità.

2. Il richiedente la certificazione può includere nella certificazione del prodotto TIC un meccanismo di patch come parte di una procedura di gestione certificata implementata nel prodotto TIC a una delle condizioni seguenti:

(a) le funzionalità interessate dalla patch non rientrano nell'oggetto della valutazione del prodotto TIC certificato;

(b) la patch riguarda una modifica di piccola entità predeterminata del prodotto TIC certificato;

(c) la patch riguarda una vulnerabilità confermata con effetti critici sulla sicurezza del prodotto TIC certificato.

3. Se la patch si riferisce a una modifica di grande entità dell'oggetto della valutazione del prodotto TIC certificato in relazione a una vulnerabilità precedentemente non rilevata che non ha effetti critici per la sicurezza del prodotto TIC, si applicano le disposizioni dell'articolo 13.

4. La procedura di gestione delle patch per un prodotto TIC sarà composta dagli elementi seguenti:

   (a) il processo di sviluppo e rilascio della patch per il prodotto TIC;

   (b) il meccanismo tecnico e le funzioni per l'adozione della patch nel prodotto TIC;

   (c) una serie di attività di valutazione relative all'efficacia e alle prestazioni del meccanismo tecnico.

5. Durante la certificazione del prodotto TIC:

   (a) il richiedente la certificazione del prodotto TIC fornisce la descrizione della procedura di gestione delle patch;

   (b) l'ITSEF verifica gli elementi seguenti:

      (1) lo sviluppatore ha implementato i meccanismi di patch nel prodotto TIC in conformità della procedura di gestione delle patch presentata ai fini della certificazione;

      (2) i limiti dell'oggetto della valutazione sono separati in modo che le modifiche apportate ai processi separati non influiscano sulla sicurezza dell'oggetto della valutazione;

      (3) il meccanismo tecnico delle patch funziona in conformità delle disposizioni della presente sezione e delle dichiarazioni del richiedente;

   (c) l'organismo di certificazione include nella relazione di certificazione l'esito della procedura di gestione delle patch valutata.

6. Il titolare del certificato può procedere all'applicazione della patch prodotta nel rispetto della procedura di gestione delle patch certificata al prodotto TIC certificato in questione e adotta le seguenti misure entro cinque giorni lavorativi nei casi indicati di seguito:

   (a) nel caso di cui al punto 2, lettera a), segnala la patch in questione all'organismo di certificazione, che non modifica il corrispondente certificato EUCC;

   (b) nel caso di cui al punto 2, lettera b), sottopone la patch in questione all'ITSEF per il riesame. L'ITSEF informa l'organismo di certificazione della ricezione della patch, e l'organismo di certificazione adotta le misure appropriate per l'emissione di una nuova versione del corrispondente certificato EUCC e l'aggiornamento della relazione di certificazione;

   (c) nel caso di cui al punto 2, lettera c), sottopone la patch in questione all'ITSEF per la nuova valutazione necessaria, ma può distribuire la patch in parallelo. L'ITSEF informa l'organismo di certificazione, che a sua volta avvia le relative attività di certificazione.

ALLEGATO V

CONTENUTO DELLA RELAZIONE DI CERTIFICAZIONE

V.1 **Relazione di certificazione**

1. Sulla base delle relazioni tecniche di valutazione fornite dall'ITSEF, l'organismo di certificazione redige una relazione di certificazione da pubblicare insieme al corrispondente certificato EUCC.

2. La relazione di certificazione è la fonte di informazioni dettagliate e pratiche sul prodotto TIC o sulla categoria di prodotti TIC e sulla diffusione sicura degli stessi, e pertanto include tutte le informazioni disponibili e condivisibili pubblicamente rilevanti per gli utenti e i portatori di interesse. La relazione di certificazione può fare riferimento a informazioni disponibili e condivisibili pubblicamente.

3. La relazione di certificazione contiene almeno le sezioni seguenti:

   (a) sintesi;

   (b) identificazione del prodotto TIC o della categoria di prodotti TIC per i profili di protezione;

   (c) servizi di sicurezza;

   (d) ipotesi e chiarimento dell'ambito di applicazione;

   (e) informazioni sull'architettura;

   (f) informazioni supplementari sulla cibersicurezza, se applicabili;

   (g) prove del prodotto TIC, se sono state eseguite;

   (h) se del caso, l'identificazione dei processi di gestione del ciclo di vita e degli impianti di produzione del titolare del certificato;

   (i) risultati della valutazione e informazioni relative al certificato;

   (j) sintesi del traguardo di sicurezza del prodotto TIC sottoposto a certificazione;

   (k) se disponibile, il marchio o l'etichetta associati al sistema;

   (l) bibliografia.

4. La sintesi è un breve riassunto dell'intera relazione di certificazione. La sintesi fornisce una panoramica chiara e concisa dei risultati della valutazione e include le informazioni seguenti:

   (a) nome del prodotto TIC valutato, elenco dei componenti del prodotto che fanno parte della valutazione e versione del prodotto TIC;

   (b) nome dell'ITSEF che ha effettuato la valutazione e se del caso elenco dei subcontraenti;

   (c) data di conclusione della valutazione;

   (d) riferimento alla relazione tecnica di valutazione redatta dall'ITSEF;

   (e) breve descrizione dei risultati della relazione di certificazione, tra cui:

      (1) la versione e l'eventuale *release* dei criteri comuni applicata alla valutazione;

      (2) il pacchetto di affidabilità dei criteri comuni e i componenti della garanzia della sicurezza, compreso il livello AVA_VAN applicato durante la valutazione e il corrispondente livello di affidabilità di cui all'articolo 52 del regolamento (UE) 2019/881 a cui si riferisce il certificato EUCC;

      (3) la funzionalità di sicurezza del prodotto TIC valutato;

      (4) una sintesi delle minacce e delle politiche di sicurezza organizzativa trattate dal prodotto TIC valutato;

(5) requisiti speciali di configurazione;

(6) ipotesi sull'ambiente operativo;

(7) se applicabile, la presenza di una procedura di gestione delle patch approvata in conformità dell'allegato IV, sezione IV.4;

(8) una o più clausole di esclusione della responsabilità.

5. Il prodotto TIC valutato è chiaramente identificato, anche indicando le informazioni seguenti:

(a) il nome del prodotto TIC valutato;

(b) un elenco dei componenti del prodotto TIC che fanno parte della valutazione;

(c) il numero di versione dei componenti del prodotto TIC;

(d) l'identificazione di requisiti aggiuntivi per l'ambiente operativo del prodotto TIC certificato;

(e) il nome e le informazioni di contatto del titolare del certificato EUCC;

(f) ove applicabile, la procedura di gestione delle patch inclusa nel certificato;

(g) il link al sito web del titolare del certificato EUCC dove sono fornite informazioni supplementari sulla cibersicurezza per il prodotto TIC certificato in conformità dell'articolo 55 del regolamento (UE) 2019/881.

6. Le informazioni incluse in questa sezione sono il più possibile accurate per garantire una rappresentazione completa e precisa del prodotto TIC che può essere riutilizzata nelle valutazioni future.

7. La sezione sulle politiche di sicurezza contiene la descrizione della politica di sicurezza del prodotto TIC, nonché le politiche o le norme che il prodotto TIC valutato applica o rispetta. Essa include un riferimento e una descrizione delle politiche seguenti:

(a) la politica di gestione delle vulnerabilità del titolare del certificato;

(b) la politica di continuità dell'affidabilità del titolare del certificato.

8. Se applicabile, la politica può includere le condizioni relative all'utilizzo di una procedura di gestione delle patch durante la validità del certificato.

9. La sezione relativa alle ipotesi e al chiarimento dell'ambito di applicazione contiene informazioni esaurienti sulle circostanze e sugli obiettivi relativi all'uso previsto del prodotto, come indicato nell'articolo 7, paragrafo 1, lettera c). Le informazioni comprendono:

(a) ipotesi sull'utilizzo e sulla diffusione del prodotto TIC sotto forma di requisiti minimi, come la corretta installazione e configurazione e il soddisfacimento dei requisiti hardware;

(b) ipotesi sull'ambiente per il funzionamento del prodotto TIC nel rispetto delle norme.

10. Le informazioni elencate al punto 9 sono il più possibile comprensibili, in modo da consentire agli utenti del prodotto TIC certificato di prendere decisioni consapevoli sui rischi associati al suo utilizzo.

11. La sezione relativa alle informazioni sull'architettura include una descrizione di alto livello del prodotto TIC e dei suoi componenti principali in conformità con la progettazione dei sottosistemi ADV_TDS dei criteri comuni.

12. In conformità dell'articolo 55 del regolamento (UE) 2019/881 è fornito un elenco completo delle informazioni supplementari sulla cibersicurezza del prodotto TIC. Tutta la documentazione pertinente è indicata con i numeri di versione.

13. La sezione relativa alle prove del prodotto TIC include le informazioni seguenti:

(a) il nome e il punto di contatto dell'autorità o dell'organismo che ha rilasciato il certificato, compresa l'autorità nazionale di certificazione della cibersicurezza responsabile;

(b) il nome dell'ITSEF che ha effettuato la valutazione, se diversa dall'organismo di certificazione;

(c) l'identificazione dei componenti dell'affidabilità utilizzati in base alle norme di cui all'articolo 3;

(d) la versione del documento sullo stato dell'arte e ulteriori criteri di valutazione della sicurezza utilizzati nella valutazione;

(e) le impostazioni e la configurazione complete e precise del prodotto TIC durante la valutazione, comprese le note e le osservazioni operative, se disponibili;

(f) l'eventuale profilo di protezione utilizzato, comprese le informazioni seguenti:

(1) l'autore del profilo di protezione;

(2) il nome e l'identificatore del profilo di protezione;

(3) l'identificatore del certificato del profilo di protezione;

(4) il nome e i dati di contatto dell'organismo di certificazione e dell'ITSEF coinvolti nella valutazione del profilo di protezione;

(5) il pacchetto o i pacchetti di affidabilità richiesti per un prodotto conforme al profilo di protezione.

14. La sezione relativa ai risultati della valutazione e alle informazioni sul certificato include le informazioni seguenti:

(a) conferma del livello di affidabilità raggiunto di cui all'articolo 4 del presente regolamento e all'articolo 52 del regolamento (UE) 2019/881;

(b) requisiti di affidabilità in base alle norme di cui all'articolo 3 che il prodotto TIC o il profilo di protezione effettivamente soddisfa, compreso il livello AVA_VAN;

(c) descrizione dettagliata dei requisiti di affidabilità, nonché informazioni dettagliate relative alle modalità con cui il prodotto soddisfa ciascuno di essi;

(d) la data di rilascio e il periodo di validità del certificato;

(e) l'identificatore unico del certificato.

15. Il traguardo di sicurezza è incluso oppure menzionato e riassunto nella relazione di certificazione e fornito insieme alla stessa ai fini della pubblicazione.

16. Il traguardo di sicurezza può essere adattato in conformità della sezione VI.2.

17. Il marchio o l'etichetta associati all'EUCC possono essere inseriti nella relazione di certificazione in conformità delle norme e delle procedure stabilite dall'articolo 11.

18. La sezione relativa alla bibliografia contiene i riferimenti a tutti i documenti utilizzati per la compilazione della relazione di certificazione. Tali informazioni comprendono almeno gli elementi seguenti:

(a) i criteri di valutazione della sicurezza, i documenti sullo stato dell'arte e altre specifiche pertinenti utilizzati e la loro versione;

(b) la relazione tecnica di valutazione;

(c) la relazione tecnica di valutazione per la valutazione dei compositi, ove applicabile;

(d) la documentazione tecnica di riferimento;

(e) la documentazione dello sviluppatore utilizzata per la valutazione.

19. Al fine di garantire la riproducibilità della valutazione, tutta la documentazione a cui si fa riferimento deve essere identificata in modo univoco con la data di rilascio e il numero di versione corretti.

V.2 **Adattamento di un traguardo di sicurezza ai fini della pubblicazione**

1. Il traguardo di sicurezza da includere o a cui si fa riferimento nella relazione di certificazione a norma della sezione VI.1, punto 1, può essere adattato rimuovendo o parafrasando le informazioni tecniche proprietarie.

2. Il traguardo di sicurezza adattato che ne risulta è una rappresentazione reale della sua versione originale completa. Ciò significa che il traguardo di sicurezza adattato non può omettere le informazioni necessarie per comprendere le proprietà di sicurezza dell'oggetto della valutazione e l'ambito della valutazione.

3. Il contenuto del traguardo di sicurezza adattato è conforme ai requisiti minimi seguenti:
   (a) la sua introduzione non è adattata, dal momento che generalmente non contiene informazioni proprietarie;
   (b) il traguardo di sicurezza adattato deve avere un identificatore unico, distinto dalla sua versione originale completa;
   (c) la descrizione dell'oggetto della valutazione può essere ridotta in quanto potrebbe includere informazioni proprietarie e dettagliate sulla progettazione dell'oggetto della valutazione che non dovrebbero essere pubblicate;
   (d) la descrizione dell'ambiente di sicurezza dell'oggetto della valutazione (ipotesi, minacce, politiche di sicurezza organizzativa) non è ridotta, nella misura in cui tali informazioni siano necessarie per comprendere l'ambito della valutazione;
   (e) gli obiettivi di sicurezza non sono ridotti, poiché tutte le informazioni devono essere rese pubbliche per comprendere l'intenzione del traguardo di sicurezza e dell'oggetto della valutazione;
   (f) tutti i requisiti di sicurezza sono resi pubblici. Le note applicative possono fornire informazioni sulle modalità con cui i requisiti funzionali dei criteri comuni di cui all'articolo 3 sono stati utilizzati per comprendere il traguardo di sicurezza;
   (g) la sintesi delle specifiche dell'oggetto della valutazione include tutte le funzioni di sicurezza dell'oggetto della valutazione, ma le informazioni proprietarie aggiuntive possono essere adattate;
   (h) sono inclusi i riferimenti ai profili di protezione applicati all'oggetto della valutazione;
   (i) le motivazioni possono essere adattate al fine di rimuovere le informazioni proprietarie.

4. Anche se il traguardo di sicurezza adattato non è formalmente valutato in conformità delle norme di valutazione di cui all'articolo 3, l'organismo di certificazione garantisce che sia conforme al traguardo di sicurezza completo e valutato e che nella relazione di certificazione siano indicati sia il traguardo di sicurezza completo sia quello adattato.

ALLEGATO VI

AMBITO DELLA VALUTAZIONE INTER PARES E COMPOSIZIONE DEL GRUPPO DI VALUTAZIONE

VI.1 **Ambito della valutazione inter pares**

1. Sono contemplati i tipi di valutazione inter pares seguenti:

   (a) tipo 1: quando un organismo di certificazione effettua attività di certificazione al livello AVA_VAN.3;

   (b) tipo 2: quando un organismo di certificazione effettua attività di certificazione relative a un settore tecnico elencato come documento sullo stato dell'arte nell'allegato I;

   (c) tipo 3: quando un organismo di certificazione effettua attività di certificazione al di sopra del livello AVA_VAN.3 facendo uso di un profilo di protezione elencato come documento sullo stato dell'arte nell'allegato II o III.

2. L'organismo di certificazione oggetto di valutazione inter pares presenta l'elenco dei prodotti TIC certificati che possono essere candidati al riesame da parte del gruppo di valutazione inter pares in conformità delle norme seguenti:

   (a) i prodotti candidati coprono l'ambito di applicazione tecnico dell'autorizzazione dell'organismo di certificazione, di cui saranno analizzate almeno due diverse valutazioni di prodotti al livello di affidabilità «elevato» attraverso la valutazione inter pares, e un profilo di protezione se l'organismo di certificazione ha rilasciato un certificato al livello di affidabilità «elevato»;

   (b) per una valutazione inter pares di tipo 2, l'organismo di certificazione presenta almeno un prodotto per settore tecnico e per ITSEF interessata;

   (c) per una valutazione inter pares di tipo 3, è valutato almeno un prodotto candidato conformemente a un profilo di protezione applicabile e pertinente.

VI.2 **Gruppo di valutazione inter pares**

1. Il gruppo di valutazione è composto da almeno due esperti, ciascuno dei quali selezionato da un diverso organismo di certificazione di un diverso Stato membro che rilascia certificati al livello di affidabilità «elevato». Gli esperti devono dimostrare di possedere le competenze necessarie per quanto riguarda le norme di cui all'articolo 3 e i documenti sullo stato dell'arte che rientrano nell'ambito della valutazione inter pares.

2. In caso di delega per il rilascio dei certificati o previa approvazione degli stessi di cui all'articolo 56, paragrafo 6, del regolamento (UE) 2019/881, al gruppo di esperti selezionato in conformità del paragrafo 1 della presente sezione partecipa anche un esperto dell'autorità nazionale di certificazione della cibersicurezza correlata all'organismo di certificazione interessato.

3. Per una valutazione inter pares di tipo 2, i membri del gruppo sono selezionati tra gli organismi di certificazione autorizzati per il settore tecnico in questione.

4. Ogni membro del gruppo di valutazione possiede almeno due anni di esperienza nello svolgimento di attività di certificazione presso un organismo di certificazione.

5. Per una valutazione inter pares di tipo 2 o 3, ogni membro del gruppo di valutazione possiede almeno due anni di esperienza nello svolgimento di attività di certificazione nel settore tecnico o nel profilo di protezione pertinente e una comprovata esperienza e partecipazione nell'ambito dell'autorizzazione di un'ITSEF.

6. L'autorità nazionale di certificazione della cibersicurezza che controlla l'organismo di certificazione oggetto di valutazione inter pares e vigila sullo stesso e almeno un'autorità nazionale di certificazione della cibersicurezza, il cui organismo di certificazione non è soggetto alla valutazione inter pares, partecipano alla valutazione inter pares in qualità di osservatori. Anche l'ENISA può partecipare alla valutazione inter pares in qualità di osservatore.

7. La composizione del gruppo di valutazione inter pares è presentata all'organismo di certificazione oggetto di valutazione inter pares. In casi giustificati, quest'ultimo può contestare la composizione di tale gruppo e chiederne la revisione.

ALLEGATO VII

Contenuto del certificato EUCC

Il certificato EUCC deve contenere almeno i seguenti elementi:

(a) identificatore unico stabilito dall'organismo di certificazione che rilascia il certificato;

(b) informazioni relative al prodotto TIC o al profilo di protezione certificato e al titolare del certificato, tra cui:

  (1) nome del prodotto TIC o del profilo di protezione e, se del caso, dell'oggetto della valutazione;

  (2) tipo del prodotto TIC o del profilo di protezione e, se del caso, dell'oggetto della valutazione;

  (3) versione del prodotto TIC o del profilo di protezione;

  (4) nome, indirizzo e informazioni di contatto del titolare del certificato;

  (5) link al sito web del titolare del certificato contenente le informazioni supplementari sulla cibersicurezza di cui all'articolo 55 del regolamento (UE) 2019/881;

(c) informazioni relative alla valutazione e alla certificazione del prodotto TIC o del profilo di protezione, tra cui:

  (1) nome, indirizzo e informazioni di contatto dell'organismo di certificazione che ha rilasciato il certificato;

  (2) se differente dall'organismo di certificazione, nome dell'ITSEF che ha effettuato la valutazione;

  (3) nome dell'autorità nazionale di certificazione della cibersicurezza responsabile;

  (4) riferimento al presente regolamento;

  (5) riferimento alla relazione di certificazione associata al certificato di cui all'allegato V;

  (6) livello di affidabilità applicabile in conformità dell'articolo 4;

  (7) riferimento alla versione delle norme utilizzate per la valutazione di cui all'articolo 3;

  (8) identificazione del livello o del pacchetto di affidabilità specificato nelle norme di cui all'articolo 3 e in conformità dell'allegato VIII, compresi i componenti dell'affidabilità utilizzati e il livello AVA_VAN coperto;

  (9) se del caso, riferimento a uno o più profili di protezione che il prodotto TIC o il profilo di protezione rispettano;

  (10) data di rilascio;

  (11) periodo di validità del certificato;

(d) il marchio e l'etichetta associati al certificato in conformità dell'articolo 11.

ALLEGATO VIII

Dichiarazione del pacchetto di affidabilità

1. Contrariamente alle definizioni di cui ai criteri comuni, un incremento:

(a) non è identificato con l'abbreviazione «+»;

(b) è indicato in dettaglio con un elenco di tutti i componenti interessati;

(c) è descritto dettagliatamente nella relazione di certificazione.

2. Il livello di affidabilità confermato in un certificato EUCC può essere integrato dal livello di garanzia della valutazione di cui all'articolo 3 del presente regolamento.

3. Se il livello di affidabilità confermato in un certificato EUCC non si riferisce a un incremento, il certificato EUCC indica uno dei pacchetti seguenti:

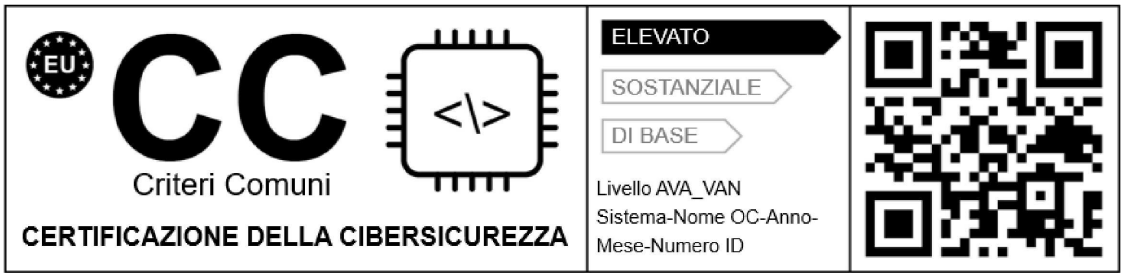
(a) «il pacchetto di affidabilità specifico»;

(b) «il pacchetto di affidabilità conforme a un profilo di protezione» nel caso in cui si faccia riferimento a un profilo di protezione senza un livello di garanzia della valutazione.

ALLEGATO IX

Marchio ed etichetta

1. Formato del marchio e dell'etichetta:



2. In caso di riduzione o di ingrandimento del marchio e dell'etichetta, sono rispettate le proporzioni indicate nel disegno sopra riportato.

3. Se fisicamente presenti, il marchio e l'etichetta hanno un'altezza minima di 5 mm.