2025/2462

9.12.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/2462 DELLA COMMISSIONE

dell'8 dicembre 2025

che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le definizioni, la certificazione delle serie di prodotti TIC, la continuità dell'affidabilità e i documenti sullo stato dell'arte

(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 regolamento di esecuzione (UE) 2024/482 della Commissione ([2]) 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.

(2) La metodologia comune di valutazione che accompagna i criteri comuni, una norma internazionale per la valutazione della sicurezza delle informazioni, consente di valutare la sicurezza dei prodotti TIC a fini di certificazione. In tale contesto alcuni prodotti TIC, denominati anche serie di prodotti, possono essere concepiti sulla stessa base funzionale al fine di offrire funzionalità di sicurezza simili su piattaforme o dispositivi diversi. La progettazione, l'hardware, il firmware o il software possono tuttavia variare da un prodotto TIC all'altro. Spetta all'organismo di certificazione decidere caso per caso se sia possibile effettuare la certificazione di una serie di prodotti. Le condizioni per la certificazione delle serie di prodotti potrebbero essere ulteriormente illustrate in orientamenti di sostegno dell'EUCC.

(3) Per mantenere l'affidabilità dei prodotti certificati, è essenziale definire cosa costituisca una modifica maggiore e minore dell'oggetto della valutazione o del suo ambiente, compresi i suoi ambienti operativi o di sviluppo. È pertanto necessario precisare tali nozioni tenendo conto delle specifiche tecniche esistenti e ampiamente utilizzate del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (SOG-IS) e dei partecipanti all'accordo «Arrangements on the Recognition of Common Criteria Certificate in the field of IT Security» (CCRA).

(4) Le modifiche minori sono spesso caratterizzate dal loro effetto limitato sulla dichiarazione di affidabilità del prodotto fornita dal certificato EUCC rilasciato. Le modifiche minori dovrebbero pertanto essere gestite nell'ambito delle procedure di mantenimento e non richiedere una nuova valutazione delle funzionalità di sicurezza del prodotto. Tra gli esempi di modifiche minori che dovrebbero essere trattate nell'ambito del mantenimento figurano, tra l'altro, le modifiche redazionali, le modifiche dell'ambiente dell'oggetto della valutazione che non incidono sull'oggetto della valutazione certificato e le modifiche dell'oggetto della valutazione certificato che non incidono sugli elementi di prova dell'affidabilità. Anche le modifiche dell'ambiente di sviluppo possono essere considerate minori, a condizione che non abbiano un impatto ulteriore sulle misure di affidabilità esistenti. In alcuni casi tali modifiche possono tuttavia richiedere una valutazione parziale delle misure pertinenti.

([1]) GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) 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) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Una modifica maggiore è qualsiasi modifica dell'oggetto della valutazione certificato o del suo ambiente che possa incidere negativamente sull'affidabilità espressa nel certificato EUCC, e dovrebbe pertanto richiedere una nuova valutazione. Tra gli esempi di modifiche maggiori figurano, tra l'altro, le modifiche della serie di requisiti di affidabilità dichiarati, fatta eccezione per i requisiti di affidabilità della famiglia CC ALC_FLR («Flaw remediation»); le modifiche dei controlli di riservatezza o integrità dell'ambiente di sviluppo, qualora tali modifiche possano pregiudicare lo sviluppo o la produzione sicuri dell'oggetto della valutazione, o le modifiche dell'oggetto della valutazione volte a risolvere una vulnerabilità sfruttabile. Inoltre, anche una serie di modifiche minori che esercitano collettivamente un impatto significativo sulla sicurezza può essere considerata una modifica maggiore. È importante anche riconoscere che, sebbene la correzione di un bug («bug fix») possa incidere solo su un aspetto specifico dell'oggetto della valutazione, la sua imprevedibilità e il suo potenziale impatto sull'affidabilità possono renderla una modifica maggiore qualora comprometta le garanzie di sicurezza fornite dalla certificazione.

(6) Le modifiche nel panorama delle minacce di un prodotto TIC certificato rimasto invariato potrebbero richiedere una nuova valutazione. È opportuno stabilire chiaramente i possibili esiti di tale processo di nuova valutazione, in particolare il suo impatto sul certificato EUCC. Se una nuova valutazione è completata con successo, l'organismo di certificazione dovrebbe confermare il certificato o rilasciarne uno nuovo con una data di scadenza prorogata. Se una nuova valutazione non ha esito positivo, l'organismo di certificazione dovrebbe revocare il certificato e eventualmente rilasciare un nuovo certificato con un ambito di applicazione diverso. Tali disposizioni dovrebbero applicarsi mutatis mutandis alla nuova valutazione dei profili di protezione.

(7) L'allegato I del regolamento di esecuzione (UE) 2024/482 elenca i documenti sullo stato dell'arte applicabili per la valutazione dei prodotti TIC e dei profili di protezione. Tali documenti sullo stato dell'arte dovrebbero essere aggiornati per tenere conto degli ultimi sviluppi, come quelli tecnologici o quelli relativi al panorama delle minacce informatiche, alle pratiche del settore o alle norme internazionali. Tale aggiornamento è opportuno per i documenti sullo stato dell'arte relativi ai requisiti minimi di sicurezza dei siti, all'applicazione dei potenziali di attacco alle smart card, all'applicazione dei potenziali di attacco ai dispositivi hardware con box di sicurezza, all'applicazione di criteri comuni ai circuiti integrati e alla valutazione di prodotto composito per le smart card e i dispositivi analoghi. Inoltre non sono inclusi i documenti sullo stato dell'arte relativi alla valutazione e alla certificazione di prodotto composito che utilizzano l'ultima versione delle norme sui criteri comuni, al riutilizzo dei risultati della valutazione degli audit dei siti e a chiarimenti sull'interpretazione dei profili di protezione relativi ai dispositivi qualificati per la creazione di una firma elettronica, ai tachigrafi e ai moduli di sicurezza hardware. Per garantire una valutazione uniforme dei prodotti TIC nell'ambito dell'EUCC, l'allegato I dovrebbe essere modificato per includervi i documenti sullo stato dell'arte aggiornati e nuovi a seguito della loro approvazione da parte del gruppo europeo per la certificazione della cibersicurezza.

(8) Il documento sullo stato dell'arte «ADV_SPM.1 interpretation for CC: 2022 transition» dovrebbe essere aggiunto al sistema per garantire che i processi di certificazione basati su profili di protezione specifici possano continuare a utilizzare la modellizzazione formale (ADV_SPM.1) fino all'aggiornamento dei corrispondenti profili di protezione, ad esempio con l'aggiunta di una configurazione dei profili di protezione multiaffidabilità conforme ai criteri comuni CC:2022 che supporta ADV_SPM.1. Per concedere al mercato tempo sufficiente per la transizione verso le norme sui criteri comuni aggiornate, è necessario prevedere norme transitorie specifiche per i profili di protezione «Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014», «Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020», oppure «Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020». Per evitare perturbazioni del mercato, è opportuno stabilire che il documento sullo stato dell'arte «ADV_SPM.1 interpretation for CC: 2022 transition» sia applicabile ai processi di certificazione avviati prima dell'adozione del presente regolamento. L'applicazione di tale documento dovrebbe tuttavia essere strettamente limitata a quanto necessario, considerando il tempo necessario per completare l'aggiornamento dei corrispondenti profili di protezione. Più precisamente, per i processi di certificazione che utilizzano i profili di protezione «Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014», oppure «Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020», il documento sullo stato dell'arte dovrebbe applicarsi ai processi avviati prima del 1º ottobre 2026. Per i processi di certificazione che utilizzano il profilo di protezione «Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020», il documento sullo stato dell'arte dovrebbe applicarsi solo ai processi avviati prima della data di entrata in vigore del presente regolamento, in considerazione del fatto che è già disponibile una nuova versione del profilo di protezione «Java Card System – Open Configuration».

(9) Una modifica dei documenti sullo stato dell'arte durante un processo di certificazione potrebbe perturbare la valutazione del prodotto e ritardare il rilascio del certificato. Sono pertanto necessarie adeguate norme transitorie per i documenti sullo stato dell'arte nuovi o aggiornati, al fine di consentire ai venditori, alle ITSEF, agli organismi di certificazione e ad altri portatori di interessi di apportare i necessari adeguamenti. I documenti sullo stato dell'arte applicabili, aggiornati e nuovi, dovrebbero riguardare le domande di certificazione, comprese le domande di nuova valutazione, mentre i processi di certificazione in corso dovrebbero poter continuare a utilizzare versioni precedenti dei documenti sullo stato dell'arte.

(10) Gli allegati II e III del regolamento di esecuzione (UE) 2024/482 elencano rispettivamente i profili di protezione certificati al livello AVA_VAN 4 o 5 e i profili di protezione raccomandati. Diversi riferimenti sono incompleti o obsoleti a causa di un aggiornamento dei profili di protezione. Tali riferimenti dovrebbero essere completati e, inoltre, dovrebbero essere inclusi nuovi riferimenti per garantire una copertura più completa dei circuiti integrati sicuri, delle smart card e relativi dispositivi e del trusted computing.

(11) È necessario modificare l'articolo 19 del regolamento di esecuzione (UE) 2024/482 per chiarire che l'allegato IV si applica, con le necessarie modifiche, al riesame dei certificati EUCC per i profili di protezione.

(12) Poiché il traguardo di sicurezza è un elemento chiave per comprendere la portata di un processo di certificazione, è altresì necessario che l'ENISA pubblichi sul proprio sito web il traguardo di sicurezza corrispondente a ciascun certificato EUCC.

(13) Gli organismi di certificazione dovrebbero inoltre fornire all'ENISA una versione in inglese del traguardo di sicurezza e della relazione di certificazione per consentire all'Agenzia di rendere disponibili tali informazioni in inglese sul sito web corrispondente, a norma dell'articolo 42, paragrafo 2, del regolamento di esecuzione (UE) 2024/482. Per tale motivo i richiedenti la certificazione dovrebbero fornire agli organismi di certificazione, ogniqualvolta richiesto, una versione in inglese del traguardo di sicurezza.

(14) Non è necessario che il riferimento al nome dell'organismo di certificazione figuri nell'identificatore unico del certificato, in quanto il numero di identificazione dell'organismo di certificazione è sufficiente per identificare tale organismo in modo univoco. Non deve figurare neppure il mese di rilascio, in quanto il conteggio dei certificati avviene su base annua. Tale requisito dovrebbe pertanto essere soppresso a fini di semplificazione. Poiché l'anno di rilascio del certificato corrisponde al rilascio del primo certificato, la stessa data dovrebbe figurare nell'identificatore unico dei certificati rilasciati dopo un riesame, al fine di garantire la tracciabilità.

(15) È pertanto opportuno modificare di conseguenza il regolamento di esecuzione (UE) 2024/482.

(16) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 66 del regolamento (UE) 2019/881,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Il regolamento di esecuzione (UE) 2024/482 è così modificato:

(1) all'articolo 2 sono aggiunti i seguenti punti 16, 17 e 18:

«(16) "serie di prodotti": un insieme di prodotti TIC di un richiedente, concepiti sulla stessa base funzionale per rispondere alle stesse esigenze di sicurezza, aventi una progettazione, un hardware, un firmware o un software che può variare da un prodotto TIC a un altro;

(17) "modifica minore": qualsiasi modifica dell'oggetto della valutazione certificato o del suo ambiente che non incide negativamente sull'affidabilità espressa nel certificato EUCC;

(18) "modifica maggiore": qualsiasi modifica dell'oggetto della valutazione certificato o del suo ambiente che può incidere negativamente sull'affidabilità espressa nel certificato EUCC.»;

(2) all'articolo 5 è aggiunto il seguente paragrafo 3:

«3. Un organismo di certificazione può consentire la certificazione di una serie di prodotti.»;

(3) all'articolo 9, paragrafo 2, la lettera a) è sostituita dalla seguente:

«a) presentazione all'organismo di certificazione e all'ITSEF di tutte le informazioni necessarie, complete e corrette, e di ulteriori informazioni necessarie se richiesto, compresa una versione in inglese del traguardo di sicurezza;»;

(4) all'articolo 11, paragrafo 3, la lettera b) è sostituita dalla seguente:

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

(1) denominazione del sistema;

(2) numero di identificazione, conformemente all'articolo 3 del regolamento di esecuzione (UE) 2024/3143, dell'organismo di certificazione che ha rilasciato il certificato;

(3) anno di rilascio del certificato iniziale;

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

(5) all'articolo 19, il paragrafo 1 è sostituito dal seguente:

«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 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 profilo di protezione certificato.»;

(6) l'articolo 42 è così modificato:

(a) al paragrafo 1 è aggiunta la seguente lettera i):

«i) il traguardo di sicurezza corrispondente a ciascun certificato EUCC.»;

(b) il paragrafo 2 è sostituito dal seguente:

«2. Le informazioni di cui al paragrafo 1 sono messe a disposizione almeno in inglese. A tal fine gli organismi di certificazione forniscono all'ENISA, unitamente alle versioni linguistiche originali delle relazioni di certificazione e dei traguardi di sicurezza, anche la versione in inglese di tali documenti senza indebito ritardo.»;

(7) all'articolo 48, il paragrafo 4 è sostituito dal seguente:

«4. Salvo diversa indicazione nell'allegato I o II, i documenti sullo stato dell'arte si applicano ai processi di certificazione, compresa la nuova valutazione, avviati a decorrere dalla data di applicazione dell'atto modificativo mediante il quale detti documenti sono stati introdotti nell'allegato I o II.»;

(8) l'allegato I è sostituito dal testo di cui all'allegato I del presente regolamento;

(9) l'allegato II è sostituito dal testo di cui all'allegato II del presente regolamento;

(10) l'allegato III è sostituito dal testo di cui all'allegato III del presente regolamento;

(11) l'allegato IV è modificato conformemente all'allegato IV del presente regolamento;

(12) l'allegato V è modificato conformemente all'allegato V del presente regolamento;

(13) l'allegato IX è sostituito dal testo di cui all'allegato VI del presente regolamento.

Articolo 2

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

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

Fatto a Bruxelles, l'8 dicembre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

«*ALLEGATO I*

Documenti sullo stato dell'arte a sostegno dei settori tecnici e altri documenti sullo stato dell'arte

1. Documenti sullo stato dell'arte a sostegno dei settori tecnici al livello AVA_VAN 4 o 5:
   (a) i seguenti documenti relativi alla valutazione armonizzata del settore tecnico "smart card e dispositivi simili":
      (1) "Minimum ITSEF requirements for security evaluations of smart cards and similar devices", versione 1.1;
      (2) "Minimum Site Security Requirements", versione 2;
      (3) "Reusing evaluation results of site audits (STAR)", versione 1;
      (4) "Application of Common Criteria to integrated circuits", versione 2;
      (5) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices", versione 1.1;
      (6) "Certification of 'open' smart card products", versione 1.1;
      (7) "Composite product evaluation for smart cards and similar devices for CC3.1", versione 2;
      (8) "Composite product evaluation and certification for CC:2022", versione 1;
      (9) "Application of Attack Potential to Smartcards and Similar Devices", versione 2;
      (10) "Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices", versione 1;
      (11) "ADV_SPM.1 interpretation for CC:2022 transition", versione 1.1, applicabile ai processi di certificazione che utilizzano profili di protezione nel modo seguente:
         (a) profili di protezione "Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014" o "Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020", avviati prima del 1º ottobre 2026;
         (b) profilo di protezione "Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020", avviato prima del 29 dicembre 2025;
   (b) i seguenti documenti relativi alla valutazione armonizzata del settore tecnico "dispositivi hardware con box di sicurezza":
      (1) "Minimum ITSEF requirements for security evaluations of hardware devices with security boxes", versione 1.1;
      (2) "Minimum Site Security Requirements", versione 2;
      (3) "Reusing evaluation results of site audits (STAR)", versione 1;
      (4) "Application of Attack Potential to hardware devices with security boxes", versione 2;
      (5) "Hardware assessment in EN 419221-5 (HSM PP)", versione 1;
      (6) "Jil Tachograph MS PP Clarification", versione 1.

2. Documenti sullo stato dell'arte relativi all'accreditamento armonizzato degli organismi di valutazione della conformità:
   (a) "Accreditation of ITSEFs for the EUCC", versione 1.1 per gli accreditamenti rilasciati prima dell'8 luglio 2025;
   (b) "Accreditation of ITSEFs for the EUCC", versione 1.6c, per i nuovi accreditamenti o per gli accreditamenti riesaminati dopo l'8 luglio 2025;
   (c) "Accreditation of CBs for the EUCC", versione 1.6b.».

ALLEGATO II

«ALLEGATO II

Profili di protezione certificati al livello AVA_VAN 4 o 5

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

   (a) EN 419241-2:2019 – Sistemi affidabili che supportano la firma lato server - Parte 2: profilo di protezione per QSCD per la firma lato server (v0.16), ANSSI-CC-PP-2018/02-M01;

   (b) EN 419221-5:2018 – Profili di protezione per moduli crittografici TSP - Parte 5: modulo crittografico per servizi fiduciari (v0.15), ANSSI-CC-PP-2016/05-M01.

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

   [...]».

ALLEGATO III

«*ALLEGATO III*

Profili di protezione raccomandati

Profili di protezione utilizzati nella certificazione dei prodotti TIC, compresi i prodotti nei settori tecnici:

1. smart card e dispositivi analoghi

   (a) Passaporti:

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

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

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

   (b) Dispositivi per la creazione di una firma sicura (SSCD):

      (1) EN 419211-2:2013 – Profili di protezione per dispositivi di creazione di firma sicura - Parte 2: dispositivi con generatore di chiave (v1.03), BSI-CC-PP-0059-2009-MA-02;

      (2) EN 419211-3:2013 – Profili di protezione per dispositivi di creazione di firma sicura - Parte 3: dispositivi con importazione di chiave (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      (3) 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 (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      (4) 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 (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      (5) EN 419211-6:2014 – Profili di protezione per dispositivi di creazione di firma sicura - Parte 6: estensione per dispositivo con importazione di chiave e canale sicuro per applicazione di creazione di firma (v1.0.4), BSI-CC-PP-0076-2013-MA-01.

   (c) Tachigrafi: Digital Tachograph – Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017.

   (d) Circuiti integrati sicuri, piattaforma Java Card e eUICC:

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

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

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

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

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

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

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

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

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

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

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

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

2. Dispositivi hardware con box di sicurezza
   (a) Punti di interazione (di pagamento) e terminali di pagamento (POI);
      (1) punto di interazione “POI-CHIP-ONLY”, (v4.0), ANSSI-CC-PP-2015/01;
      (2) punto di interazione “POI-CHIP-ONLY and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/02;
      (3) punto di interazione “POI-COMPREHENSIVE” (v4.0), ANSSI-CC-PP-2015/03;
      (4) punto di interazione “POI-COMPREHENSIVE and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/04;
      (5) punto di interazione “POI-PED-ONLY” (v4.0), ANSSI-CC-PP-2015/05;
      (6) punto di interazione “POI-PED-ONLY and Open Protocol Package” (v4.0), ANSSI-CC-PP-2015/06.
   (b) Moduli di sicurezza hardware:
      (1) Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;
      (2) Cryptographic Module for CSP Key Generation Services – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;
      (3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10.
   (c) Tachigrafi:
      (1) Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CC-PP-0093-2017;
      (2) Digital Tachograph – Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;
      (3) Digital Tachograph – External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.
3. Altri: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.».

ALLEGATO IV

L'allegato IV del regolamento di esecuzione (UE) 2024/482 è così modificato:

1. al punto IV.2, il punto 4 è sostituito dal seguente:

«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 o dell'articolo 19. Se il processo di nuova valutazione ha esito positivo, nel caso della certificazione di un prodotto si applica l'articolo 13, paragrafo 2, lettera a) o c), e nel caso della certificazione di un profilo di protezione si applica l'articolo 19, paragrafo 2, lettera a) o c). Se il processo di nuova valutazione non ha esito positivo, nel caso della certificazione di un prodotto si applica l'articolo 13, paragrafo 2, lettera b) o d), e nel caso della certificazione di un profilo di protezione si applica l'articolo 19, paragrafo 2, lettera b) o d).»;

2. il punto IV.3 è così modificato:

a) il titolo del punto IV.3 è sostituito dal seguente:

«IV.3 **Modifiche di un prodotto TIC certificato – Mantenimento e nuova valutazione**»

b) i punti 4) e 5) sono sostituiti dai seguenti:

«4. A seguito dell'esame, l'organismo di certificazione stabilisce l'entità di una modifica definendola minore o maggiore in base al suo impatto sull'affidabilità espressa nel certificato EUCC.

5. Qualora l'organismo di certificazione abbia confermato che le modifiche sono minori, non è rilasciato alcun nuovo certificato per il prodotto TIC modificato a norma dell'articolo 13, paragrafo 2, lettera a) o dell'articolo 19, paragrafo 2, lettera a) ed è redatta una relazione di manutenzione in riferimento alla relazione di certificazione iniziale.»;

c) è inserito il seguente punto 5 bis:

«5.bis In caso di modifiche delle misure di affidabilità nell'ambiente di sviluppo, compresa l'aggiunta di requisiti di affidabilità della famiglia CC ALC_FLR ("Flaw remediation"), l'organismo di certificazione può chiedere all'ITSEF di effettuare una valutazione del sottoinsieme delle misure di affidabilità interessate. L'ITSEF pubblica una relazione tecnica di valutazione parziale, sulla base della quale l'organismo di certificazione conferma che le modifiche sono minori o maggiori. Se le modifiche sono state confermate dall'organismo di certificazione come minori, si applica l'allegato IV.3, punto 5. Se le modifiche sono state confermate dall'organismo di certificazione come maggiori, si applica l'allegato IV.3, punto 7.».

ALLEGATO V

All'allegato V del regolamento di esecuzione (UE) 2024/482, il punto V.1 è sostituito dal seguente:

«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 certificato e al traguardo di sicurezza EUCC corrispondenti.

2. La relazione di certificazione è la fonte di informazioni dettagliate e pratiche sul prodotto TIC e sulla sua diffusione sicura. Essa include pertanto tutte le informazioni disponibili e condivisibili pubblicamente rilevanti per gli utenti e i portatori di interessi. La relazione di certificazione può fare riferimento a informazioni disponibili e condivisibili pubblicamente.

3. La relazione di certificazione contiene almeno le seguenti informazioni:
   (a) sintesi;
   (b) identificatore del prodotto TIC;
   (c) informazioni di contatto relative alla valutazione del prodotto TIC;
   (d) politiche di sicurezza;
   (e) ipotesi e chiarimento dell'ambito di applicazione;
   (f) informazioni sull'architettura;
   (g) informazioni supplementari sulla cibersicurezza, se applicabili;
   (h) sintesi della valutazione del prodotto TIC e configurazione valutata;
   (i) risultati della valutazione e informazioni relative al certificato;
   (j) osservazioni e raccomandazioni, se del caso;
   (k) allegati, se del caso;
   (l) riferimento al traguardo di sicurezza del prodotto TIC sottoposto a certificazione;
   (m) se disponibile, il marchio o l'etichetta associati al sistema;
   (n) glossario, se del caso;
   (o) bibliografia.

4. La sintesi di cui al paragrafo 3, lettera a) è un breve riassunto dell'intera relazione di certificazione e fornisce una panoramica chiara e concisa dei risultati della valutazione, con le informazioni seguenti:
   (a) nome del prodotto TIC valutato;
   (b) nome dell'ITSEF che ha effettuato la valutazione;
   (c) data di conclusione della valutazione;
   (d) data di rilascio del certificato;
   (e) se del caso, data di rilascio del certificato iniziale;
   (f) periodo di validità;
   (g) identificatore unico del certificato di cui all'articolo 11;
   (h) breve descrizione dei risultati della relazione di certificazione, tra cui:
      i) la versione e l'eventuale release dei criteri comuni applicata alla valutazione;
      ii) il pacchetto di affidabilità dei criteri comuni o un elenco dei componenti della garanzia della sicurezza, 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;
      iii) se del caso, il profilo o i profili di protezione cui il prodotto TIC dichiara la conformità;
      iv) un riferimento alla politica di sicurezza del prodotto TIC valutato;
      v) una o più clausole di esclusione della responsabilità, se del caso.

5. L'identificatore di cui al punto 3, lettera b), identifica chiaramente il prodotto TIC valutato e comprende le informazioni seguenti:

   (a) identificatore unico del prodotto TIC valutato;

   (b) elenco dei componenti del prodotto TIC che fanno parte della valutazione con il numero di versione di ciascun componente;

   (c) riferimento ai requisiti aggiuntivi per l'ambiente operativo del prodotto TIC certificato.

6. Tra le informazioni di contatto di cui al punto 3, lettera c), figura almeno quanto segue:

   (a) nome dello sviluppatore;

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

   (c) nome dell'organismo di certificazione che ha rilasciato il certificato;

   (d) autorità nazionale di certificazione della cibersicurezza responsabile;

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

7. La politica di sicurezza di cui al punto 3, lettera d) contiene la descrizione della politica di sicurezza del prodotto TIC quale insieme di servizi di sicurezza e delle politiche o norme che il prodotto TIC valutato applica o rispetta. Sono inoltre incluse le seguenti informazioni:

   (a) una descrizione delle procedure di gestione e divulgazione delle vulnerabilità del titolare del certificato, da completare esclusivamente con le informazioni che possono essere rese pubbliche;

   (b) la politica di continuità dell'affidabilità del titolare del certificato, compresa, se del caso, la descrizione della gestione del ciclo di vita o dei processi di produzione del titolare del certificato conformemente all'allegato IV, sezione IV.1;

   (c) se del caso, la presenza di una procedura di gestione delle patch e l'esito della sua valutazione conformemente all'allegato IV, sezione IV.4.

8. Le ipotesi e il chiarimento dell'ambito di applicazione di cui al punto 3, lettera e), contengono informazioni relative alle circostanze e agli obiettivi relativi all'uso previsto del prodotto, come indicato all'articolo 7, paragrafo 1, lettera c), e comprendono quanto segue:

   (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;

   (c) descrizione di eventuali minacce al prodotto TIC che non sono contrastate dalle funzioni di sicurezza valutate del prodotto in base all'uso previsto, se ritenuta pertinente per un potenziale utente di un prodotto TIC.

   Le informazioni di cui al primo comma sono il più possibile chiare e comprensibili, per consentire ai potenziali utenti del prodotto TIC certificato di prendere decisioni informate in merito ai rischi associati al suo utilizzo.

9. Tra le informazioni sull'architettura, di cui al punto 3, lettera f), figura una descrizione di alto livello del prodotto TIC e dei suoi componenti principali, sulla base dei deliverable definiti nella famiglia di affidabilità dei criteri comuni: Development - TOE Design (ADV_TDS).

10. Le informazioni supplementari sulla cibersicurezza di cui al punto 3, lettera g), comprendono il link al sito web del titolare del certificato EUCC di cui all'articolo 55 del regolamento (UE) 2019/881.

11. La valutazione e la configurazione del prodotto TIC di cui al punto 3, lettera h), descrivono le attività di prova sia dello sviluppatore che del valutatore, delineando l'approccio alle prove, la loro configurazione e la loro profondità. Vi figurano quantomeno le seguenti informazioni:

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

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

    (c) le impostazioni e la configurazione del TOE utilizzato per le prove e l'analisi delle vulnerabilità;

    (d) l'eventuale profilo di protezione utilizzato, comprese le informazioni seguenti: il nome, la versione, la data e il certificato del profilo di protezione.

12. I risultati della valutazione e le informazioni relative al certificato di cui al punto 3, lettera i), comprendono informazioni sul livello di affidabilità raggiunto di cui all'articolo 4 del presente regolamento e all'articolo 52 del regolamento (UE) 2019/881.

13. Le osservazioni e le raccomandazioni di cui al punto 3, lettera j), sono utilizzate per fornire ulteriori informazioni sui risultati della valutazione. Tali osservazioni e raccomandazioni possono illustrare carenze del prodotto TIC rilevate durante la valutazione o menzionare caratteristiche particolarmente utili.

14. Gli allegati di cui al punto 3, lettera k), sono utilizzati per delineare eventuali informazioni supplementari che possono essere utili ai destinatari della relazione ma che non rientrano logicamente nelle sezioni prescritte della relazione, anche nel caso di una descrizione completa della politica di sicurezza.

15. Il traguardo di sicurezza di cui al punto 3, lettera l), fa riferimento al traguardo di sicurezza valutato. Il traguardo di sicurezza valutato è corredato della relazione di certificazione ai fini della pubblicazione sul sito web di cui all'articolo 50, paragrafo 1, del regolamento (UE) 2019/881. Qualora sia necessario adattare il traguardo di sicurezza valutato prima della pubblicazione, si procede conformemente all'allegato V, punto V.2, del presente regolamento.

16. Il marchio o l'etichetta associati al sistema EUCC di cui al punto 3, lettera m), sono inseriti nella relazione di certificazione in conformità delle norme e delle procedure stabilite dall'articolo 11.

17. Il glossario di cui al punto 3, lettera n), è utilizzato per aumentare la leggibilità della relazione fornendo definizioni di acronimi o termini il cui significato potrebbe non essere immediatamente evidente.

18. La bibliografia di cui al punto 3, lettera o), contiene i riferimenti a tutti i documenti utilizzati per la compilazione della relazione di certificazione. Tali informazioni comprendono almeno i seguenti elementi:

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

    (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) orientamenti in materia di sicurezza dello sviluppatore;

    (f) elenco delle configurazioni dello sviluppatore.

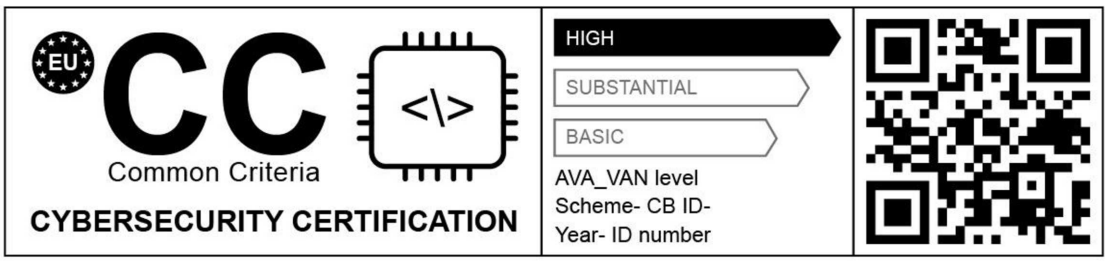
    Al fine di garantire la riproducibilità della valutazione, tutta la documentazione a cui si fa riferimento deve essere identificata in modo univoco con la data di rilascio e il numero di versione corretti.».

ALLEGATO VI

«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 al punto 1.

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