2024/3144

19.12.2024

REGOLAMENTO DI ESECUZIONE (UE) 2024/3144 DELLA COMMISSIONE

del 18 dicembre 2024

che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione

(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) Il regolamento di esecuzione (UE) 2024/482 si basa su norme internazionali consolidate, vale a dire i criteri comuni e la metodologia comune di valutazione mantenuti in essere dall'Organizzazione internazionale per la normazione (ISO) e dalla Commissione elettrotecnica internazionale (IEC). Il regolamento di esecuzione (UE) 2024/482 fa riferimento alle norme ISO/IEC, ma non specifica la versione applicabile di tali norme. È pertanto opportuno specificare quale versione delle norme si applica ai certificati rilasciati nell'ambito dell'EUCC.

(3) Le organizzazioni governative che hanno contribuito allo sviluppo dei criteri comuni e della metodologia comune di valutazione attraverso l'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security» (CCRA) sono contitolari, insieme all'ISO/IEC, dei relativi diritti d'autore. Tali organizzazioni governative conservano il diritto di utilizzarli. In considerazione dell'importanza di tali documenti derivanti dal CCRA, questi dovrebbero anche costituire la base per la certificazione nell'ambito dell'EUCC.

(4) Le norme dei criteri comuni e della metodologia comune di valutazione sono soggette alle interpretazioni fornite dal CCRA che ne facilitano l'attuazione e che possono essere prese in considerazione dalle strutture di valutazione della sicurezza delle tecnologie dell'informazione (*Information Technology Security Evaluation Facilities* – ITSEF) e dagli organismi di certificazione.

(5) Le norme internazionali per quanto riguarda i criteri comuni potrebbero essere soggette ad aggiornamenti. Al fine di garantire una transizione ordinata e tempestiva, è opportuno definire norme transitorie per concedere ai fornitori, alle ITSEF, agli organismi di certificazione e ad altri attori pertinenti il tempo sufficiente per gli adeguamenti necessari. Tali norme transitorie dovrebbero allinearsi in misura adeguata alle pratiche globali, come quelle stabilite dal CCRA.

([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).

(6) Il regolamento di esecuzione (UE) 2024/482 non specifica fino a quando la certificazione di un prodotto TIC possa basarsi sulle versioni precedenti delle norme dei criteri comuni e della metodologia comune di valutazione. I settori tecnici e i profili di protezione di cui agli allegati I, II e III di tale regolamento di esecuzione si basano sulle versioni precedenti delle norme ISO/IEC 15408 e 18045. Il regolamento di esecuzione (UE) 2024/482 dovrebbe pertanto specificare in quali circostanze si applica ancora la versione precedente dei criteri comuni e della metodologia comune di valutazione e in che modo si svolgerà la transizione verso l'ultima versione delle norme internazionali.

(7) Durante il periodo di transizione la priorità dei portatori di interessi dovrebbe essere l'aggiornamento dei settori tecnici e dei profili di protezione pertinenti. Il regolamento di esecuzione (UE) 2024/482 dovrebbe prevedere che i traguardi di sicurezza basati su una versione precedente delle norme siano accettati fino al 31 dicembre 2027 in linea con la politica di transizione adottata dal CCRA. Occorre tuttavia osservare che la politica di transizione del CCRA riguarda le valutazioni iniziali dei prodotti e dei profili di protezione a partire da non oltre il 30 giugno 2024, data in cui l'EUCC non era ancora applicabile. Conformemente alla politica di transizione del CCRA, il regolamento di esecuzione (UE) 2024/482 dovrebbe inoltre prevedere che i traguardi di sicurezza conformi a tale regolamento di esecuzione che dichiarino la conformità ai profili di protezione basati su una versione precedente delle norme siano accettati fino al 31 dicembre 2027. Quando è rilasciato un nuovo certificato a norma del regolamento di esecuzione (UE) 2024/482 nel contesto di un processo di riesame di un certificato nazionale avviato entro due anni dal certificato iniziale, dovrebbe inoltre essere possibile utilizzare una versione precedente delle norme. Ciò non riguarderebbe un processo di riesame che non richieda il rilascio di un nuovo certificato a norma del regolamento di esecuzione (UE) 2024/482 e in cui il certificato rimanga valido.

(8) Al fine di garantire una transizione ordinata verso l'ultima versione delle norme, il regolamento di esecuzione (UE) 2024/482 dovrebbe prevedere norme transitorie specifiche e continuare a consentire il rilascio di certificati a norma di tale regolamento di esecuzione che dichiarino la conformità ai profili di protezione basati su versioni precedenti delle norme pubblicate dal CCRA qualora l'uso di tali profili di protezione sia richiesto dal diritto dell'Unione. Gli atti in questione sono il regolamento di esecuzione (UE) 2016/799 della Commissione ([3]), il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([4]) e la decisione di esecuzione (UE) 2016/650 della Commissione ([5]).

(9) 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. Non sono tuttavia precisate le versioni dei documenti. È pertanto opportuno precisare quale versione dei documenti si applica ai certificati rilasciati nell'ambito dell'EUCC. Tali versioni si basano su documenti approvati dal gruppo europeo per la certificazione della cibersicurezza (*European Cybersecurity Certification Group* – ECCG) e sono state soggette a un ulteriore riesame ai fini della loro inclusione nell'EUCC. L'allegato I dovrebbe inoltre essere modificato per includere documenti sullo stato dell'arte aggiornati e nuovi, previa approvazione da parte dell'ECCG, garantendo in tal modo un accreditamento uniforme degli organismi di valutazione della conformità nell'ambito dell'EUCC. I requisiti per l'accreditamento relativi all'accreditamento delle ITSEF dovrebbero essere aggiornati per chiarire l'applicazione dei criteri di indipendenza e imparzialità e dovrebbe essere adottato un nuovo documento sullo stato dell'arte per l'accreditamento degli organismi di certificazione.

(10) I documenti sullo stato dell'arte potrebbero essere aggiunti all'EUCC o potrebbero essere soggetti ad aggiornamenti nel contesto delle attività per il suo mantenimento. Per i documenti sullo stato dell'arte nuovi o aggiornati potrebbe essere necessario stabilire norme transitorie adeguate per consentire ai fornitori, alle ITSEF, agli organismi di certificazione e ad altri portatori di interessi di effettuare i necessari adeguamenti. Per l'aggiornamento del documento sullo stato dell'arte relativo all'accreditamento delle ITSEF, il documento aggiornato dovrebbe applicarsi agli accreditamenti rilasciati prima dell'8 luglio 2025 solo quando sono riesaminati, ad esempio nel contesto di una procedura di valutazione o di nuova valutazione. Il documento aggiornato dovrebbe inoltre applicarsi a tutti gli accreditamenti per le ITSEF rilasciati dopo l'8 luglio 2025.

([3]) 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 recante le prescrizioni per la costruzione, il collaudo, il montaggio, il funzionamento e la riparazione dei tachigrafi e dei loro componenti (GU L 139 del 26.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (GU L 109 del 26.4.2016, pag. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Ulteriori rettifiche degli articoli 5, 8, 16, 29 e 44 e dell'allegato IV del regolamento di esecuzione (UE) 2024/482 contribuiscono a garantire una formulazione uniforme e una chiara interpretazione giuridica.

(12) Le norme per le notifiche degli organismi di valutazione della conformità dovrebbero essere stabilite orizzontalmente per tutti i sistemi nell'ambito del quadro europeo di certificazione della cibersicurezza. Il regolamento di esecuzione (UE) 2024/3143 della Commissione ([6]) riguarda tali norme per le notifiche. Gli articoli 23 e 24 del regolamento di esecuzione (UE) 2024/482 dovrebbero pertanto essere soppressi a decorrere dalla data di applicazione del regolamento di esecuzione (UE) 2024/3143.

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

(14) 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, i punti 1 e 2 sono sostituiti dai seguenti:

«1) «criteri comuni»: i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione quali definiti nelle norme ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 o ISO/IEC 15408-5:2022, o quali definiti nella norma «Common Criteria for Information Technology Security Evaluation», versione CC:2022, parti da 1 a 5, pubblicata dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security»;

2) «metodologia comune di valutazione»: la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione quale definita nella norma ISO/IEC 18045:2022, o nella norma «Common Methodology for Information Technology Security Evaluation», versione CEM:2022, pubblicata dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security";»;

2) l'articolo 3 è sostituito dal seguente:

«*Articolo 3*

Norme di valutazione

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

a) i criteri comuni;

b) la metodologia comune di valutazione.

2. Fino al 31 dicembre 2027 può essere rilasciato nell'ambito del sistema EUCC un certificato che applica una delle norme seguenti:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 o ISO/IEC 15408-3:2008;

b) «Common Criteria for Information Technology Security Evaluation», versione 3.1, revisione 5, pubblicata dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security»;

([6]) Regolamento di esecuzione (UE) 2024/3143 della Commissione, del 18 dicembre 2024, che stabilisce le circostanze, i formati e le procedure per le notifiche a norma dell'articolo 61, paragrafo 5, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (GU L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008;

d) «Common Methodology for Information Technology Security Evaluation», revisione 5, versione 3.1, pubblicata dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security».

3. Fino al 31 dicembre 2027 può essere rilasciato nell'ambito del sistema EUCC un certificato che applica le norme di cui al paragrafo 1 e che dichiari la conformità a un profilo di protezione che ha applicato le norme di cui al paragrafo 2.

4. Può essere rilasciato nell'ambito del sistema EUCC anche un certificato che applica le norme di cui al paragrafo 1 e che dichiari la conformità a un profilo di protezione che ha applicato una delle due norme seguenti, a condizione che l'uso di tale profilo di protezione sia richiesto a norma del regolamento di esecuzione (UE) 2016/799 della Commissione (*), del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio (**) o della decisione di esecuzione (UE) 2016/650 della Commissione (***):

a) «Common Criteria for Information Technology Security Evaluation», versione 3.1, revisioni da 1 a 4, pubblicata dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security»;

b) «Common Methodology for Information Technology Security Evaluation», versione 3.1, revisioni da 1 a 4, pubblicata dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security».

_____

(*) 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 recante le prescrizioni per la costruzione, il collaudo, il montaggio, il funzionamento e la riparazione dei tachigrafi e dei loro componenti (GU L 139 del 26.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (GU L 109 del 26.4.2016, pag. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).»;

3) al capo IV è inserito il seguente articolo 20 *bis*:

«*Articolo 20* bis

Specificazione dei requisiti per l'accreditamento degli organismi di valutazione della conformità

L'accreditamento degli organismi di valutazione della conformità tiene conto della specificazione dei requisiti per l'accreditamento degli organismi di certificazione e delle ITSEF di cui ai documenti sullo stato dell'arte applicabili figuranti all'allegato I, punto 2.»;

4) gli articoli 23 e 24 sono soppressi;

5) all'articolo 48 è aggiunto il seguente paragrafo 4:

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

6) all'articolo 49 è aggiunto il seguente paragrafo 4:

«4. Nell'effettuare il riesame di cui al paragrafo 3 entro due anni dal rilascio del certificato iniziale e qualora tale riesame porti al rilascio di un nuovo certificato conformemente al presente regolamento, possono essere applicate le norme di cui all'articolo 3, paragrafo 2. La data di rilascio del certificato iniziale è intesa come la data di rilascio dell'ultimo certificato per un prodotto TIC o un profilo di protezione su cui si basa l'attuale certificazione.»;

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

8) l'allegato IV è modificato conformemente all'allegato II del presente regolamento.

Articolo 2

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

1) all'articolo 5, paragrafo 1, la lettera b) è sostituita dalla seguente:

«b) dichiarando la conformità a 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) l'articolo 8 è così rettificato:

a) il titolo è sostituito dal seguente:

«Informazioni necessarie per la certificazione e la valutazione»;

b) il paragrafo 1 è sostituito dal seguente:

«1. Il richiedente la certificazione nell'ambito dell'EUCC fornisce o mette altrimenti a disposizione dell'organismo di certificazione e dell'ITSEF tutte le informazioni necessarie per le attività di certificazione e valutazione.»;

3) l'articolo 16 è sostituito dal seguente:

«*Articolo 16*

Informazioni necessarie per la certificazione e la valutazione 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, in forma completa e corretta, necessarie per le attività di certificazione e valutazione. Si applicano, mutatis mutandis, le disposizioni dell'articolo 8, paragrafi 2, 3, 4 e 7.»;

4) all'articolo 17, il paragrafo 1 è soppresso;

5) all'articolo 29, il paragrafo 2 è sostituito dal seguente:

«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 dell'articolo 14 o dell'articolo 20.».

Articolo 3

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

L'articolo 1, paragrafo 4, si applica a decorrere dall'8 gennaio 2025.

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

Fatto a Bruxelles, il 18 dicembre 2024

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 1.1;
      3) "Application of Common Criteria to integrated circuits", versione 1.1;
      4) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices", versione 1.1;
      5) "Certification of 'open' smart card products", versione 1.1;
      6) "Composite product evaluation for smart cards and similar devices", versione 1.1;
      7) "Application of Attack Potential to Smartcards and Similar Devices", versione 1.2;
   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 1.1;
      3) "Application of Attack Potential to hardware devices with security boxes", versione 1.2.

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

Nell'allegato IV del regolamento di esecuzione (UE) 2024/482, alla sezione IV.3 i punti 5 e 6 sono sostituiti dai seguenti:

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

La relazione di manutenzione è inclusa come sottoinsieme della relazione sull'analisi dell'impatto e contiene le sezioni seguenti:

a) introduzione;

b) descrizione delle modifiche;

c) *developer evidence* interessata;

6. La relazione di manutenzione di cui al punto 5 è fornita all'ENISA per la pubblicazione sul sito web relativo alla certificazione della cibersicurezza.».