CIRCOLARE TECNICA

Prot. DC2025MGR052 **Milano**, 21-07-2025

A tutti gli Organismi di certificazione accreditati/accreditandi PRD
Alle Associazioni degli Organismi di valutazione della conformità
A tutti gli Ispettori/Esperti del Dipartimento DC

Loro sedi

OGGETTO: Circolare tecnica DC N° 32/2025 - Disposizioni in merito all'avvio dell'accreditamento, in ambito PRD, dello schema di certificazione EUCC a fronte del Regolamento di Esecuzione (UE) 2024/482

Premessa

Il quadro legislativo di riferimento per la sicurezza cibernetica si fonda sul Cybersecurity Act, ovvero il Regolamento UE 2019/881, che si affianca, ed è in parte complementare, alla prima normativa in materia di sicurezza cibernetica introdotta a livello dell'Unione, ossia la Direttiva NIS, n. 2016/1148. Il Regolamento nasce con un duplice obiettivo: da un lato rafforzare il ruolo di ENISA (Agenzia dell'Unione Europea per la Cybersecurity) e, dall'altro, creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali. Il Cybersecurity Act costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici e a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi ICT.

Un primo punto chiave del Cybersecurity Act riguarda il rafforzamento del ruolo di ENISA, cui viene garantito un mandato permanente, consentendo alla stessa di svolgere non solo compiti di consulenza tecnica, ma anche attività di supporto alla gestione operativa degli incidenti informatici accaduti Stati membri. Il secondo punto chiave riguarda l'introduzione di un sistema europeo di certificazione accreditata della sicurezza informatica dei prodotti e dei servizi ICT, al fine di facilitare la circolazione degli stessi all'interno dell'UE e di accrescere la fiducia dei consumatori nei medesimi.

A cascata, l'UE ha poi varato la Direttiva NIS 2, n. 2022/2555 in abrogazione della precedente NIS. La NIS 2 ha modernizzato il quadro giuridico esistente per tenere il passo con una maggiore digitalizzazione e un panorama in evoluzione delle minacce alla cibersicurezza. Ciò ha di fatto esteso l'ambito di applicazione delle norme in materia di cibersicurezza a nuovi settori ed entità; ne consegue un ulteriore miglioramento della resilienza e delle capacità di risposta agli incidenti di sicurezza informatica degli enti pubblici e privati, delle autorità competenti e dell'UE nel suo complesso.

In tale contesto, l'evoluzione normativa europea in materia di sicurezza informatica, ha portato alla definizione dello Schema europeo di certificazione della cybersicurezza basato sui Common Criteria (EUCC), dedicato alla certificazione di prodotti ICT (Tecnologie dell'Informazione e della Comunicazione) come prodotti e componenti hardware e software. L'implementazione di tale schema richiede che gli Organismi di Valutazione della Conformità (CAB) siano accreditati al fine di assicurare la fiducia nelle certificazioni di cybersicurezza rilasciate.

La presente circolare ha lo scopo di informare sull'avvio della procedura per l'accreditamento degli Organismi di Certificazione ai sensi della norma ISO/IEC 17065, specificamente per le attività previste dallo schema EUCC, e di illustrare i principali requisiti e riferimenti normativi applicabili

Quadro normativo di riferimento

L'accreditamento degli Organismi di Certificazione per lo schema EUCC si basa su un quadro normativo europeo e su standard internazionali riconosciuti. I principali riferimenti normativi applicabili sono i seguenti:

- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione (Cybersecurity Act). Tale regolamento stabilisce il quadro per i regimi europei di certificazione della cybersicurezza, compresi i requisiti generali per gli Organismi di Valutazione della Conformità;
- Regolamento di Esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, che stabilisce le norme per l'applicazione del Regolamento (UE) 2019/881 per quanto riguarda l'adozione dello schema europeo di certificazione della cibersicurezza basato sui Common Criteria (EUCC). Questo regolamento definisce lo schema EUCC e i requisiti specifici per la sua attuazione. Fanno parte integrante di questo regolamento i documenti citati in Allegato 1, "State-of-the-Art" (*c.d. SotA*) disponibili sul portale ENISA[1];
- 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;
- ISO/IEC 18045:2022 - Sicurezza delle informazioni, cibersicurezza e protezione della privacy - Criteri di valutazione per la sicurezza IT - Metodologia per la valutazione della sicurezza IT. Questa norma fornisce la metodologia per la valutazione della sicurezza IT, fondamentale per le attività degli Organismi nell'ambito EUCC;
- ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022, ISO/IEC 15408-5:2022 – Criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione. Queste norme forniscono criteri e metodologie per analizzare la sicurezza di un prodotto ICT.

[1] https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en#state-of-the-art-documents-for-eucc

Banca dati ACCREDIA delle certificazioni rilasciate

Come noto, gli OdC sono tenuti a trasmettere ad ACCREDIA-DC tramite il servizio web – SIAC i dati relativi ai soggetti in possesso di certificazioni da essi rilasciate, secondo le procedure definite da ACCREDIA-DC e i relativi Regolamenti (RG01 §1.10.7). Per tale schema, pertanto, sarà attivato specifico codice per il caricamento. L'NCCA è esonerata da tale obbligo, in quanto essa stessa renderà disponibile una banca dati sul portale di competenza.

Regole di Certificazione

Il Regolamento (UE) 2019/881 stabilisce che i prodotti ICT siano classificati in base al livello di affidabilità. Esso può essere di tre tipologie distinte:

a. Elevato;
b. Sostanziale;
c. Di base

Nello specifico lo schema di certificazione EUCC consente la certificazione dei prodotti ICT a un livello di affidabilità "Sostanziale" o "Elevato".

Nel caso specifico della certificazione di un prodotto TIC a livello di affidabilità "Elevato", il Regolamento (UE) 2019/881 stabilisce che la certificazione spetta esclusivamente alla NCCA (National Cybersecurity Certification Authority) - in Italia tale ruolo è ricoperto dall'Agenzia per la cybersicurezza nazionale (ACN) con D.Lgs. 123/2022 per tramite di OCSI, tuttavia, come indicato dallo stesso Cybersecurity Act, esistono due casi in cui tali certificati possono essere emessi anche da un Organismo di valutazione della conformità:

- a seguito di una delega generale all' OdC, da parte della NCCA, di rilasciare tali certificati;
- previa autorizzazione, da parte della NCCA, per ogni singolo certificato europeo di cibersicurezza rilasciato dall' OdC.

Tuttavia, le modalità operative della NCCA ai sensi dell'articolo 4 del D.Lgs. n. 123/2022 sono indicate nelle linee guida per l'EUCC adottate con Decreto del Direttore Generale di ACN del 3 febbraio 2025 le quali non prevedono i due casi di emissione di certificati di livello "Elevato" su "delega generale di ACN" o con "pre-approvazione di ACN".

Diversamente, nel caso di certificati con livello di affidabilità "Sostanziale", la valutazione della conformità può essere eseguita un Organismo accreditato da ente designato ex Reg. CE 765/2008.

Lo schema EUCC, consolidato con il Regolamento di Esecuzione (UE) 2024/482, prevede fondamentalmente la collaborazione di 2 soggetti distinti: i Laboratori accreditati a fronte della ISO/IEC 17025 (c.d. ITSEFs) e gli Organismi di certificazione accreditati a fronte della ISO/IEC 17065 (c.d. CBs).

Gli Organismi di Certificazione accreditati per lo schema EUCC sono, pertanto, responsabili di diverse attività cruciali nel processo di certificazione della cybersicurezza dei prodotti ICT. Tali attività, come definite dal Regolamento di Esecuzione (UE) 2024/482, includono:

1. la revisione dei risultati della valutazione e la verifica del rapporto tecnico di valutazione (ETR - Evaluation Technical Report) prodotto dagli ITSEF (laboratori di prova);
2. l'emissione, il rinnovo e il ritiro dei certificati EUCC;
3. le attività di monitoraggio successive alla certificazione;
4. le attività relative alla conformità e alla compliance;
5. le attività di gestione e divulgazione delle vulnerabilità.

Il loro ambito di certificazione copre prodotti ICT rientranti in specifiche categorie, quali Smartcard e dispositivi simili, dispositivi hardware con security boxes, prodotti software, dispositivi di rete, dispositivi crittografici, firewall etc. È, pertanto, necessario che gli Organismi di certificazione accreditati si avvalgano di laboratori di prova (ITSEF - Information Technology Security Evaluation Facility) a loro volta accreditati secondo la norma EN ISO/IEC 17025:2017 e che rispettino i requisiti del Regolamento di Esecuzione (UE) 2024/482 e del Regolamento (UE) 2019/881.

I CBs devono selezionare e approvare gli ITSEF con cui collaborano, stipulando contratti o accordi vincolanti che definiscano ruoli, responsabilità, gestione della riservatezza e prevenzione dei conflitti di interesse. L'OdC si assume la piena responsabilità per le attività di valutazione esternalizzate agli ITSEF. L'OdC deve mantenere un elenco degli ITSEF selezionati e approvati e disporre di un processo per valutare la loro continua conformità ai requisiti di accreditamento e contrattuali.

Regole di Accreditamento

Si applicano i requisiti della ISO/IEC 17065 unitamente alle prescrizioni aggiuntive previste nell'Allegato al Regolamento (UE) 2019/881 e ai requisiti specifici del Regolamento di Esecuzione (UE) 2024/482.

A	OdC già accreditato UNI CEI EN ISO/IEC 17065:2012	• Esame documentale di 1 g/u; • 1 (una) Verifica in accompagnamento simulata (ricostruzione del processo di valutazione) di durata 0,5 g/u volta ad approfondire le procedure e le registrazioni del CAB nelle erogazione del processo di certificazione.
B	OdC non ancora accreditato UNI UNI CEI EN ISO/IEC 17065:2012 ma accreditato per altri schemi di accreditamento (Livello 3)	• Esame documentale di 1 g/u; • Verifica ispettiva presso la sede dell'OdC della durata di 3 g/u; • 1 (una) Verifica in accompagnamento simulata (ricostruzione del processo di valutazione) di durata 0,5 g/u volta ad approfondire le procedure e le registrazioni del CAB nelle erogazione del processo di certificazione. L'attività può essere accorpata alla verifica in sede.

C	OdC non accreditato	• Esame documentale di 1 g/u da svolgersi, se possibile, in parte in modalità sincrona da remoto; • Verifica ispettiva presso la sede dell'OdC della durata di 4 g/u; • 1 (una) Verifica in accompagnamento simulata (ricostruzione del processo di valutazione) di durata 0,5 g/u volta ad approfondire le procedure e le registrazioni del CAB nelle erogazione del processo di certificazione. L'attività può essere accorpata alla verifica in sede.
Mantenimento dell'Accreditamento	Si ricorda che ACCREDIA-DC, in ogni caso, deve condurre annualmente una verifica presso la sede degli Organismi di certificazione per valutare la conformità alla ISO/IEC 17065. Per quanto attiene ai criteri di campionamento verticale, esso sarà perfezionato in sede ogni anno.	

Documentazione da presentare ad ACCREDIA-DC per l'esame documentale

Oltre a quanto elencato nella domanda di accreditamento DA-01 si richiede l'invio di:

a. liste di riscontro, template rapporto di certificazione, linea guida/istruzioni predisposte dall'OdC per la valutazione della conformità;
b. criteri di qualifica e curricula del personale addetto al riesame del contratto, dei valutatori e dei decision maker e relative schede di qualifica;
c. procedure applicabili al processo commerciale per la definizione degli impegni di valutazione, nonché le procedure per la gestione della pratica di certificazione.

L'occasione è gradita per porgere cordiali saluti.

Dott.ssa Mariagrazia Lanzanova

Vice Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 21/07/2025 17:10:51