Agenzia per la Cybersicurezza Nazionale

Attuazione nazionale del

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)

Decreto Direttoriale recante "Organizzazione e procedure per lo svolgimento dei compiti dell'agenzia quale autorità nazionale di certificazione della cybersicurezza ex art. 7, comma 1, lettera e), del decreto – legge 14 giugno 2021, e 4, comma 2, del d. lgs. 3 agosto 2022, n. 123" (*integrazione ex articolo 15 del decreto legislativo 3 agosto 2022, n. 123*)

Linea Guida NCCA N. 1

Attività di vigilanza nazionale e autorizzazione per il sistema EUCC

(art. 5 e art. 8 cc. 3 e 4 del d.lgs. 123/2022)

Versione 1.0

3 febbraio 2025

REGISTRO DELLE VERSIONI

L’elenco delle versioni sarà mantenuto aggiornato in modo da riportare le modifiche apportate al presente documento.

Versione	Autore	Modifiche	Data
1.0	ACN	Prima emissione	3 febbraio 2025

1. Indice

2. Acronimi

ACN	Agenzia per la Cybersicurezza Nazionale
CAB	Conformity Assessment Body (Organismo di valutazione della conformità)
CEI	Comitato Elettrotecnico Italiano
CSA	Cybersecurity Act
DLGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
ECCG	European Cybersecurity Certification Group
EUCC	European Cybersecurity Scheme on Common Criteria
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LG	Linea Guida
LVS	Laboratorio per la Valutazione della Sicurezza
NCCA	National Cybersecurity Certification Authority
OC	Organismo di Certificazione
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto Della Valutazione (TOE - Target of Evaluation)
PDV	Piano Di Valutazione
TIC	Tecnologia dell'Informazione e delle Comunicazioni (ICT - Information and Communication Technology)
UNI	Ente Nazionale Italiano di Unificazione

3. Scopo del documento

Il presente documento ha come scopo la definizione delle modalità operative in materia di attività di vigilanza nazionale e di autorizzazione dell'autorità nazionale di certificazione della cybersicurezza designata per l'Italia ai sensi dell'articolo 58, paragrafo 1, del regolamento europeo sulla cybersicurezza ([CSA]) nell'ambito del sistema europeo di certificazione della cybersicurezza basato sui Common Criteria ([EUCC]).

L'autorità di certificazione della cybersicurezza in Italia è l'Agenzia per la cybersicurezza nazionale[1] ([ACN]), nel seguito indicata anche con il termine «Agenzia».

All'Agenzia spetta il compito di monitorare e supervisionare i certificati di cybersicurezza EUCC emessi in Italia. Ha potere sanzionatorio[2] nei confronti dei soggetti che operano in contrasto con quanto previsto dal quadro europeo di certificazione della cybersicurezza. In tale ambito è necessario in particolare il coinvolgimento degli organismi di valutazione della conformità e dei Titolari dei certificati.

L'Agenzia coopera con l'Organismo nazionale di accreditamento (Accredia)[3], con le autorità nazionali di certificazione della cybersicurezza designate negli altri stati membri, con le autorità di vigilanza del mercato competenti.

L'Agenzia ha il compito di autorizzare gli organismi di valutazione della conformità (organismi di certificazione e ITSEF[4]) ad operare al *livello di garanzia elevato*[5] per l'EUCC. In Italia l'unico organismo di certificazione designato per l'emissione di certificati di livello elevato è l'OCSI ([OCSI]), organismo di certificazione dell'Agenzia[6]. Di conseguenza gli unici ITSEF che operano in valutazioni a livello di garanzia elevato sono gli ITSEF autorizzati dall'OCSI, denominati anche Laboratori per la Valutazione della Sicurezza (LVS).

L'Agenzia notifica[7] alla Commissione europea gli organismi di valutazione della conformità accreditati e autorizzati sul territorio nazionale.

[1] I compiti dell'autorità nazionale di certificazione della cybersicurezza in Italia sono assegnati all'Agenzia nazionale per la cybersicurezza (ACN) dall'articolo 7, comma 1, lettera e) del decreto-legge del 14 giugno 2021, n. 82 ([ACN]); la designazione dell'ACN quale autorità di certificazione della cybersicurezza è anche confermata dall'articolo 4, comma 1 del decreto legislativo 3 agosto 2022, n. 123 ([DLGS]).

[2] Articolo 10 del [DLGS].

[3] L'organismo nazionale di accreditamento autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'articolo 2, paragrafo 1, numero 11, del regolamento (CE) 765/2008 è Accredia. Tale organismo è designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99.

[4] L'ITSEF (Information Technology Security Evaluation Facility) è il termine utilizzato per riferirsi ai laboratori di prova che effettuano valutazioni Common Criteria.

[5] Articolo 60, par.3 del [CSA]; articoli 21-22 dell'[EUCC].

[6] Articolo 6, comma 1 del [DLGS].

[7] Articolo 61 dell'[EUCC].

La seguente linea guida definisce le **modalità operative per le attività di vigilanza nazionale[8] e di autorizzazione dell'OCSI[9] e degli LVS[10] a svolgere valutazioni e certificazioni al livello di garanzia elevato** nell'ambito delle nuove regole europee armonizzate del sistema europeo di certificazione della cybersicurezza EUCC attuato in Italia.

Si evidenzia che per gli eventuali aspetti non trattati dalla presente linea guida che dovessero rientrare nell'ambito della stessa, si applicano le disposizioni contenute nel regolamento di esecuzione [EUCC].

[8] Articolo 5 del [DLGS].
[9] Articolo 21 dell'[EUCC].
[10] Articolo 22 dell'[EUCC].

4. Introduzione

La presente Linea Guida NCCA N.1 tratta delle attività di vigilanza nazionale e autorizzazione dell'Agenzia per quanto concerne il sistema [EUCC]. In questa linea guida sono richiamate le principali attività svolte dall'Agenzia per il monitoraggio dei certificati e dei soggetti coinvolti nella loro emissione e successiva gestione.

In particolare, all'Agenzia spetta il compito di monitorare e supervisionare i certificati emessi in Italia dagli organismi di certificazione e detenuti dai rispettivi Titolari dei certificati per far rispettare le disposizioni del [CSA] e dell'[EUCC]. Nell'ambito dell'EUCC possono essere emessi certificati di cybersicurezza relativi a:

- prodotti TIC
- a profili di protezione

I profili di protezione dettagliano il processo di valutazione di prodotti TIC appartenenti a una specifica categoria sulla base di requisiti di sicurezza e di garanzia predefiniti per tale categoria[11].

L'Agenzia ha potere sanzionatorio[12] nei confronti dei soggetti coinvolti nel processo di certificazione e nella successiva gestione dei certificati, che includono in particolare gli organismi di valutazione della conformità (organismi di certificazione e ITSEF) e i Titolari dei certificati. In questa linea guida sono elencati i principali controlli per l'irrogazione delle sanzioni, non è tuttavia trattato il dettaglio del procedimento sanzionatorio.

All'Agenzia spetta autorizzare l'OCSI e gli LVS ad operare al *livello di garanzia elevato*[13]. In particolare, la procedura di autorizzazione degli LVS è trattata in questa linea guida allo scopo di informare i candidati LVS sulle modalità di presentazione della domanda e ottenimento dell'autorizzazione. Per le modalità di autorizzazione dell'OCSI, quale organismo di certificazione interno all'Agenzia, si rinvia all'articolo 21 dell'[EUCC].

All'Agenzia spetta notificare[14] alla Commissione europea gli organismi di valutazione della conformità accreditati e autorizzati sul territorio nazionale.

Nel seguito sono dettagliate le modalità operative dell'Agenzia per l'attuazione delle suddette funzioni ad esclusione dell'attività di irrogazione delle sanzioni per violazioni degli obblighi sanciti dal [CSA] e dall'[EUCC].

[11] Articolo 2, n. 5 dell'[EUCC].
[12] Articolo 10 del [DLGS].
[13] Articolo 60, par.3 del [CSA]; articoli 21-22 dell'[EUCC].
[14] Articolo 61 dell'[EUCC].

5. L'attività di vigilanza nazionale

L'Agenzia vigila in ambito nazionale[15] ai fini della corretta applicazione delle regole previste dal [CSA] e dall'[EUCC], cooperando con Accredia, con le autorità di vigilanza del mercato e con le autorità di certificazione della cybersicurezza degli altri Stati Membri.

Quanto agli aspetti di *vigilanza oggettiva*, l'Agenzia in particolare:

- monitora i certificati europei di cibersicurezza EUCC;
- in raccordo con l'OCSI sospende o revoca certificati di cybersicurezza di livello elevato;
- richiede misure correttive ai Titolari dei certificati in caso di non conformità rilevate con la possibilità di revoca o sospensione del certificato[16].

Quanto agli aspetti di *vigilanza soggettiva*, l'Agenzia:

- assiste e sostiene attivamente Accredia nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità (organismi di certificazione e ITSEF);
- monitora gli LVS e l'OCSI ai fini del mantenimento dell'autorizzazione per le attività di valutazione e l'emissione dei certificati EUCC di livello elevato[17];
- può eseguire indagini ed audit nei confronti degli organismi di valutazione della conformità, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei Titolari dei certificati europei di cybersicurezza;
- irroga sanzioni pecuniarie ed accessorie agli organismi di valutazione della conformità, ai Titolari dei certificati, per violazioni alle disposizioni dell'[EUCC] o del [CSA].

5.1. Attività di monitoraggio dei certificati EUCC da parte dell'Agenzia

Fatto salvo l'articolo 58, paragrafo 7, del regolamento [CSA], l'Agenzia[18] controlla:

- il rispetto, da parte degli organismi di certificazione e degli ITSEF, degli obblighi a essi incombenti a norma del presente regolamento e del regolamento (UE) 2019/881;
- il rispetto, da parte dei Titolari dei certificati EUCC, degli obblighi a essi incombenti a norma dell'[EUCC] e del [CSA] con particolar riguardo:

[15] Articolo 58, paragrafo 7.
[16] Articoli 28, 29 e 30 dell'[EUCC].
[17] Nell'[EUCC] si classificano come certificati di livelli elevato i certificati che contengono il componente di garanzia AVA_VAN.3, AVA_VAN.4 e AVA_VAN.5.
[18] Articolo 25 dell'[EUCC].

- al monitoraggio, da parte del Titolare del certificato, della conformità dei prodotti TIC certificati ai loro requisiti di sicurezza, mediante il monitoraggio delle relative vulnerabilità e del livello di affidabilità espresso nel certificato EUCC[19];
- all'utilizzo corretto del marchio e dell'etichetta EUCC[20];
- agli obblighi informativi riguardo ai certificati detenuti[21];

- il rispetto, da parte dei prodotti TIC certificati, dei requisiti stabiliti nell'EUCC;
- il livello di affidabilità espresso nel certificato EUCC in relazione all'evoluzione del panorama delle minacce.

L'Agenzia svolge le sue attività di monitoraggio in particolare sulla base:

- delle informazioni provenienti dagli organismi di certificazione, dagli organismi nazionali di accreditamento e dalle autorità di vigilanza del mercato competenti;
- delle informazioni derivanti da audit e indagini propri o di altre autorità;
- delle informazioni raccolte sulla base di un campione di certificati controllati;
- dei reclami ricevuti.

L'Agenzia, in collaborazione con le altre autorità di vigilanza del mercato, adotta i criteri di campionamento dei certificati EUCC emessi sul territorio nazionale previsti da [EUCC], in base a una valutazione dei rischi. Su richiesta e per conto dell'Agenzia, gli organismi di certificazione e, se necessario, gli ITSEF assistono tale autorità nel monitoraggio della conformità[22].

L'Agenzia seleziona il campione di prodotti TIC certificati da controllare utilizzando criteri oggettivi tra cui:

- la categoria del prodotto TIC;
- il livello di affidabilità del prodotto TIC;
- il Titolare di un certificato;
- l'organismo di certificazione e, se del caso, l'ITSEF a cui sono state esternalizzate le attività;
- qualsiasi altra informazione portata all'attenzione dell'autorità.

L'Agenzia informa i Titolari dei certificati EUCC in merito ai prodotti TIC selezionati e ai criteri di selezione.

[19] Articolo 27 dell'[EUCC].
[20] Articolo 11 dell'[EUCC].
[21] Articolo 41 dell'[EUCC].
[22] Articolo 25, par. 3 dell'[EUCC].

Su richiesta dell'Agenzia, e con l'assistenza del rispettivo 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 del [CSA], e informa l'Agenzia in merito ai risultati.

Qualora abbia motivi sufficienti per ritenere che un prodotto TIC certificato non sia più conforme al regolamento [CSA] o al regolamento di attuazione [EUCC], l'Agenzia può svolgere indagini o avvalersi di qualsiasi altro potere di monitoraggio di cui all'articolo 58, paragrafo 8 del [CSA].

L'Agenzia informa l'organismo di certificazione e l'ITSEF in questione delle indagini in corso relative ai prodotti TIC selezionati. Se rileva che un'indagine in corso riguarda prodotti TIC certificati da organismi di certificazione stabiliti in altri Stati membri, l'Agenzia, se del caso, ne informa le autorità nazionali di certificazione della cibersicurezza degli Stati membri interessati ai fini della collaborazione alle indagini. L'Agenzia informa inoltre l'ECCG[23] in merito alle indagini transfrontaliere e ai relativi risultati.

5.2. Soggetti vigilati dall'Agenzia

I soggetti vigilati dall'Agenzia sono tutti gli attori coinvolti nel processo di certificazione e successiva gestione dei certificati di prodotti TIC e profili di protezione.

In particolare, durante il processo di certificazione si individuano i seguenti attori:

- Il *Committente* (o *Richiedente della certificazione*) – richiede la certificazione di un prodotto TIC o profilo di protezione ad un organismo di certificazione, con il supporto di un ITSEF. Collabora nel processo di certificazione fornendo tutte le informazioni necessarie e corrette per il processo certificazione.
- Il *laboratorio di prova* (*ITSEF)*, sulla base delle evidenze fornite dal Committente, richiedendo eventuali chiarimenti e integrazioni, esegue le attività di valutazione e redige i rapporti di valutazione per attestare il superamento delle verifiche del prodotto in valutazione.
- L'*organismo di certificazione* – supervisiona il processo di valutazione ed effettua il riesame dei rapporti di valutazione verificando in particolare la consistenza delle evidenze esaminate dall'ITSEF ed i rapporti di valutazione ricevuti dall'ITSEF per attestare, con l'emissione del certificato, il raggiungimento del livello di garanzia di valutazione da parte del prodotto TIC o del profilo di protezione valutato.
- Lo *Sviluppatore* (o *Fornitore*) – il soggetto che sviluppa o fornisce il prodotto da valutare, può coincidere con il Committente o può essere un soggetto diverso. Se è un soggetto diverso dal Committente, il Committente deve stabilire un accordo

[23] ECCG (European Cybersecurity Certification Group) ai sensi dell'articolo 62 del [CSA].

di cooperazione che permetta di fornire tutti gli elementi necessari per la conduzione della valutazione (specifiche dettagliate, accesso al sito di sviluppo, campioni dell'oggetto della valutazione, guide utente e guide operative).

I suddetti attori cooperano nel processo di certificazione garantendo l'emissione di certificati conformi, verificando la presenza di vulnerabilità in base allo standard Common Criteria [CC 1,2,3,4,5] e relativa metodologia di valutazione [CEM].

Viceversa, una volta emesso il certificato, si individuano i seguenti attori nella gestione del certificato:

- Il *Titolare del certificato* – il soggetto che diviene responsabile della gestione del certificato successivamente all'emissione; ha in particolare l'obbligo di monitorare e gestire le eventuali non conformità dei certificati EUCC e le eventuali vulnerabilità dei prodotti TIC e dei profili di protezione certificati, mettere a disposizione e pubblicare la documentazione e le informazioni relative ai prodotti certificati, utilizzare il marchio e le etichette EUCC in modo appropriato.
- L'*organismo di certificazione* – monitora e gestisce le eventuali non conformità dei certificati EUCC e le eventuali vulnerabilità dei prodotti TIC e dei profili di protezione certificati, eventualmente riesaminando i prodotti TIC o profili di protezione certificati e sospendendo o revocando i certificati EUCC.
- L'*ITSEF* – partecipa al riesame dei certificati ove richiesto dall'organismo di certificazione, dal Titolare del certificato o dall'Agenzia ripetendo una o più attività di valutazione.
- Lo *Sviluppatore* – normalmente coincide con il Titolare del certificato; se diverso deve essere coinvolto nelle attività di monitoraggio e riesame dei certificati su richiesta dal Titolare. Tale coinvolgimento richiede normalmente un contratto tra Titolare e Sviluppatore se i due ruoli non sono svolti dallo stesso soggetto. È responsabilità del Titolare assicurare il necessario supporto dallo Sviluppatore nelle attività di revisione del certificato e di analisi di vulnerabilità.

5.3.Supervisione dell'emissione dei certificati EUCC sul territorio nazionale

L'Agenzia supervisiona l'emissione dei certificati sul territorio nazionale.

I certificati EUCC per i prodotti TIC sono emessi sul territorio nazionale dai seguenti soggetti:

- per il livello di garanzia elevato dall'OCSI[24],

[24] Articolo 56, par. 6 del [CSA].

- per il livello di garanzia sostanziale da un qualsiasi organismo di certificazione accreditato[25].

I certificati EUCC per profili di protezione sono emessi sul territorio nazionale dai seguenti soggetti:

- per il livello di garanzia elevato dall'OCSI[26],
- per il livello di garanzia sostanziale dall'OCSI o da un qualsiasi organismo di certificazione accreditato pubblico[27].

La pubblicazione sul sito web dell'ENISA[28] dei certificati emessi sul territorio nazionale è riservata all'Agenzia. Le modalità di pubblicazione sono concordate tra l'Agenzia e l'ENISA. Solo i certificati emessi sul territorio nazionale con le suddette modalità sono pubblicati dall'Agenzia sul sito web di ENISA.

5.4. Controlli dell'Agenzia per l'irrogazione di sanzioni pecuniarie e accessorie

In accordo a quanto previsto dall'articolo 5 del [DLGS], relativamente ai compiti di cui alla sezione 5.1, l'Agenzia esegue attività di vigilanza circa le seguenti violazioni degli obblighi stabiliti dal [CSA] e dall'[EUCC] per l'irrogazione di sanzioni pecuniarie e accessorie applicabili al sistema EUCC[29]:

Vigilanza sui Titolari dei certificati, Committenti e Sviluppatori:

Sono irrogate sanzioni pecuniarie ai sensi dell'articolo 10 del [DLGS] a seguito delle seguenti violazioni:

- la mancata notifica e trattamento di eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza di prodotti TIC o profili di protezione certificati, non riscontrate durante il processo di valutazione (art.10 comma 8 del [DLGS])[30];
- la mancata messa a disposizione della documentazione tecnica relativa ad un certificato EUCC (Art.10 comma 9 del [DLGS])[31];
- la mancata messa a disposizione o pubblicazione di tutte le informazioni previste per il certificato EUCC o il mancato rispetto del formato o delle procedure per l'aggiornamento delle informazioni relative al certificato EUCC o la pubblicazione di

[25] Articolo 56, par. 4 del [CSA].
[26] Articolo 56, par. 6 del [CSA].
[27] Articolo 17, par. 4, lett. b) dell'[EUCC].
[28] Articolo 42 dell'[EUCC].
[29] Articolo 10, paragrafo 1 del [DLGS].
[30] CAPO VI dell'[EUCC].
[31] Articolo 41 dell'[EUCC].

informazioni non corrette riguardo al certificato EUCC (Art.10 comma 9 del [DLGS])[32];

- l'eventuale fornitura eseguita scientemente nell'ambito dello svolgimento dell'attività di valutazione e di rilascio dei certificati, di informazioni o documentazione falsi, o l'omissione di informazioni necessarie per espletare la certificazione[33] o durante l'attività di vigilanza[34] (Art.10 comma 12 del [DLGS]);
- la violazione delle condizioni di utilizzo del marchio o dell'etichetta EUCC (Art.10 comma 13 del [DLGS])[35];

Vigilanza sugli organismi di valutazione della conformità (CAB)[36]:

Sono irrogate sanzioni pecuniarie ai sensi dell'articolo 10 del [DLGS] a seguito delle seguenti violazioni:

- l'emissione di certificati EUCC non conformi e l'omessa revoca su richiesta dell'Agenzia (Art.10 comma 2 del [DLGS]) [37];
- la mancata comunicazione e trattamento di eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza di prodotti TIC o profili di protezione certificati, non riscontrate durante il processo di valutazione (Art.10 comma 8 del [DLGS])[38];
- il mancato adempimento degli obblighi di divulgazione dell'emissione, modifica o revoca dei certificati EUCC (Art.10 comma 10 del [DLGS])[39];
- la mancata specifica da parte dell'LVS autorizzato dall'Agenzia, nella procedura per i reclami, dell'inoltro degli stessi per conoscenza anche all'Agenzia (art.10 comma 10 del [DLGS]);
- l'esercizio, in qualità di organismo autorizzato, di un organismo di valutazione della conformità senza disporre dell'autorizzazione (art.10 comma 11 del [DLGS]);
- l'eventuale fornitura durante le verifiche di vigilanza di dati, informazioni o documentazione falsi da parte del soggetto sottoposto alle stesse verifiche di vigilanza (art.10 comma 12 del [DLGS]);
- l'ottemperanza agli obblighi di conservazione dei registri di cui all'art.54 paragrafo 1 lettera n) del [CSA] (art.10 comma 14 del [DLGS])[40]

[32] Articolo 42 dell'[EUCC].
[33] Articolo 56, paragrafo 7 del [CSA].
[34] Articolo 5, comma 8 del [DLGS] e sezione .
[35] Articolo 11 e allegato IX dell'[EUCC].
[36] Dalle sanzioni pecuniarie è da escludere l'OCSI in quanto parte della Agenzia che irroga le sanzioni pecuniarie.
[37] CAPO V dell'[EUCC].
[38] CAPO VI dell'[EUCC].
[39] Articolo 42 dell'[EUCC].
[40] Articolo 40 dell'[EUCC].

Inoltre, l'eventuale reiterazione di una o più delle precedenti violazioni in un quinquennio o biennio comporta la sospensione per sei mesi o revoca dell'autorizzazione (art.10 comma 19 del [DLGS]).

5.5. Conseguenze delle non conformità da parte di un CAB

Fatte salve le sanzioni irrogate dall'Agenzia ai sensi dell'articolo 10 del [DLGS] in esito ai controlli di cui alla sezione 5.2, in caso di mancato rispetto dei propri obblighi da parte di un organismo di certificazione o da parte di un ITSEF, qualora sia rilevata una non conformità, l'Agenzia, senza indebito ritardo:

- identifica con il sostegno dell'ITSEF in questione i certificati EUCC potenzialmente interessati;
- 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 altro ITSEF accreditato e, se del caso, autorizzata che possa trovarsi in una posizione tecnica migliore per sostenere tale identificazione;
- analizza gli impatti della non conformità;
- informa il Titolare del certificato EUCC interessato dalla non conformità.

L'organismo di certificazione, in relazione a ciascun certificato EUCC interessato da una non conformità rilevata, adotta una delle decisioni indicate di seguito:

- mantenere il certificato EUCC inalterato;
- revocare il certificato EUCC[41] e, nei casi previsti[42], rilasciare un nuovo certificato EUCC.

L'Agenzia:

- segnala, se necessario, la non conformità dell'organismo di certificazione o del relativo ITSEF all'organismo nazionale di accreditamento;
- valuta, se del caso, il potenziale impatto sull'autorizzazione.

[41] In conformità dell'articolo 14 o dell'articolo 20 dell'[EUCC].
[42] Come specificato dagli articoli 13 e 19 dell'[EUCC].

5.6. Obbligo di cooperazione dei soggetti vigilati

Gli organismi della valutazione della conformità e i Titolari dei certificati EUCC hanno l'obbligo di cooperare[43] con l'Agenzia nell'attività di verifica di certificati da essi emessi o di cui risultano titolari.

Tali soggetti mettono a disposizione su richiesta dell'Agenzia i documenti di valutazione necessari per dimostrare la conformità dei certificati e le dichiarazioni oggetto di verifica da parte dell'Agenzia, insieme agli strumenti di valutazione forniti dallo Sviluppatore durante l'attività di valutazione come descritto nei rapporti di valutazione.

5.7. Oneri per la vigilanza

Gli oneri[44] per i controlli effettuati dall'Agenzia e relativi, in particolare, all'impiego del personale in forza all'Agenzia, della strumentazione utilizzata nelle prove e dei materiali di consumo e per le missioni e spese generali, sono a carico dell'organismo di valutazione della conformità o del Titolare del certificato sottoposto all'attività di vigilanza. Nel caso in cui l'attività di vigilanza includa ulteriori spese, tra cui l'utilizzo di laboratori di prova esterni[45] ed eventuali spese di trasporto per prodotti da sottoporre a verifica, le ulteriori spese sono ugualmente a carico del soggetto sottoposto all'attività di vigilanza.

[43] Articolo 5, comma 8 del [DLGS].
[44] Articolo 5, comma 9 del [DLGS].
[45] Articolo 31, paragrafo 1, lettera b) dell'[EUCC].

6. Autorizzazione degli LVS per il sistema EUCC

L'OCSI è l'unico organismo di certificazione emittente certificati EUCC di livello elevato: tra tutti i laboratori di prova accreditati dall'organismo nazionale di accreditamento[46], solo per gli LVS, in qualità di laboratori di prova che operano in valutazioni condotte da OCSI, è richiesta l'autorizzazione da parte dell'Agenzia.

Un LVS è autorizzato dall'Agenzia 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 [CSA] per quanto riguarda l'accreditamento degli organismi di valutazione della conformità, dimostra di rispettare tutte le condizioni seguenti[47]:

- 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;
- per quanto riguarda i domini tecnici e i profili di protezione riferibili al prodotto TIC da certificare:
    - possesso delle competenze per svolgere le attività di valutazione specifiche necessarie a determinare metodicamente la resistenza di un ODV agli attacchi commessi da soggetti qualificati nel suo ambiente operativo, ipotizzando un potenziale di attacco «moderato»[48] o «elevato»[49];
    - possesso delle competenze tecniche specificate nei documenti sullo stato dell'arte di cui all'Allegato I dell'[EUCC];
- possesso delle competenze richieste e adozione di misure tecniche e operative adeguate a proteggere efficacemente le informazioni riservate e sensibili per il livello di affidabilità «elevato», oltre al soddisfacimento dei requisiti di cui all'articolo 43 del regolamento [EUCC].

L'Agenzia valuta se l'LVS soddisfa tutti i requisiti tramite interviste strutturate e un riesame di almeno una valutazione pilota effettuata dall'LVS in conformità all'[EUCC]. Nella sua valutazione, l'Agenzia può riutilizzare elementi di prova adeguati provenienti da una precedente autorizzazione o da attività analoghe concesse a norma:

- del regolamento [EUCC]

[46] Per gli LVS stabiliti in Italia l'organismo nazionale di accreditamento è l'Ente Nazionale di Accreditamento (Accredia in Italia), per gli LVS stabiliti all'estero nell'Unione Europea, l'organismo nazionale di accreditamento è l'organismo designato nello Stato Membro.
[47] Articolo 22 dell'[EUCC].
[48] Corrispondente al livello AVA_VAN.4
[49] Corrispondente al livello AVA_VAN.5

- di un altro sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del [CSA];
- dello schema nazionale di certificazione della cybersicurezza ai sensi del decreto [OCSI].

L'Agenzia elabora un rapporto di autorizzazione soggetto a valutazione *inter pares* in conformità dell'articolo 59, paragrafo 3, lettera d), del [CSA].

L'Agenzia 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 dell'LVS. Tale autorizzazione può essere rinnovata su richiesta dell'LVS. Per il rinnovo dell'autorizzazione non sono richieste valutazioni pilota.

6.1. Cooperazione tra Accreditamento e Autorizzazione

L'accreditamento rilasciato dall'organismo nazionale di accreditamento costituisce la base per l'autorizzazione di LVS che intendono operare valutazioni nel sistema EUCC con livello di garanzia elevato.

Per accelerare l'iter di autorizzazione l'LVS può richiedere l'avvio della procedura per ottenere l'autorizzazione prima della conclusione del processo di accreditamento. In tal caso l'organismo di accreditamento (italiano o estero) e l'Agenzia restano responsabili ciascuno per la procedura di rispettiva competenza.

L'organismo di accreditamento e l'Agenzia collaborano, oltre che in fase di primo accreditamento e prima autorizzazione, anche in caso di rinnovo di accreditamento/autorizzazione e di non conformità potenziali emerse durante il periodo di validità dell'accreditamento/autorizzazione.

Infatti, se durante il periodo di validità dell'accreditamento di un LVS, l'organismo di accreditamento, a seguito del rilevamento di una non conformità, opera una decisione di riduzione della validità o di sospensione dell'accreditamento, tale decisione ha un impatto sull'autorizzazione. L'organismo di accreditamento informa quindi l'Agenzia in merito all'avvio e il progresso della procedura di non conformità e della previsione circa eventuali modifiche alla validità di accreditamento.

6.2.Ambito dell'autorizzazione

Un LVS può essere autorizzato ad eseguire la valutazione a livello di garanzia elevato delle seguenti categorie di prodotti:

- prodotti che ricadono nelle categorie segnalate dall'Agenzia in Allegato A (sez.11) per valutazioni che includono componenti di garanzia AVA_VAN.3;

- prodotti che dichiarano conformità a profili di protezione (PP) certificati EUCC[50] ed inseriti nella lista di PP "*state of the art*" definita in Annesso II ad [EUCC], che includono componenti di garanzia della classe AVA fino ad AVA_VAN.5;
- prodotti che ricadono nell'ambito dei domini tecnici *Smart Cart and similar Devices* e "*Hardware Devices with Security Boxes"*, o in altri domini tecnici istituiti in futuro, con richieste di valutazione che includono componenti di garanzia della classe AVA fino ad AVA_VAN.5;

L'LVS può richiedere di estendere l'ambito di autorizzazione.

6.3. Impiego di esperti esterni all'LVS

Nello svolgimento delle attività di valutazione per un prodotto TIC, l'LVS potrebbe avere la necessità di avvalersi delle prestazioni di esperti su determinati domini di sicurezza.

Nei casi in cui l'LVS si avvalga di tali terze parti anch'esse sono soggette alla procedura di autorizzazione nello stesso ambito dell'LVS e con le stesse modalità utilizzate per l'autorizzazione dell'LVS.

[50] A meno di eccezioni previste dagli aggiornamenti del Regolamento EUCC.

7. La procedura di autorizzazione di un LVS

L'autorizzazione di un LVS si svolge in quattro fasi:

1. richiesta;
2. istruttoria;
3. verifica;
4. rilascio.

Le verifiche previste nella fase tre includono verifiche sulla documentazione descritte nelle sezioni successive e l'esecuzione monitorata dall'Agenzia di una valutazione pilota.

Nelle sezioni dalla 7.1 alla 7.4 viene fornito uno schema riassuntivo di tutte le fasi che caratterizzano la procedura di abilitazione di un LVS.

7.1. Richiesta (Fase 1)

L'LVS interessato all'autorizzazione deve presentare formale richiesta all'Agenzia, utilizzando il modulo predisposto disponibile sul sito web dell'Agenzia.

Nel modulo, compilato nella sua interezza, devono essere obbligatoriamente contenute le seguenti informazioni, che devono coincidere con quelle fornite in fase di accreditamento:

1. nome e ragione sociale del laboratorio candidato;
2. indirizzo della sede del laboratorio candidato;
3. ambito dell'autorizzazione richiesta[51];
4. nominativo del personale coinvolto operativamente nell'attività di laboratorio;
5. dichiarazione di avvenuto accreditamento [17025] da parte dell'Ente Nazionale di Accreditamento (Accredia) o da altro organismo nazionale di accreditamento estero o dichiarazione sul processo di accreditamento in corso;
6. eventuale lista di tutti gli organismi di certificazione cui l'LVS fornisce il servizio di valutazione al di fuori del territorio nazionale italiano;
7. firma del legale Rappresentante per il laboratorio;
8. firma del Responsabile del laboratorio.

[51] L'ambito può includere una o più delle categorie previste in Allegato A, un profilo di protezione tra quelli presenti nell'Annesso di [EUCC] o in alternativa il dominio tecnico per cui si richiede l'autorizzazione ad operare.

7.2. Istruttoria (Fase 2)

Sulla base delle informazioni presenti nella richiesta di autorizzazione, l'Agenzia emette un preventivo di spesa tariffario per l'autorizzazione dell'LVS, calcolato in base al [DM][52].

Il richiedente, ricevuto il preventivo, per avviare la fase delle verifiche di competenza e tecnico organizzative dell'LVS, deve presentare la seguente documentazione[53]:

1. attestazione di pagamento dell'acconto specificato nel preventivo;
2. certificato di accreditamento secondo la norma [17025] per l'EUCC rilasciato all'LVS da parte dell'Organismo nazionale di accreditamento (se già conseguito) o di altro Organismo di accreditamento europeo;
3. curricula vitae e le schede del personale e dei valutatori dell'LVS registrati nel sistema di gestione per la qualità;
4. il rapporto di accreditamento da cui risultano le prove verificate con riferimento all'Allegato A2 del documento [SOA-LB][54];
5. la documentazione aggiuntiva, necessaria per le verifiche di competenza e per le verifiche delle misure tecnico-organizzative descritte in [ENISA] sez. 6.2.1 pag.15, capoverso 42. Per quanto riguarda gli aspetti relativi alla competenza, la documentazione deve includere una descrizione dei metodi di valutazione e degli strumenti adottati dall'LVS;
6. il prodotto TIC oggetto della valutazione pilota e il Piano di Valutazione (PDV) per tale progetto potrà essere uno dei seguenti:
   i. nel caso in cui l'LVS abbia concluso, negli ultimi quattro anni, per lo schema nazionale OCSI istituito ai sensi del DPCM del 30 ottobre 2003, una valutazione (terminata con esito positivo) il cui ODV ricade nell'ambito dell'autorizzazione richiesta, il relativo procedimento può essere utilizzato come valutazione pilota;
   ii. nel caso in cui non sia disponibile la valutazione pilota di cui al precedente punto i., la procedura di valutazione si svolgerà in concomitanza con una valutazione condotta dal laboratorio su un prodotto ricadente nell'ambito di autorizzazione[55];

[52] Si applica il [DM] come riferimento attuale per tutte le attività di certificazione e vigilanza di ACN nelle more dell'adozione del decreto del Presidente del Consiglio dei ministri ex articolo 13, comma 1 del [DLGS].
[53] Nel caso di laboratorio estero la seguente documentazione dovrà essere prodotta in originale e tradotte in lingua inglese.
[54] Si veda sezione 5 del documento [SOA-LB].
[55] Si evidenzia che l'emissione del certificato per il prodotto in valutazione potrà essere emesso solo se il laboratorio, conclusa la valutazione, otterrà l'autorizzazione. Si raccomanda quindi di includere questo punto esplicitamente nel contratto con il Committente della certificazione.

7.3. Verifica (Fase 3)

Le verifiche sono eseguite tramite analisi documentale, visita ispettiva, interviste al personale e tramite revisione di un progetto pilota sottoposto dall'LVS.

Per l'esecuzione delle attività di verifica relative al rilascio dell'autorizzazione, l'Agenzia nomina un gruppo di valutazione della richiesta di autorizzazione.

L'Agenzia fornisce all'LVS un piano di lavoro composto almeno da quanto segue:

- revisione della documentazione per la completezza e adeguatezza del contenuto;
- composizione del gruppo di valutazione, segnalando il ruolo di ciascun membro del gruppo (auditor/esperto/osservatore);
- piano di interviste strutturate e della visita ispettiva che si prevede siano eseguite per la verifica delle competenze tecniche e per verificare l'applicazione delle misure tecnico-organizzative;
- attività di verifica che si intende eseguire sulla certificazione pilota.

L'attività svolta dal gruppo di valutazione dell'autorizzazione esegue le seguenti attività:

1. verifica della documentazione fornita dall'LVS in fase di richiesta e istruttoria;
2. verifica, tramite interviste strutturate al personale dell'LVS e tramite analisi della valutazione pilota, delle competenze possedute da parte dell'LVS in materia di valutazione nell'ambito dichiarato[56];
3. verifica delle misure tecnico-organizzative per la gestione delle informazioni[57];
4. monitoraggio della conduzione della valutazione pilota[58] (o revisione del procedimento già eseguito come previsto in sez. 7.2). Per il dettaglio circa la valutazione pilota si rimanda alla sezione 6.2.4 di [ENISA].

7.3.1. Verifiche della documentazione di accreditamento

L'Agenzia per predisporre le attività di controllo in sede di visita ispettiva esamina preliminarmente la documentazione di accreditamento per individuare requisiti specifici o supplementari da verificare. In particolare, esamina l'ambito di accreditamento per individuare:

- prove non campionate dall'Allegato A2 del documento [SOA-LB]

[56] Per ogni ambito di autorizzazione, il laboratorio deve disporre di almeno tre valutatori con competenze nello specifico ambito di autorizzazione.
[57] Per una lista degli aspetti da prendere in esame per la verifica delle misure tecnico-organizzative, si rimanda ad Annexc IV, sez.17 di [ENISA].

- eventuali componenti di garanzia non inclusi nell'ambito di accreditamento da integrare in fase di autorizzazione, anche su richiesta dell'LVS,
- competenze non esplicitate nei CV e schede del personale necessarie per l'autorizzazione,
- ogni altro elemento utile per la preparazione della visita ispettiva e delle interviste strutturate ai valutatori.

I suddetti ambiti sono oggetto di approfondimento nelle successive fasi di verifica in sede di visita ispettiva e intervista ai valutatori.

7.3.2. Verifiche di autorizzazione concomitanti con la valutazione

L'Agenzia può prevedere un incontro preliminare a supporto della pianificazione delle attività necessarie per l 'autorizzazione dell'LVS.

Per la conduzione delle attività di certificazione simultanee al processo di autorizzazione (caso valutazione pilota punto 6.ii sezione 7.2), l'**OCSI opera come in un normale processo di certificazione**. L'emissione del certificato è subordinata alla conclusione con successo della procedura di autorizzazione.

Il gruppo di valutazione della richiesta di autorizzazione, durante la propria attività, può interagire con il Responsabile del laboratorio al fine di richiedere modifiche e integrazioni alla documentazione fornita.

7.4. Rilascio (Fase 4)

Al termine delle verifiche, l'Agenzia produce un rapporto di autorizzazione sul modello di cui all'Allegato III del documento [ENISA].

In caso di esito positivo delle verifiche, al termine delle attività, l'Agenzia trasmette all'LVS la comunicazione di avvenuta autorizzazione o comunicazione di rigetto altrimenti.

Nel caso di LVS estero la comunicazione di autorizzazione sarà trasmessa anche all'autorità nazionale di certificazione della cybersicurezza dello Stato Membro in cui è stabilito LVS per la successiva notifica.

7.5. Durata della procedura di autorizzazione

L'istruttoria (fase 2) si conclude entro 30 giorni dalla richiesta (fase 1).

La verifica ed il rilascio (fasi 3 e 4) si concludono entro sessanta giorni, in alternativa

- a partire dalla conclusione della fase 2 in caso di valutazione pilota già disponibile da precedente attività dell'LVS nello schema nazionale [OCSI],
- a partire dalla conclusione della valutazione pilota condotta in concomitanza con il processo di autorizzazione,

con il rilascio del provvedimento di autorizzazione o con la comunicazione di rigetto dell'istanza di autorizzazione.

L'Agenzia può sospendere, al più una volta, le attività di autorizzazione fino a 30 giorni per l'acquisizione di elementi istruttori.

7.6. Validità, durata dell'autorizzazione

L'autorizzazione può essere emessa solo dopo l'accreditamento, ha quindi decorrenza successiva all'accreditamento.

L'autorizzazione è emessa con la stessa scadenza dell'accreditamento.

In caso di revoca o sospensione dell'accreditamento anche l'autorizzazione è revocata o sospesa dallo stesso momento o per lo stesso periodo.

7.7. Rinnovo dell'autorizzazione

Allo scadere dell'autorizzazione, per prorogarne la validità senza soluzione di continuità si effettua la procedura di rinnovo dell'autorizzazione.

La procedura di rinnovo non richiede di esaminare una valutazione pilota e procede in modo coordinato con la procedura di rinnovo dell'accreditamento.

Per poter avviare una procedura di rinnovo dell'autorizzazione sono necessarie le seguenti condizioni:

- l'accreditamento non deve essere scaduto;
- l'LVS nell'attuale periodo di accreditamento deve aver eseguito almeno una valutazione che ricade nell'ambito dell'autorizzazione.

Dal momento che la data di scadenza dell'autorizzazione e la data di scadenza dell'accreditamento sono uguali, il rinnovo dell'autorizzazione degli LVS deve essere eseguito dopo il rinnovo dell'accreditamento.

Pertanto, l'LVS, prima della scadenza dell'accreditamento presenterà domanda di rinnovo dell'autorizzazione in modo da poter completare l'iter di rinnovo dell'autorizzazione immediatamente dopo la conclusione dell'iter di accreditamento.

Nelle more del completamento dell'iter di rinnovo dell'accreditamento ove tale iter superi la scadenza dell'accreditamento originario, l'autorizzazione rimane valida per tutto l'iter di rinnovo dell'accreditamento. Terminato l'iter di rinnovo dell'accreditamento con esito positivo l'autorizzazione è ulteriormente estesa e rimane valida sino alla conclusione dell'iter del rinnovo dell'autorizzazione.

La domanda di rinnovo dell'autorizzazione a differenza della domanda di prima autorizzazione non includerà inizialmente la documentazione dell'accreditamento (certificato di accreditamento, rapporto di accreditamento, CV e schede del personale valutatore). Tale documentazione sarà integrata a conclusione dell'iter di accreditamento.

7.9. Notifica degli organismi di valutazione della conformità

L'Agenzia, ai sensi dell'articolo 61 del [CSA] notifica alla Commissione europea gli organismi di valutazione della conformità accreditati e autorizzati. In particolare:

- notifica gli organismi di certificazione e gli ITSEF accreditati da Accredia per il livello di affidabilità sostanziale ai sensi dell'articolo 8, comma 1 del decreto [DLGS];
- notifica l'autorizzazione rilasciata all'OCSI e agli LVS stabiliti nel territorio nazionale.[59]

L'accreditamento e l'autorizzazione di uno stesso organismo di valutazione della conformità possono essere notificati separatamente o anche simultaneamente.

7.10. Sospensione e revoca dell'autorizzazione

L'autorizzazione può essere sospesa o revocata sulla base degli elementi raccolti dalla Agenzia durante l'attività di vigilanza[60] o per tramite dell'organismo di accreditamento durante le attività di monitoraggio eseguite per il mantenimento o il rinnovo dell'accreditamento.

L'autorizzazione di un LVS[61] ad operare nell'EUCC è sospesa per 6 mesi o revocata nel caso di più di due violazioni di cui alla sezione 5.2 rispettivamente in un quinquennio o in un biennio. In caso di revoca dell'autorizzazione, l'LVS non può ottenere nuova autorizzazione nei successivi cinque anni dal provvedimento di revoca.

[59] La notifica delle eventuali autorizzazioni a LVS stabiliti all'estero sarà effettuata dall'autorità di certificazione della cybersicurezza del paese estero in cui è stabilito l'LVS.
[60] Articolo 31, paragrafo 3, lett. b) dell'[EUCC].
[61] Articolo 10, comma 19 del [DLGS].

8. Laboratori di prova abilitati per le attività di vigilanza

605 L’Agenzia non prevede, almeno nella fase iniziale di avvio del sistema di certificazione della cybersicurezza di sistemi e prodotti TIC, l’utilizzo di laboratori di prova abilitati, previsti dal [DLGS], art.8 comma 4, per il supporto nelle attività di vigilanza.

9. Glossario

Regolamento sulla cybersicurezza (Cybersecurity Act)	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.
Common Crtieria (CC)	Common Criteria for Information Technology Security Evaluation, come stabiliti negli standard 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, o stabiliti nei Common Criteria for Information Technology Security Evaluation, version CC:2022, Parts 1 through 5, pubblicato dai partecipanti all'accordo sul riconoscimento dei certificati Common Criteria nel campo della Sicurezza IT (CCRA).
Common Evaluation Methodology (CEM)	Common Methodology for Information Technology Security Evaluation, come stabiliti nello standard ISO/IEC 18045:2022, or Common Methodology for Information Technology Security Evaluation, versione CEM:2022, pubblicato dai partecipanti all'accordo sul riconoscimento dei certificati Common Criteria nel campo della Sicurezza IT (CCRA).
Sistema EUCC (European Common Criteria)	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).
ENISA	L'Agenzia dell'Unione europea per la cibersicurezza di cui al Titolo II del Regolamento sulla cybersicurezza.
Agenzia	L'Agenzia per la cybersicurezza nazionale di cui all'articolo 5 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, designata dall'articolo 7, comma 1, lettera e), del medesimo decreto-legge, per l'Italia, quale autorità nazionale di certificazione della cybersicurezza, di cui all'articolo 58, paragrafo 1, del Regolamento sulla cybersicurezza.
Organismo di Certificazione (OCSI)	Organismo di certificazione dell'Agenzia, accreditato ai sensi dell'articolo 60, paragrafo 2, del Regolamento (UE) 2019/881, istituito ai sensi dell'articolo 4 del decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Committente (o Richiedente di un certificato EUCC)	La persona fisica, giuridica o altro organismo o associazione che commissiona e sostiene gli oneri economici della

	valutazione e certificazione e che può anche rivestire il ruolo di Sviluppatore.
Sviluppatore (o Fornitore)	La persona fisica, giuridica o altro organismo o associazione che fornisce l'oggetto della valutazione e che può rivestire anche il ruolo di Committente.
Titolare del certificato	La persona fisica, giuridica o altro organismo o associazione a cui spettano gli oneri di gestione del certificato dopo l'emissione: corretto utilizzo del marchio EUCC, revisione e revoca dei certificati, monitoraggio delle non conformità e gestione delle conseguenze di non conformità rilevate, gestione delle vulnerabilità rilevate, pubblicazione delle informazioni sul certificato per l'utente richieste dall'[EUCC][62]. Può coincidere anche con il Committente successivamente all'emissione del certificato o con lo Sviluppatore.
Prodotto	Elemento *software*, *hardware* o *firmware* o un gruppo di elementi di una rete o di un sistema informativo.
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.
Valutazione	L'analisi di un prodotto, profilo di protezione o traguardo di sicurezza condotta in base allo standard Common Criteria.
Laboratorio per la Valutazione della Sicurezza (LVS)	L'organizzazione indipendente che ha ottenuto l'abilitazione dall'Organismo di Certificazione per effettuare valutazioni nell'ambito di un processo di certificazione condotto dall'Organismo di Certificazione.
Piano di Valutazione	Il documento che descrive le attività che saranno svolte dal Laboratorio per la Valutazione della Sicurezza durante il processo di valutazione, i tempi di esecuzione e le risorse necessarie.
Garanzia (o Affidabilità)	La fiducia che si può riporre nel soddisfacimento degli obiettivi di sicurezza da parte dell'oggetto della valutazione considerando le minacce e l'ambiente descritti nel traguardo di sicurezza.
Livello di Garanzia della Valutazione	Pacchetto di requisiti di garanzia della sicurezza ben formato che rappresenta un punto nella scala predefinita di garanzia.

[62] Gestione corretta del marchio EUCC (art. 11) revisione e revoca del certificato (artt. 13, 14, 19, Annex IV), monitoraggio delle non conformità e gestione delle conseguenze (artt. 25, 27, 29, 30) gestione delle vulnerabilità (artt. 33, 35, 38, 39), pubblicazione delle informazioni per gli utenti (art. 41).

Livello di garanzia sostanziale	Pacchetto di requisiti di garanzia della sicurezza ben formato che include il componente di garanzia AVA_VAN.1 o AVA_VAN.2
Livello di garanzia elevato	Pacchetto di requisiti di garanzia della sicurezza ben formato che include AVA_VAN.3, AVA_VAN.4 o AVA_VAN.5.
Funzioni di Sicurezza	Le contromisure di sicurezza di tipo tecnico di cui è dotato l'oggetto della valutazione.
Meccanismo di Sicurezza	Le componenti *hardware*, *software* e *firmware* che realizzano le funzioni di sicurezza di cui è dotato l'oggetto della valutazione.
Materiale per la valutazione	La documentazione tecnica o le componenti software, hardware, firmware realizzati durante lo sviluppo del prodotto
Accreditamento	Attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità.
Organismo di accreditamento	L'organismo nazionale di accreditamento autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'articolo 2, paragrafo 1, numero 11, del regolamento (CE) 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99;
Autorizzazione	Provvedimento con il quale l'Agenzia accerta il possesso, a norma dell'articolo 54, paragrafo 1, lettera f), del Regolamento sulla cybersicurezza, dei requisiti di competenza a cui sono soggetti gli organismi di valutazione della conformità per poter operare nell'ambito dei processi di certificazione o valutazione per l'emissione di certificati con livello di garanzia elevato.
Abilitazione	Provvedimento con il quale l'Agenzia accerta i requisiti necessari affinché' un Laboratorio per la Valutazione della Sicurezza possa coadiuvare 'Agenzia nelle attività di vigilanza.
Oggetto della Valutazione (ODV) mantenuto	Un ODV modificato per il quale sono completate le attività relative alla procedura di mantenimento del certificato e per il quale risulta ancora valido il certificato dell'ODV originale. Le garanzie fornite dall'ODV certificato sono anche fornite dall'ODV mantenuto.

10. Riferimenti

[ACN] Decreto-legge 14 giugno 2021, n. 82, “Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.” convertito con modificazioni dalla L. 4 agosto 2021, n. 109.

[CC1] “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, November 2022, CC:2022, Revision 1, CCMB-2022-11-001.

[CC2] “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements”, November 2022, CC:2022, Revision 1, CCMB-2022-11-002.

[CC3] “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements”, November 2022, CC:2022, Revision 1, CCMB-2022-11-003.

[CC4] “Common Criteria for Information Technology Security Evaluation, Part 4 – Framework for the specification of evaluation methods and activities”, November 2022, CC:2022, Revision 1, CCMB-2022-11-004.

[CC5] “Common Criteria for Information Technology Security Evaluation, Part 5 – Pre-defined packages of security requirements”, November 2022, CC:2022, Revision 1, CCMB-2022-11-005.

[CEM] “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, November 2022, CC:2022, Revision 1, CCMB-2022-11-006.

[CSA] 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»).

[DLGS] Decreto Legislativo 3 agosto 2022 , n. 123, recante “Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» del 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»).

[DM] Decreto Ministero Comunicazioni del 15 febbraio 2006, GU n. 82 del 7 aprile 2006, "Individuazioni delle prestazioni, eseguite dal Ministero delle comunicazioni per conto terzi, ai sensi dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366".

[ENISA] ‘Authorisation of CBs and ITSEFs for the EUCC Scheme’, version 0.7.

[EUCC] 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).

[OCSI] Decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003, "Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10".

[SOA-LB] EUCC Scheme state-of-the-art document 'Accreditation of ITSEFs for the EUCC', version 1.6c.

[17025] UNI/CEI EN ISO/IEC 17025, "Requisiti generali per la competenza dei laboratori di prova e di taratura", 2018.

11. Allegato A – Categorie di prodotti ai fini dell'autorizzazione

Sono soggetti ad autorizzazione, in caso di valutazioni con componente di garanzia AVA_VAN.3, i prodotti che ricadono nelle seguenti categorie:

- dispositivi e sistemi per il controllo di accesso;
- sistemi e dispositivi biometrici;
- dispositivi e sistemi di protezione perimetrale;
- protezione dei dati;
- database;
- dispositivi e sistemi di rilevamento;
- circuiti integrati, smart-card e dispositivi e sistemi relativi alle smart-card;
- sistemi per la gestione delle chiavi;
- prodotti per le comunicazioni con dispositivi mobili;
- dispositivi multifunzione;
- rete e dispositivi e sistemi di rete;
- sistemi operativi;
- prodotti per la firma digitale;
- trusted computing;
- altre categorie proposte dall'LVS e approvate dall'OCSI.

Resta inteso che, laddove le predette categorie afferiscano a domini tecnici definiti in [EUCC] si applicano le indicazioni contenute nei documenti allo stato dell'arte richiamati in [EUCC].