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*)

Organismo di Certificazione della Sicurezza Informatica

Linea Guida OCSI N. 1

Sistema EUCC: le caratteristiche generali e gli attori del processo di certificazione dell'OCSI (art. 4 c. 2, art. 11 cc. 3-4 d.lgs. n. 123/2022)

Versione 1.0

3 febbraio 2025

REGISTRAZIONE 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	OCSI	Prima emissione	3 febbraio 2025

1. Indice

1. Indice 3
2. Acronimi 4
3. Scopo del documento 5
4. Pubblicazioni del sistema EUCC 6
5. Il sistema EUCC e la transizione dallo Schema nazionale 8
6. Introduzione 12
7. Finalità dell'attività di valutazione e di certificazione 13
8. Organizzazione e ruoli del processo di valutazione e certificazione 14
8.1. L'Agenzia 14
8.2. L'Organismo nazionale di accreditamento 15
8.3. L'Organismo di Certificazione 15
8.4. Il Laboratorio per la Valutazione della Sicurezza 16
8.5. Il Committente e il Titolare del certificato 17
8.6. Lo Sviluppatore 18
8.7. L'Assistente 18
9. Le fasi del processo di valutazione e certificazione 20
10. Accordo di certificazione 21
10.1. Impegni dell'OCSI 22
10.2. Impegni del Committente e Titolare del certificato 23
10.3. Impegni dell'LVS 24
11. Il marchio OCSI 26
11.1. Elementi grafici e dimensioni 26
11.2. Condizioni di impiego 27
11.3. Sorveglianza e azioni in caso di violazioni 28
12. Reclami e ricorsi 29
13. Monitoraggio e revoca dei certificati 30
14. Glossario 31
15. Oneri dovuti all'OCSI 36
15.1. Impegno richiesto all'OCSI per le attività di abilitazione 36
15.2. Impegno richiesto all'OCSI per le attività di certificazione 36
16. Riferimenti 38

2. Acronimi

ACN	Agenzia per la cybersicurezza nazionale
CC	Common Criteria
CE	Commissione Europea
CEI	Comitato Elettrotecnico Italiano
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	(Evaluation Assurance Level) Livello di garanzia della valutazione
EUCC	European Cybersecurity Scheme on Common Criteria
EN	European Norm
GU	Gazzetta Ufficiale
IEC	International Electrotechnical Commission
ISCTI	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ISO	International Organization for Standardization
IT	Information Technology
TIC	Tecnologia dell'Informazione e della Comunicazione (ICT – Information and Communication Technology)
LVS	Laboratorio di Valutazione della Sicurezza
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto Della Valutazione (TOE - Target of Evaluation)
PP	Profilo di Protezione (Protection Profile)
TDS	Traguardo di Sicurezza (ST – Security Target)
UNI	Ente Nazionale Italiano di Unificazione

3. Scopo del documento

Il presente documento ha come scopo la definizione delle modalità operative dell'organismo di certificazione 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 con il termine «Agenzia». L'organismo di certificazione dell'Agenzia è individuato nell'Organismo di Certificazione della Sicurezza Informatica (OCSI)[2], stabilito inizialmente presso il Ministero delle comunicazioni ([OCSI])[3] e trasferito presso l'Agenzia per la cybersicurezza nazionale con decorrenza primo luglio 2022 ([TRNSF])[4].

L'OCSI è l'organismo di certificazione originariamente istituito per sovrintendere alle attività operative di valutazione e certificazione nell'ambito dello schema nazionale di certificazione della cybersicurezza basato sui Common Criteria ([OCSI]). Con l'entrata in vigore dell'EUCC, lo schema nazionale cessa di produrre i propri effetti[5], come altri schemi nazionali stabiliti in EU basati sui Common Criteria, venendo superato dalle nuove regole armonizzate stabilite dall'EUCC ([EUCC]).

La presente linea guida tratta in particolare **delle caratteristiche generali e degli attori del sistema, dell'accordo di certificazione tra tali attori, inclusi l'utilizzo del marchio OCSI e del marchio EUCC, trattamento dei reclami e risoluzione delle controversie** 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].

---

[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, numero 123 ([DLGS]).

[2] L'organismo di certificazione dell'autorità è individuato nell'OCSI dall'articolo 6, comma 1 del decreto legislativo 3 agosto 2022, numero 123 ([DLGS]).

[3] L'articolo 4 del Decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003 ([OCSI]) istituisce l'OCSI presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero delle comunicazioni.

[4] Il Decreto del Presidente del Consiglio dei ministri del 15 giugno 2022 ([TRNSF]), trasferisce l'OCSI presso l'Agenzia per la cybersicurezza nazionale dal primo luglio 2022, in attuazione dell'articolo 7, lettera e) del decreto-legge 14 giugno 2021, n. 82 ([ACN]).

[5] Le modalità di transizione degli schemi nazionali operativi in EU verso le regole armonizzate dell'EUCC sono stabilite nell'art. 49 di [EUCC].

4. Pubblicazioni del sistema EUCC

Per consentire l'attuazione nazionale dell'EUCC come previsto dall'articolo 4 comma 2 del [DLGS], l'Agenzia ha adottato il

- Decreto del Direttore Generale dell'Agenzia per la cybersicurezza nazionale, "Organizzazione e procedure per lo svolgimento dei compiti dell'agenzia quale autorità nazionale di certificazione della cybersicurezza ex art. 4. comma 2 del d.lgs. 3 agosto 2022, n. 123." ([DD]),

che disciplina l'operatività dell'Agenzia, in quanto autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del [CSA]. Lo stesso, oltre a stabilire organizzazione e attribuzione dei compiti dell'autorità nazionale di certificazione della cybersicurezza, include le seguenti linee guida vincolanti per l'attuazione nazionale del sistema europeo di certificazione della cybersicurezza EUCC):

- Linea Guida NCCA N. 1– Attività di vigilanza nazionale e autorizzazione per il sistema EUCC (art. 5, art. 8 cc. 3-4 d.lgs. 123/2022) ([LG1-CA]);
- Linea Guida OCSI N. 1– Sistema EUCC: le caratteristiche generali e gli attori del processo di certificazione dell'OCSI (art. 4 c. 2, art. 11 cc. 3-4 d.lgs. 123/2022) ([LG1-OC]);
- Linea Guida OCSI N. 2 – Abilitazione dei laboratori per la valutazione della sicurezza per il sistema EUCC (art. 8 c. 4 d.lgs. 123/2022) ([LG2-OC]);
- Linea Guida OCSI N. 3 – Attività di valutazione ed emissione dei certificati per il sistema EUCC (art. 6 d.lgs. 123/2022) ([LG3-OC]).

Per l'operatività dell'OCSI si applicano in particolare le linee guida [LG1-OC], [LG2-OC] ed [LG3-OC].

La linea guida [LG1-CA] si applica alle attività dell'Agenzia in merito

- alla vigilanza degli organismi di valutazione della conformità, dei titolari dei certificati, e
- all'autorizzazione dell'OCSI e degli LVS, che costituiscono gli organismi di valutazione della conformità operativi al livello di garanzia elevato nell'attuazione nazionale dell'EUCC[6].

[6] L'unico organismo di certificazione emittente di certificati di livello elevato è l'OCSI operativo presso l'Agenzia ai sensi dell'articolo 56, paragrafo 6. Per l'attuazione nazionale dell'EUCC in Italia si sceglie di non avvalersi di altri organismi di certificazione accreditati ai sensi dell'articolo 56, paragrafo 6, lett. a)-b). Pertanto gli unici ITSEF operativi a livello elevato sono gli LVS abilitati dall'OCSI per operare nei propri processi di certificazione.

Le linee guida [LG1-OC], [LG2-OC], [LG3-OC] devono essere osservate da tutti coloro (persone fisiche, giuridiche e qualsiasi altro organismo o associazione) cui competono le decisioni in ordine alla richiesta, acquisizione, progettazione, realizzazione, installazione ed impiego di prodotti TIC sottoposti e certificazione o che sono stati
115 certificati in Italia con l'OCSI nell'ambito del sistema EUCC.

Si evidenzia che per gli eventuali aspetti non trattati nelle linee guida che dovessero rientrare nell'ambito specifico di ciascuna di esse, si applicano le disposizioni contenute nel regolamento di esecuzione [EUCC].

5. Il sistema EUCC e la transizione dallo Schema nazionale

Con l'adozione del primo sistema europeo di certificazione della cybersicurezza da parte della Commissione europea il 31 gennaio 2024, ovvero l'EUCC ([EUCC]), si stabilisce nell'Unione Europea il sistema di regole armonizzate per la certificazione di cybersicurezza di prodotti TIC basato sullo standard Common Criteria e per la successiva gestione dei certificati.

L'attuale Schema nazionale italiano per la valutazione e la certificazione della sicurezza dei sistemi e dei prodotti nel settore della tecnologia dell'informazione adottato con Decreto del Presidente del Consiglio dei ministri ([OCSI]) cessa gradualmente i propri effetti per lasciar spazio alle nuove regole armonizzate per la certificazione della cybersicurezza basata sui Common Criteria ([CC 1,2,3,4,5]) e relativa metodologia di valutazione ([CEM]), che sono stabilite con l'EUCC[7].

L'Organismo di certificazione della sicurezza informatica (OCSI), che dal 2003 è stato individuato per sovraintendere alle attività operative di valutazione e certificazione nell'ambito dello Schema nazionale, attualmente operativo presso l'Agenzia[8], è designato dal [DLGS][9] anche quale organismo di certificazione dell'Agenzia per il sistema EUCC, per proseguire le attività di certificazione basate sui Common Criteria con le nuove regole europee armonizzate.

La transizione dallo Schema nazionale all'EUCC prevede alcune tappe fondamentali[10]. Oltre il **26 febbraio 2025** non potranno essere più avviati processi di certificazione nell'ambito dello Schema nazionale ([OCSI]). Dal **27 febbraio 2025** sarà consentita l'emissione dei primi certificati EUCC. Oltre il **26 febbraio 2026** non potranno più essere emessi certificati basati sullo Schema nazionale. Sarà tuttavia possibile effettuare il mantenimento dei certificati[11] già rilasciati nell'ambito dello Schema nazionale fino alla loro naturale scadenza.

Va evidenziato che il nuovo modello operativo europeo nel quale è chiamato ad operare l'OCSI per effetto del combinato delle disposizioni del [CSA] e dell'[EUCC] è sensibilmente diverso dal quadro stabilito per lo Schema nazionale ([OCSI]) nonostante

[7] Le modalità di transizione degli schemi nazionali europei al nuovo sistema europeo di certificazione della cybersicurezza EUCC sono stabilite dall'art. 49 dell'[EUCC].
[8] Il decreto [OCSI] aveva inizialmente individuato l'OCSI nell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle Comunicazioni. Successivamente, con il decreto [TRNSF] con decorrenza primo luglio 2022 l'OCSI è divenuto operativo presso l'Agenzia.
[9] L'OCSI è designato organismo di certificazione dell'Agenzia ai sensi dell'articolo 6, comma 1 del [DLGS].
[10] La transizione dagli schemi nazionali europei all'EUCC è stabilita dall'articolo 49 dell'[EUCC].
[11] Con il termine mantenimento di un certificato si intende un processo che consiste in una rivalutazione parziale dell'oggetto della valutazione a fronte di modifiche da ritenersi minori che interessino lo stesso o il suo ambiente di sviluppo. Il processo di mantenimento, con esito positivo non produrrà un nuovo certificato bensì un rapporto di mantenimento che sarà aggiunto al rapporto di certificazione rimodulandone l'ambito di applicazione.

il comune riferimento allo standard Common Criteria ([CC 1,2,3,4,5]) e relativa metodologia di valutazione ([CEM]).

In particolare, nell'EUCC si distinguono, per ogni pacchetto di garanzia selezionato per una valutazione, due possibili livelli di garanzia, ovvero:

- il ***livello sostanziale*** nel caso in cui il pacchetto di garanzia contenga il componente AVA_VAN.1 oppure AVA_VAN.2;
- il ***livello elevato*** nel caso in cui il pacchetto di garanzia contenga il componente AVA_VAN.3 oppure AVA_VAN.4 oppure AVA_VAN.5;

Inoltre, per poter operare come organismo di certificazione o laboratorio di prova per l'EUCC è necessario l'accreditamento da parte dell'organismo nazionale di accreditamento del paese in cui è stabilito l'organismo o il laboratorio. Tale organismo in Italia è Accredia[12]. L'accreditamento da parte di Accredia è necessario anche per l'operatività dell'OCSI come organismo di certificazione stabilito in Italia.

I laboratori di prova accreditati per poter operare in una valutazione per conto dell'OCSI devono essere preliminarmente abilitati ([LG2-OC]) attraverso un processo di formale ingaggio ad operare per l'OCSI. Tali laboratori in continuità con lo Schema nazionale prendono il nome di Laboratori per la Valutazione della Sicurezza (LVS).

Infine, si individua l'Agenzia[13] quale autorità nazionale di certificazione della cybersicurezza in Italia con il compito principale di supervisionare e monitorare le attività di emissione e gestione dei certificati di cybersicurezza per l'EUCC che non riguardano il solo OCSI, ma anche possibili altri organismi di certificazione accreditati da Accredia ad operare al livello sostanziale. Tra i compiti dell'Agenzia vi è anche quello di autorizzare l'OCSI e gli LVS ad operare a livello elevato, che nel caso di valutazioni con componenti di garanzia AVA_VAN.4 o AVA_VAN.5 richiede una verifica di competenza specifica rispetto alle metodologie armonizzate stabilite dall'EUCC[14]. In Tabella 1 sono riportate in modo analitico le principali differenze tra l'operatività dell'OCSI e degli LVS nell'ambito dello Schema nazionale attualmente operativo ([OCSI]) e nell'ambito dell'EUCC ([EUCC]).

[12] 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.

[13] Articolo 4, comma 1 del d.lgs. 123/2022.

[14] Le metodologie di valutazione per i domini tecnici *security boxes* e *smart-cards a similar devices* sono individuati nell'Annex I, comma 1, lett. (a) e (b) dell'EUCC.

	Schema nazionale ([OCSI])	Sistema europeo ([EUCC])
Livelli di garanzia e di valutazione	Per la valutazione di un prodotto TIC è possibile selezionare un qualsiasi pacchetto di componenti garanzia ben formato (tutte le dipendenze dirette e indirette tra componenti previste dallo standard devono essere rispettate), tra cui gli EAL previsti dallo standard con eventuali aggiunte, o i componenti previsti da un PP certificato.	Per la valutazione di un prodotto TIC è possibile selezionare un qualsiasi pacchetto di garanzia ben formato (tutte le dipendenze dirette e indirette tra componenti previste dallo standard devono essere rispettate), tra cui gli EAL previsti dallo standard con eventuali aggiunte, o i componenti previsti da un PP. Un componente della famiglia AVA_VAN deve essere obbligatoriamente incluso nel pacchetto. Al pacchetto di garanzia selezionato corrisponde un *livello di garanzia sostanziale* se il pacchetto include il componente di garanzia AVA_VAN.1 o AVA_VAN.2, oppure un *livello di garanzia elevato* se include il componente di garanzia AVA_VAN.3 o AVA_VAN.4 o AVA_VAN.5.
Operatività degli organismi di certificazione in Italia	L'OCSI è l'unico organismo di certificazione che può emettere certificati Common Criteria in Italia. L'OCSI è designato come organismo di certificazione nazionale per decreto. L'OCSI può emettere certificati senza accreditamento o autorizzazione preliminari da organismi esterni.	Qualsiasi organismo di certificazione accreditato da Accredia, rispetto alla norma [17065] per l'EUCC può emettere certificati di livello sostanziale in Italia. Anche l'OCSI per poter emettere certificati CC in Italia è accreditato rispetto alla norma [17065] per l'EUCC da Accredia. Solo l'OCSI, in Italia, emette certificati di livello elevato per l'EUCC. Gli altri organismi di certificazione accreditati da Accredia rispetto alla norma [17065] per l'EUCC possono emettere solo certificati di livello sostanziale. Per emettere certificati di livello elevato, l'OCSI è autorizzato dall'Agenzia[15] ([LG1-CA]).
Operatività dei laboratori di prova in	I laboratori di prova, denominati nello Schema nazionale LVS, per poter effettuare valutazioni con l'OCSI sono	I laboratori di prova per poter effettuare valutazioni in seno all'EUCC in EU a qualsiasi livello di garanzia devono essere accreditati rispetto alla [17025] per l'EUCC dall'organismo nazionale di accreditamento nel quale sono stabiliti.

[15] Articolo 60, par. 3 del [CSA] e articolo 21 dell'[EUCC].

	Schema nazionale ([OCSI])	Sistema europeo ([EUCC])
Italia	accreditati dall'OCSI. L'accreditamento dell'OCSI permette di operare in valutazioni fino al livello EAL4 con eventuali componenti di garanzia aggiunti. Valutazioni da EAL5 in poi possono essere autorizzate per singole valutazioni. Le eventuali attività di valutazione basate sui Common Criteria di laboratori di prova al di fuori dello Schema nazionale governato dall'OCSI non portano a certificati Common Criteria.	I laboratori di prova che operano per l'OCSI sono denominati LVS. Per poter operare nei processi di certificazione dell'OCSI devono essere abilitati dall'OCSI ([LG2-OC]). I laboratori di prova che possono operare in una valutazione con livello di garanzia elevato sono solo gli LVS dell'OCSI. Gli LVS per poter effettuare valutazioni in seno all'EUCC in Italia al livello di garanzia elevato devono essere anche autorizzati per l'EUCC dall'Agenzia[16] ([LG1-CA]). Per poter operare in valutazioni di livello elevato con componenti di garanzia AVA_VAN.4 o AVA_VAN.5 occorre saper applicare le metodologie armonizzate previste dall'EUCC. Le competenze degli LVS per tali metodologie sono verificate durante l'autorizzazione.

Tabella 1 – Differenze tra l'attuale Schema nazionale e l'EUCC.

[16] Articolo 60, par. 3 del [CSA] e articolo 22 dell'[EUCC].

6. Introduzione

La Linea Guida OCSI N.1 ([LG1-OC]) tratta delle caratteristiche generali processo di certificazione condotto dall'OCSI e della gestione successiva dei certificati emessi in cooperazione con i principali attori coinvolti (Agenzia, LVS, Committente, Titolare del certificato, Sviluppatore).

Il processo di certificazione del sistema EUCC utilizza i criteri contenuti nello standard Common Criteria [CC 1,2,3,4,5] e la corrispondente metodologia di valutazione [CEM] realizzando delle modalità di certificazione e gestione dei certificati armonizzate in EU. Un certificato emesso nell'ambito del sistema EUCC dall'OCSI è riconosciuto in tutti gli Stati Membri[17].

Il sistema EUCC, come tutti i sistemi europei di certificazione della cybersicurezza adottati dalla Commissione europea ai sensi dell'articolo 49 del [CSA], non si applica ai prodotti TIC che trattano informazioni classificate o impiegati nelle attività del settore della pubblica sicurezza, della difesa, della sicurezza nazionale e nelle attività dello Stato nell'ambito del diritto penale[18]. Per tali ambiti gli Stati Membri possono prevedere sistemi di certificazioni nazionali.

In particolare, per l'autorizzazione all'utilizzo di prodotti TIC nell'ambito del perimetro di sicurezza nazionale cibernetica è previsto uno schema nazionale separato ([CVCN], [DPCM1], [DPCM2], [DPCM3], [DPCM4]).

[17] I certificati emessi dall'OCSI, in virtù della sua adesione all'accordo internazionale CCRA ([CCRA]), sono riconosciuti fino al livello EAL2 (per gli eventuali cPP certificati fino a EAL4) anche da tutti i partecipanti all'accordo non appartenenti all'UE.

[18] Articolo 1, paragrafo 2 del [CSA].

7. Finalità dell'attività di valutazione e di certificazione

L'utilità primaria della certificazione della sicurezza di un prodotto TIC o di un Protection Profile (PP) secondo le regole del sistema EUCC è quella di fornire una stima del livello di sicurezza secondo uno standard condiviso da tutti i soggetti coinvolti e di garantire che tale stima venga eseguita da una terza parte indipendente rispetto ai soggetti stessi.

Il sistema EUCC utilizza come specifiche di riferimento i criteri contenuti nello standard Common Criteria [CC 1,2,3,4,5] e la corrispondente metodologia [CEM] individuando delle modalità di certificazione e gestione dei certificati armonizzate in EU.

L'attività di valutazione è finalizzata all'emissione di un rapporto in cui viene dichiarato se:

a. l'ODV soddisfa il traguardo di sicurezza con il livello di garanzia richiesto;
b. il profilo di protezione è completo, consistente e tecnicamente corretto;
c. il traguardo di sicurezza è completo, consistente e tecnicamente corretto ed adatto ad essere usato come base per la valutazione del corrispondente ODV.

La certificazione stabilisce che la valutazione è stata condotta conformemente ai criteri necessari a verificare il soddisfacimento del livello di fiducia, della robustezza dei meccanismi o delle funzioni di sicurezza dichiarati e conseguentemente garantisce i risultati della valutazione stessa.

I risultati delle attività di valutazione e certificazione sono riferibili esclusivamente ad una specifica e determinata configurazione dell'ODV e il certificato è valido ed efficace limitatamente a tale configurazione.

La commercializzazione di un sistema o prodotto TIC certificato è vincolata a tale configurazione.

La certificazione effettuata dall'OCSI avviene a titolo oneroso. Le relative tariffe sono stabilite dal Ministro delle comunicazioni di concerto con il Ministro dell'economia e delle finanze nel decreto [DM][19], nelle more dell'adozione del decreto di cui all'art. 13, comma 1, del [DLGS].

[19] Articolo 3, comma 3 del decreto ([OCSI]).

8. Organizzazione e ruoli del processo di valutazione e certificazione

I soggetti coinvolti nel processo di valutazione e certificazione della sicurezza all'interno del sistema EUCC sono:

a. l'Agenzia,
b. l'Organismo nazionale di accreditamento,
c. l'Organismo di Certificazione (OCSI),
d. il Laboratorio per la Valutazione della Sicurezza (LVS),
e. il Committente,
f. lo Sviluppatore,
g. il Titolare del certificato,
h. l'Assistente

8.1. L'Agenzia

L'autorità nazionale di certificazione della cybersicurezza designata[20] per l'Italia è l'Agenzia[21].

All'Agenzia spetta il compito di monitorare e supervisionare i certificati emessi in Italia dall'OCSI e dagli altri organismi di certificazione operativi a *livello di garanzia sostanziale* e detenuti dai rispettivi Titolari dei certificati per far rispettare le disposizioni del [CSA] e dell'[EUCC].

Ha potere sanzionatorio ai sensi dell'articolo 10 del [DLGS] 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 e i Titolari dei certificati.

All'Agenzia spetta autorizzare l'OCSI e gli LVS ad operare al *livello di garanzia elevato*[22]. Ai fini dell'accreditamento, assiste e sostiene l'organismo nazionale di accreditamento (Accredia) nel monitoraggio degli organismi di valutazione della conformità (organismi di certificazione e ITSEF).

L'Agenzia coopera anche con le autorità nazionali di certificazione della cybersicurezza designate negli altri stati membri, le autorità di vigilanza del mercato competenti.

[20] Articolo 58, paragrafo 1 del [CSA].
[21] Articolo 7, comma 1, lett. e) del decreto [ACN] e articolo 4, comma 1 del [DGLS].
[22] Articolo 60, par.3 del [CSA]; articoli 21-22 dell'[EUCC].

8.2. L'Organismo nazionale di accreditamento

Ogni Stato Membro designa un unico organismo nazionale di accreditamento[23] per attestare che un determinato organismo di valutazione della conformità soddisfi i criteri per svolgere una specifica attività di valutazione della conformità.

Il [CSA] prevede un accreditamento obbligatorio[24] per ogni organismo di valutazione della conformità che voglia operare in un sistema europeo di certificazione della cybersicurezza, verificando in generale le competenze, la capacità di operare in modo indipendente ed imparziale e di tutelare anche la riservatezza delle informazioni acquisite durante la valutazione[25].

Per l'[EUCC] si individuano due principali categorie di organismi da accreditare:

- Gli organismi di certificazione da accreditare rispetto alla norma [17065] e con le modalità armonizzate definite dal documento stato dell'arte per l'accreditamento degli organismi di certificazione [SOA-OC],
- i laboratori di prova (ITSEF) da accreditare rispetto alla norma [17025] e con le modalità armonizzate definite dal documento stato dell'arte per l'accreditamento degli ITSEF [SOA-LB].

Un ITSEF accreditato in uno Stato Membro dell'UE dal proprio organismo nazionale di accreditamento può operare per l'OCSI previa abilitazione ([LG2-OC]) da parte dello stesso. Per l'Italia l'organismo nazionale di accreditamento designato è Accredia.

8.3. L'Organismo di Certificazione

In base al decreto istitutivo [OCSI] e successivi decreti ([ACN], [TRNSF]) l'OCSI è stabilito presso l'Agenzia e opera come organismo di certificazione dell'autorità nazionale di certificazione della cybersicurezza.

L'OCSI, nell'implementazione nazionale dell'EUCC è l'unico organismo di certificazione per l'emissione dei certificati di cybersicurezza per il livello di garanzia elevato in Italia.

Per l'operatività nel sistema EUCC l'OCSI è accreditato dall'organismo nazionale di accreditamento designato in Italia, Accredia. Per l'emissione dei certificati di livello elevato l'OCSI è autorizzato dall'Agenzia ([LG1-CA]).

L'OCSI sovrintende alle attività operative di valutazione e certificazione nell'ambito dell'implementazione nazionale dell'EUCC, in base alle linee guida [LG1-OC], [LG2-OC] ed [LG3-OC], attraverso:

[23] Ai sensi dell'articolo 4, paragrafo 1 del regolamento [ACCR].
[24] Articolo 50, paragrafi 1,2,4 del [CSA].
[25] Allegato 1 del [CSA].

a. l'abilitazione ([LG2-OC]), la sospensione e la revoca dell'abilitazione degli LVS accreditati da Accredia e, se del caso, autorizzati dall'Agenzia;

b. cooperazione con l'Agenzia e con l'organismo nazionale di accreditamento nel monitoraggio dell'indipendenza, imparzialità, affidabilità, competenze tecniche e capacità operative da parte degli LVS durante le valutazioni;

c. la predisposizione, l'aggiornamento e la pubblicazione dell'elenco degli LVS abilitati;

d. il monitoraggio degli obblighi incombenti sui Titolari dei certificati a norma dei regolamenti [CSA] ed [EUCC];

e. il monitoraggio dei requisiti di sicurezza dei certificati emessi per i prodotti TIC;

f. il monitoraggio del livello di affidabilità dei profili di protezione certificati;

g. l'approvazione dei Piani di Valutazione;

h. l'iscrizione delle valutazioni approvate nel sistema EUCC;

i. l'approvazione dei Rapporti Finali di Valutazione;

j. l'emissione dei Rapporti di Certificazione;

k. l'emissione, il riesame, la sospensione e la revoca dei Certificati;

l. la definizione, l'aggiornamento e la pubblicazione della lista di prodotti TIC e profili di protezione certificati e in corso di certificazione;

m. la gestione delle vulnerabilità riscontrate nei prodotti TIC certificati, cooperando con gli LVS, i Titolari dei certificati e l'Agenzia;

n. la gestione delle patch per i prodotti certificati cooperando con gli LVS e i Titolari dei certificati secondo la procedura definita dal Committente;

o. la ricerca e sviluppo di progetti nel campo della certificazione della cybersicurezza;

p. la formazione e l'addestramento dei Certificatori, personale dipendente dell'OCSI;

q. la formazione e l'abilitazione dei Valutatori, dipendenti degli LVS, ai fini dello svolgimento delle attività di valutazione.

8.4. Il Laboratorio per la Valutazione della Sicurezza

Nell'attività di valutazione l'OCSI si avvale di Laboratori per la Valutazione della Sicurezza (LVS), che svolgono le attività connesse alla valutazione. Gli LVS per poter operare con l'OCSI devono essere accreditati da Accredia e abilitati ([LG2-OC]) dall'OCSI stesso. Inoltre, per poter operare in una valutazione di livello elevato (contenente il componente AVA_VAN.3 o superiore) gli LVS devono anche essere autorizzati dall'Agenzia ([LG1-CA]).

In definitiva, un LVS è un ITSEF, preventivamente accreditato da Accredia secondo la norma [17025] ed eventualmente autorizzato dall'Agenzia, che è stato *abilitato* dall'OCSI.

Ai fini dell'abilitazione, l'LVS deve possedere i seguenti requisiti (Rif. [LG2-OC]):

a. un ambito di accreditamento adeguato a condurre valutazioni con l'OCSI;
b. la disponibilità di personale sufficiente dotato delle necessarie competenze tecniche;
c. la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

L'LVS nelle attività di valutazione (Rif. [LG3-OC])

a. coopera con il Committente (e con lo Sviluppatore, se soggetto diverso dal Committente) e con l'OCSI nei processi di certificazione per l'emissione dei certificati;
b. coopera con il Titolare del certificato (e con lo Sviluppatore, se soggetto diverso dal Titolare del certificato) e con l'OCSI nel mantenimento e analisi di vulnerabilità dei certificati;

Oltre alle attività di valutazione, un LVS può svolgere assistenza al Committente secondo le modalità specificate nella sezione 6.4 di [LG2-OC]. In particolare, l'LVS è tenuto a dare comunicazione all'OCSI in merito ad attività assistenza al Committente nell'ambito di una valutazione, specificando la natura e le modalità di assistenza nel piano di valutazione e fornendo anche un'analisi dei rischi di imparzialità nel piano di valutazione sottoposto ad approvazione da parte dell'OCSI.

I Valutatori devono essere indipendenti nello svolgimento delle loro attività. Il Valutatore è formato, addestrato ed abilitato dall'Organismo di Certificazione a condurre le attività di valutazione. Qualora uno o più Valutatori di un LVS diano assistenza ad un Committente per un ODV o parte di esso, gli stessi non potranno partecipare alla valutazione dello stesso ODV.

L'LVS deve assicurare che tutto il personale coinvolto nei processi di valutazione abbia sottoscritto un vincolo di riservatezza e di assenza di conflitti di interesse prima di essere impiegato nelle attività di valutazione.

8.5. Il Committente e il Titolare del certificato

Il Committente (o Richiedente della valutazione) è la persona fisica, giuridica o qualsiasi altro organismo che commissiona la valutazione.

Il Committente può anche rivestire il ruolo di Sviluppatore.

Il Committente sceglie l'LVS e richiede all'Organismo di Certificazione l'iscrizione della valutazione nello Schema nazionale. Durante il processo di valutazione fornisce all'LVS tutte le informazioni necessarie, complete e corrette per lo stesso. Il Committente si astiene dal promuovere il prodotto TIC in valutazione come già certificato.

Ottenuto il certificato il Committente diviene Titolare del certificato, salvo diversa indicazione, ed è soggetto agli obblighi stabiliti dal [CSA] e dall'[EUCC] in merito al monitoraggio delle eventuali non conformità del certificato e vulnerabilità del prodotto TIC certificato[26], al corretto utilizzo del marchio EUCC[27] e logo OCSI (rif. sezione 11), oltreché agli obblighi informativi nei confronti degli utenti del certificato previsti dall'EUCC[28].

8.6. Lo Sviluppatore

Lo Sviluppatore (o Fornitore) è la persona fisica, giuridica o qualsiasi altro organismo che realizza e fornisce l'ODV o parti componenti dell'ODV. Lo Sviluppatore può anche rivestire il ruolo di Committente della valutazione e del Titolare del certificato successivamente alla sua emissione.

Nel caso in cui il Committente non sia anche lo Sviluppatore, sarà necessario che quest'ultimo si renda disponibile a cooperare con il Committente nel processo di valutazione e certificazione, fornendo le informazioni tecniche e la documentazione in suo possesso richieste per la valutazione.

Nel caso in cui il Titolare del certificato non sia anche lo Sviluppatore, sarà necessario che quest'ultimo si renda disponibile a cooperare con il Titolare nel monitoraggio e gestione delle vulnerabilità e delle non conformità.

8.7.L'Assistente

Nell'ambito di un processo di certificazione per la preparazione della domanda di certificazione e/o per la revisione dei materiali di valutazione si rende frequentemente necessario il supporto da parte di un'organizzazione o singoli esperti che abbiano conoscenze approfondite sui Common Criteria, specialmente nei casi in cui uno Sviluppatore non faccia frequentemente ricorso alla certificazione Common Criteria. L'assistenza si focalizza generalmente nella preparazione della documentazione della domanda di certificazione e della relativa revisione durante le valutazioni.

Per sopperire a tale esigenza uno Sviluppatore o Committente farà ricorso a figure disponibili sul mercato. Le organizzazioni che dispongono del maggior numero di esperti con tale profilo sono gli ITSEF. Va tuttavia evidenziato che l'attività di assistenza e l'attività di valutazione sono tra loro incompatibili. Ovvero i valutatori impegnati in una valutazione non possono effettuare anche assistenza al Committente, altrimenti inficerebbero l'obiettività dei risultati della valutazione. I limiti all'attività di assistenza da parte di un LVS sono dettagliati in [SOA-LB].

[26] Sezioni V e VI e allegato IV dell'[EUCC].
[27] Articolo 11 dell'[EUCC].
[28] Articolo 41 dell'[EUCC].

Per operare come Assistente non occorre una abilitazione specifica da parte dell'OCSI. La selezione di un Assistente è una libera scelta da parte dello Sviluppatore o Committente di una valutazione. Con la scelta dell'Assistente va tuttavia garantita l'indipendenza e imparzialità del processo di certificazione. Si specificano di seguito alcune possibili modalità di assistenza riconosciute dall'OCSI che non inficiano l'obiettività di una valutazione condotta dall'OCSI.

Per la presentazione della domanda di valutazione e successiva conduzione della valutazione lo Sviluppatore può ingaggiare

- un'organizzazione diversa dall'LVS (o dall'organizzazione a cui appartiene l'LVS[29]) che condurrà la valutazione; tale organizzazione agirà come Committente durante la valutazione,
- singoli esperti non appartenenti all'LVS (o all'organizzazione di cui fa parte l'LVS) che condurrà la valutazione; lo Sviluppatore, coadiuvato dagli esperti, svolgerà il ruolo di Committente durante la valutazione,
- singoli esperti appartenenti all'LVS (o all'organizzazione di cui fa parte l'LVS) che condurrà la valutazione; l'ingaggio di personale dell'LVS per l'assistenza richiede tuttavia particolari cautele che sono trattate nella sezione 6.4 della [LG2-OC].

[29] In base al punto 5.1 della [17025] il laboratorio deve essere un soggetto giuridico, o una parte definita di esso, che sia legalmente responsabile delle proprie attività di laboratorio.

9. Le fasi del processo di valutazione e certificazione

Si descrivono sinteticamente le fasi del processo di certificazione che consistono nelle seguenti:

1. *Preparazione della valutazione* – attività con cui il Committente e l'LVS preparano la documentazione necessaria per richiedere all'OCSI l'avvio di una valutazione di un prodotto TIC o profilo di protezione.
2. *Conduzione della valutazione* – attività durante la quale l'LVS sulla base delle evidenze e materiali di valutazione acquisiti dall'LVS emette rapporti di valutazione per l'OCSI con cui comunica all'OCSI i risultati della valutazione rispetto ai componenti del pacchetto di garanzia selezionato.
3. *Conclusione della valutazione* – consiste nell'emissione da parte dell'LVS di un rapporto finale che sintetizza i risultati della valutazione dichiarando l'ODV conforme o non conforme ai requisiti di garanzia dichiarati.
4. *Preparazione ed emissione del certificato* – attività di elaborazione da parte dell'OCSI e del rapporto di certificazione che indica il contesto e le condizioni di validità del certificato per il prodotto TIC o profilo di protezione.
5. *Chiusura del processo di certificazione* – attività finali del processo di certificazione che includono la pubblicazione del certificato da parte dell'OCSI e l'eventuale tenuta di una riunione di chiusura della valutazione tra OCSI, LVS e Titolare del certificato.
6. *Gestione nel tempo delle garanzie dei prodotti certificati* – attività successive di monitoraggio e gestione del certificato che coinvolgono l'Agenzia, l'OCSI, l'LVS e il Titolare del certificato per garantire la conformità ed il livello di garanzia del certificato nel tempo.

Maggiori dettagli sono forniti nella linea guida [LG3-OC].

10. Accordo di certificazione

Il sistema EUCC, ha natura volontaria, ovvero l'emissione di un certificato di prodotto TIC non rappresenta un requisito necessario per l'immissione del prodotto sul mercato nazionale o europeo.

È bene evidenziare che una volta intrapreso volontariamente tale percorso, l'EUCC stabilisce obblighi in capo ai soggetti che partecipano al processo di certificazione (Committente, LVS, OCSI) ed al successivo monitoraggio e gestione dei certificati (Titolare del certificato, LVS, OCSI). Tali obblighi sono individuati puntualmente in particolare nei seguenti articoli e capi dell'[EUCC]:

- articoli 8 e 16 – Informazioni necessarie per la certificazione,
- articoli 9 e 17 – Condizioni per il rilascio di un certificato EUCC,
- articolo 11 – Gestione del marchio ed etichetta,
- articolo 13 e 19 – Riesame del certificato EUCC,
- articolo 14 e 20 – Revoca del certificato EUCC,
- CAPO V – Monitoraggio, non conformità e non compliance
- CAPO VI – Gestione e divulgazione delle vulnerabilità
- CAPO VII – Conservazione, divulgazione e protezione delle informazioni
- ALLEGATO IV – Continuità dell'affidabilità e riesame dei certificati

Per le attività di certificazione condotte con l'OCSI si aggiungono inoltre ulteriori impegni da parte dell'OCSI, del Committente e Titolare del certificato e dell'LVS per soddisfare i requisiti della norma [17065] per le certificazioni dell'OCSI, quali ad esempio la gestione del logo OCSI e i doveri dell'LVS in merito alla riservatezza, imparzialità e indipendenza.

Pertanto, i soggetti che intervengono nel processo di certificazione e nella successiva gestione dei certificati emessi sono vincolati da quanto stabilito dall'EUCC e per quanto non esplicitamente previsto nell'EUCC anche dalle norme nazionali di implementazione dell'EUCC pubblicate sul sito web dell'ACN (rif. sezione 4 Pubblicazioni del sistema EUCC).

Nel seguito sono trattati gli impegni richiesti a tali soggetti rispetto a quanto richiesto dall'EUCC e dalle norme nazionali di implementazione dell'EUCC. In particolare:

- gli impegni dell'OCSI relativamente ai certificati da esso emessi sono trattati nella sezione 10.1;
- gli impegni che il Committente garantisce di assumersi nell'ambito del processo di certificazione e che il Titolare del certificato garantisce di assumersi nell'utilizzo e gestione dei certificati emessi dall'OCSI, sono descritti nella sezione 10.2;

- gli impegni che l'LVS si assume relativamente alle attività di valutazione durante la valutazione e successivamente all'emissione del certificato nella sezione 10.3.

L'OCSI in quanto organismo pubblico è vincolato al rispetto alla norma europea e norme nazionali per l'EUCC. L'LVS sottoscrive l'impegno a rispettare le prescrizioni dell'EUCC e le norme di implementazione nazionale dell'EUCC in fase di domanda di abilitazione. Il Committente sottoscrive l'impegno a rispettare le prescrizioni dell'EUCC e le norme di implementazione nazionale dell'EUCC in fase di domanda di iscrizione della valutazione.

10.1. Impegni dell'OCSI

Con l'emissione di un certificato da parte dell'OCSI si attesta la conformità del prodotto valutato ai requisiti individuati dai Criteri Comuni ([CC 1,2,3,4,5])) e relativa metodologia di valutazione ([CEM]) con il livello di garanzia individuato nel certificato.

In conformità con i Criteri Comuni è bene evidenziare che il pacchetto di garanzia e relativo livello di garanzia attestati riguarda unicamente il prodotto nella configurazione valutata, comprensiva non solo delle caratteristiche tecniche del prodotto in sé, ma anche del processo produttivo, della catena di fornitura, del processo di consegna e dell'ambiente di utilizzo da parte dell'utente, con tutte le pertinenze fisiche, logiche e organizzative coinvolte. In particolare, l'eventuale utilizzo del prodotto in un ambiente operativo differente, con configurazioni, elementi SW, FW o HW di supporto, modalità di installazione e configurazione diverse da quelle indicate nel certificato o in caso di ipotesi di esposizione a minacce di sicurezza delle informazioni e di sicurezza cibernetica differenti da quanto descritto nel documento Traguardo di Sicurezza, valutato nell'ambito del processo di certificazione, inficiano il pacchetto e il livello di garanzia attestati nel certificato. Inoltre, il prodotto certificato risulta resistente alle sole minacce individuate nel problema di sicurezza del Traguardo di Sicurezza.

L'OCSI emette certificati per l'utilizzo in ambito civile. Un certificato OCSI non attesta in generale l'idoneità del prodotto per l'ambito classificato o per l'utilizzo nell'ambito del perimetro di sicurezza nazionale cibernetica. Per tali ambiti sono istituiti a livello nazionale schemi distinti ([UCSE], [CVCN]).

Inoltre, l'OCSI non attesta l'assenza di vulnerabilità che potrebbero emergere nel corso di una successiva attività di valutazione del prodotto e non note al momento dell'emissione del certificato.

Successivamente all'emissione del certificato l'OCSI, in collaborazione l'LVS che ha eseguito la valutazione, con il Titolare del certificato e l'Agenzia monitora la conformità del certificato e le vulnerabilità dei prodotti TIC certificati nel tempo, effettuando riesami, anche su richiesta del Titolare del certificato, per confermare il certificato, estendendone la validità o revocare, sospendere o ridurre l'ambito del certificato in ragione della scoperta di non conformità o vulnerabilità.

L'organismo di certificazione garantisce, per il tramite dell'articolazione competente, che le informazioni e i documenti emessi o condivisi durante le valutazioni non siano rilasciati a soggetti terzi o divulgati e siano conservati e trattati in modo da tutelarne la

riservatezza, in linea con le procedure adottate da ACN per la gestione dei flussi documentali. Gli accessi alla documentazione di valutazione necessari per gli adempimenti discendenti da norma nazionale o europea sono autorizzati e supervisionati dal responsabile della gestione documentale dell'Agenzia. In particolare, nell'ambito di visite ispettive finalizzate all'accreditamento dell'OCSI ai sensi dell'articolo 60, paragrafo 2 del regolamento [CSA] potrà rendersi necessario esibire documentazione registrata nei fascicoli afferenti a procedimenti di certificazione. In tal caso è prevista l'esibizione documentale *de visu* agli ispettori incaricati preferibilmente a video. L'estrazione di copia potrà essere valutata ove strettamente necessaria per le attività di verifica, previa autorizzazione e supervisione da parte del responsabile della gestione documentale e del responsabile della conservazione dell'Agenzia e tale evenienza sarà comunicata al relativo portatore di interessi.[30].

È facoltà del Titolare accedere alle informazioni di certificazione e presentare richieste di chiarimenti o reclami che saranno adeguatamente trattati dall'OCSI in modalità trasparente e imparziale come descritto nella sezione 12.

L'OCSI è tenuto a mantenere le evidenze alla base dei certificati emessi assicurando che le proprie registrazioni siano conservate per almeno 5 anni dall'emissione del certificato.[31]

Il Titolare di un certificato EUCC può richiedere la revoca del certificato all'OCSI.

10.2. Impegni del Committente e Titolare del certificato

Il Committente si assume gli impegni seguenti durante il processo di certificazione:

- presentazione all'organismo di certificazione e all'LVS di tutte le informazioni necessarie, complete e corrette, e di ulteriori informazioni necessarie, se richiesto;
- astensione dalla promozione del prodotto TIC come certificato nel quadro dell'EUCC prima che il certificato EUCC sia stato rilasciato;
- promozione del prodotto TIC come certificato solo in relazione all'ambito di applicazione stabilito nel certificato EUCC;
- cessazione immediata della promozione del prodotto TIC come certificato in caso di sospensione, revoca o scadenza del certificato EUCC.

Il Committente della certificazione, prima dell'emissione del certificato, si assume, in qualità di futuro Titolare del certificato, i seguenti impegni:

[30] Punto 4.5.2 della [17065].
[31] Articolo 40, paragrafo 2 dell'[EUCC].

- garanzia che i prodotti TIC venduti facendo riferimento al certificato EUCC siano esattamente identici al prodotto TIC oggetto della certificazione;
- rispetto delle norme di utilizzo del marchio e dell'etichetta stabilite per il certificato EUCC[32];

Inoltre, il Titolare del certificato si impegna a:

- collaborare con l'OCSI nel monitoraggio della conformità dei certificati di cui è titolare e realizzare le eventuali misure correttive richieste dall'OCSI in relazione a prodotti TIC certificati a seguito di non conformità rilevate;
- non utilizzare il logo OCSI in maniera difforme rispetto alle regole stabilite dall'Agenzia (rif. sezione 11);
- accettare l'eventuale esibizione della documentazione di valutazione del Committente per la conduzione di visite ispettive di accreditamento dell'OCSI ai sensi dell'articolo 60, paragrafo 2 del [CSA] con le modalità descritte in sezione 10.1;
- assicurare che il prodotto TIC o il profilo di protezione, una volta emesso il certificato, continui a soddisfare i requisiti verificati durante l'attività di valutazione e comunicare all'OCSI l'eventuale notizia di vulnerabilità e gestirle opportunamente di cui venga a conoscenza o di non conformità del certificato[33];
- informare l'OCSI di eventuali modifiche che possano influenzare la capacità del Titolare del certificato di soddisfare i requisiti di certificazione (ad es. stato giuridico del Titolare del certificato, modifiche al prodotto o al metodo di produzione, al Sistema di Gestione per la Qualità) senza indugio, in modo da consentire all'OCSI di attivare un processo di verifica;
- nei rapporti con gli utilizzatori, non deve rappresentare informazioni, materiale pubblicitario o pubblicazioni ingannevoli, gli obblighi informativi da parte del Titolare del certificato sono stabiliti dall'[EUCC].[34]

In caso di mancato rispetto di tali obblighi l'OCSI si riserva la possibilità di sospendere o revocare certificati.

10.3. Impegni dell'LVS

Nell'ambito di un processo di certificazione l'OCSI si avvale di un laboratorio per la valutazione della sicurezza (LVS) per l'esecuzione dell'attività di valutazione scelto dal

[32] In conformità dell'articolo 11 dell'[EUCC].
[33] I capi V e VI dell'[EUCC] individuano gli obblighi di gestione delle vulnerabilità e non conformità da parte di tutti i soggetti interessati nei relativi processi, incluso il Titolare del certificato.
[34] L'articolo 41 dell'[EUCC] individua obblighi di pubblicazione delle informazioni sul certificato per gli utenti.

Committente dall'elenco degli LVS abilitati dall'OCSI pubblicato sul sito web dell'ACN. A tal fine l'LVS accede alla documentazione e alle ulteriori evidenze prodotte dal Committente come richiesto dai Criteri ([CC 1,2,3,4,5]) e relativa metodologia di valutazione ([CEM]) oltreché ad eventuali ulteriori informazioni connesse al prodotto da valutare negli incontri e nelle comunicazioni tra Committente ed LVS.

In virtù dell'accreditamento ricevuto dall'organismo nazionale di accreditamento, un LVS ha le capacità, gli strumenti ed è organizzato in modo tale da poter proteggere adeguatamente le informazioni acquisite sui prodotti valutati.

Attraverso un accordo con il Committente, l'LVS si impegna a non divulgare le informazioni acquisite e a proteggerle adeguatamente.

L'LVS è tenuto a mantenere le evidenze alla base delle valutazioni effettuate assicurando che le proprie registrazioni siano conservate per almeno 5 anni dall'emissione del certificato.[35]

L'LVS si impegna a prestare eventuali attività di assistenza o formazione ad un Committente, garantendo separazione ed indipendenza con attività di valutazione di prodotti per lo stesso Committente. In particolare, nell'ambito di una valutazione di un prodotto è richiesto ad un LVS di dichiarare esplicitamente l'impiego di personale abilitato come valutatore dall'OCSI in eventuali attività di assistenza o formazione già prestate o in corso con il Committente. Al personale dell'LVS che eventualmente effettui attività di assistenza o formazione ad un Committente non è consentito svolgere attività di valutazione di prodotti che coinvolgano il medesimo Committente per almeno due anni.

È facoltà del Titolare del certificato richiedere all'LVS che ha effettuato la valutazione di incaricare nuovamente l'LVS per lo svolgimento di un processo di analisi di vulnerabilità volontaria per il prodotto specifico certificato per garantire nel tempo il mantenimento del livello di garanzia attestato con l'emissione del certificato iniziale.

LVS accetta l'eventuale esibizione della documentazione di valutazione dell'LVS per la conduzione di visite ispettive di accreditamento dell'OCSI ai sensi dell'articolo 60, paragrafo 2 del [CSA] con le modalità descritte in sezione 10.1.

[35] Articolo 40, paragrafo 2 dell'[EUCC].

11. Il marchio OCSI

Il marchio OCSI è un elemento grafico riferibile all'Organismo di Certificazione della Sicurezza Informatica, il quale opera come organismo di certificazione dell'Agenzia per la cybersicurezza nazionale (ACN), tra l'altro, ai sensi del regolamento europeo sulla cybersicurezza ([CSA]), così come disposto dal Decreto Legislativo 3 agosto 2022 , n. 123 ([DLGS]).

Il marchio riporta la scritta OCSI, in caratteri stilizzati, con la prima lettera parzialmente integrata in un quadrato traslucido di colore giallo, a simboleggiare un lucchetto. Immediatamente sotto alla scritta stilizzata è riportato per esteso il nominativo dell'organismo ("Organismo di Certificazione della Sicurezza Informatica"). Il marchio è riportato di seguito:

Organismo di Certificazione della Sicurezza Informatica

Nell'esercizio delle proprie funzioni di Organismo di certificazione, ACN garantisce l'uso del marchio OCSI a documenti relativi alla certificazione di prodotti per i quali sia stato formalmente condotto un processo certificazione/accertamento.

L'uso del marchio è previsto anche sulla documentazione afferente all'abilitazione di laboratori ai sensi del [DLGS].

Il marchio OCSI è riconducibile allo stesso Organismo e all'Agenzia per la cybersicurezza nazionale, che ne detiene i diritti di utilizzo, conformemente ai requisiti di cui alle sezioni 11.1 e 11.2. L'Agenzia per la cybersicurezza nazionale effettua inoltre attività di sorveglianza sull'utilizzo del marchio OCSI come descritto nella sezione 11.3.

11.1. Elementi grafici e dimensioni

Il marchio OCSI è impiegabile nell'unica versione illustrata nella presente procedura, composta da sfondo bianco e scritta nera.

La componente grafica colorata in giallo corrisponde alle seguenti codifiche cromatiche:

- HEX #FDDC39
- RGB 253, 220, 57
- CMYK 0%, 13%, 77%, 1%

Larghezza minima consentita: 3 cm

11.2. Condizioni di impiego

Ogni riproduzione del marchio OCSI deve rispettare i requisiti inclusi nella sezione 11.1.

L'uso del marchio OCSI è autorizzato esclusivamente alle condizioni della presente sezione, che i Titolari dei certificati, gli Sviluppatori e gli LVS si impegnano a rispettare.

Il marchio OCSI può essere applicato ai seguenti documenti solo da ACN :

- certificati rilasciati da OCSI;
- rapporti di certificazione;
- rapporti di mantenimento;
- rapporti di sorveglianza;
- documentazione dell'OCSI afferente al proprio sistema di gestione;
- contenuti del sito web dell'ACN;
- ogni documento collegato ai precedenti.

ACN garantisce il diritto all'uso del marchio OCSI nelle seguenti circostanze:

1. uso del marchio OCSI da parte dei Committenti, degli Sviluppatori e dei Titolari dei certificati su documentazione tecnica correlata al prodotto certificato e sul prodotto stesso, alle seguenti condizioni:
   (a) solo la versione certificata può essere associata al marchio OCSI;
   (b) un prodotto sottoposto a vigilanza, il cui certificato è sospeso, non può essere associato al marchio OCSI;
   (c) se diversi prodotti o parti di essi, o diverse versioni di prodotti appaiono sulla documentazione per gli utenti messa a disposizione dal Committente, Sviluppatore o Titolare del certificato, il marchio deve essere riferito chiaramente e in modo inequivocabile solo al prodotto nella versione certificata;
2. uso del marchio OCSI all'interno di comunicazioni pubbliche da parte di un soggetto diverso da ACN, ad esempio LVS o Titolare del certificato, alle seguenti condizioni; la comunicazione che utilizza il marchio OCSI è redatta dal soggetto in coordinamento con l'area comunicazione di ACN, secondo il seguente flusso:

(a) invio alla Divisione Comunicazione di ACN (comunicazione@acn.gov.it) di una manifestazione di interesse a realizzare una comunicazione pubblica con utilizzo del marchio OCSI;

(b) invio al medesimo indirizzo e-mail di una bozza di comunicazione pubblica per la verifica e il coordinamento dei contenuti;

(c) finalizzazione della comunicazione e invio al citato indirizzo e-mail del documento in duplice formato (.docx e .pdf), unitamente a tempistiche per la pubblicazione, destinatari della comunicazione e canali di divulgazione;

(d) eventuale nulla osta di ACN al rilancio della comunicazione sui propri canali.

Ogni impiego differente del marchio OCSI deve essere preventivamente autorizzato da ACN. Qualsiasi impiego non rientrante nelle condizioni descritte e non preventivamente autorizzato è da considerarsi abusivo.

11.3. Sorveglianza e azioni in caso di violazioni

ACN si riserva di monitorare l'impiego non autorizzato del marchio OCSI.

Ogni utilizzatore (ad esempio Titolare di un certificato o LVS) è responsabile di impieghi non autorizzati del marchio OCSI. ACN si riserva di far valere il diritto all'utilizzo legittimo e autorizzato del marchio OCSI attraverso le seguenti azioni:

- la richiesta di azioni correttive all'utilizzatore entro un lasso temporale definito da ACN;
- la sospensione o revoca dell'autorizzazione all'impiego del marchio OCSI per l'utilizzatore;
- la sospensione o revoca del provvedimento di abilitazione dell'LVS;
- la sospensione o revoca del certificato EUCC emesso;
- la segnalazione all'Ente di accreditamento nazionale di eventuali violazioni all'uso del marchio OCSI che possano condizionare il soddisfacimento dei requisiti di accreditamento;
- azioni legali da parte di ACN.

12. Reclami e ricorsi

L'operatività dell'OCSI prevede procedure per la risoluzione extragiudiziale delle controversie eventualmente insorte in ordine alle attività di valutazione e certificazione svolte secondo l'EUCC, nel rispetto dei principi di imparzialità, trasparenza, efficacia ed equità della procedura, nonché nel rispetto del principio del contraddittorio.

Tutte le segnalazioni, reclami o ricorsi rivolti all'OCSI dovranno essere inoltrati attraverso l'indirizzo PEC ocsi@pec.acn.gov.it.

Nei reclami dovrà essere chiaramente specificato l'oggetto cui si riferisce il reclamo presentato, le ragioni del reclamo ed eventuali azioni risolutive richieste all'OCSI, allegando tutta la documentazione ritenuta necessaria. L'OCSI, al momento della ricezione del reclamo da riscontro di ricezione al reclamante. Entro trenta giorni lavorativi dal ricevimento del reclamo, comunica l'esito dell'esame dello stesso. Ove rilevi la necessità di azioni correttive, nella stessa risposta comunica le modalità che saranno adottate per la risoluzione del problema segnalato.

Per richiedere all'OCSI l'annullamento di un provvedimento è possibile inviare una richiesta di riesame in autotutela ai sensi dell'art. 21-nonies della legge 7 agosto 1990, n. 241. Valutate le motivazioni esposte, sussistendo ragioni di interesse pubblico e tenendo conto degli interessi del richiedente e di eventuali controinteressati, l'OCSI può annullare il provvedimento.

Infine, contro un provvedimento dell'OCSI è esperibile ricorso al TAR del Lazio nel termine di 60 giorni o, in alternativa, ricorso straordinario al Presidente della Repubblica nel termine di 120 giorni, decorrenti dalla data di notifica dell'atto o da quando l'interessato ne abbia avuto piena conoscenza.

13. Monitoraggio e revoca dei certificati

Con l'accordo di certificazione il Titolare del certificato (Rif. § 10.2) si impegna ad assicurare che il prodotto continui a soddisfare i requisiti verificati durante l'attività di valutazione e a comunicare immediatamente all'OCSI eventuali vulnerabilità del prodotto o non conformità del certificato di cui venga a conoscenza.

Nel caso in cui la notizia di vulnerabilità o non conformità sia disponibile prima all'OCSI, esso procederà ad informare il Titolare del Certificato. L'OCSI può venire a conoscenza di vulnerabilità e di altre violazioni nell'utilizzo del certificato e dei relativi marchi e loghi da parte del Titolare del certificato, tramite fonti pubbliche, segnalazioni inoltrate alla casella di posta elettronica certificata ocsi@pec.acn.gov.it o tramite altri canali, incluse le informazioni acquisite tramite il CSIRT Italia.

Le modalità per il monitoraggio delle non conformità e delle vulnerabilità ed eventuali successive sospensioni, riduzioni di ambito e revoca dei certificati sono dettagliate nelle seguenti sezioni dell'EUCC:

- CAPO V - Monitoraggio, non conformità e non compliance
- CAPO VI - Gestione e divulgazione delle vulnerabilità
- ALLEGATO IV - Continuità dell'affidabilità e riesame dei certificati

Inoltre, un certificato è revocato in caso di violazione dell'accordo di certificazione riguardo le modalità di utilizzo del certificato e dei relativi marchi e loghi se, una volta accertata la violazione dalla OCSI, il Titolare del certificato non applica le azioni correttive comunicate da OCSI entro i termini stabiliti dall'OCSI.

14. 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	La persona fisica, giuridica o altro organismo o associazione che commissiona e sostiene gli oneri economici della

certificato EUCC)	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][36]. 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.
Oggetto della Valutazione (ODV)	un prodotto TIC o una sua parte, o un profilo di protezione come parte di un processo TIC, sottoposto a valutazione di cibersicurezza allo scopo di ricevere la certificazione EUCC.
Traguardo di Sicurezza (TdS)	Una dichiarazione dei requisiti di sicurezza dipendenti dall'implementazione per uno specifico prodotto TIC.
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.
Rapporto di Attività	Il documento che l'LVS invia all'OC, nel quale sono indicati

[36] 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).

	dettagliatamente i risultati raggiunti e le attività svolte dal laboratorio stesso durante le varie fasi della valutazione
Rapporto di Osservazione	Il rapporto dell'LVS finalizzato alla richiesta di chiarimenti o modifiche relativamente a delle evidenze di valutazione.
Rapporto Finale di Valutazione	Il rapporto dell'LVS, contenente i risultati della valutazione, che costituisce la base per la certificazione dell'ODV, profilo di protezione o traguardo di sicurezza.
Certificato	L'attestazione da parte dell'OC che conferma i risultati della valutazione e la corretta applicazione dei criteri adottati e della relativa metodologia
Rapporto di Certificazione	Il documento emesso dall'organismo di certificazione, che accompagna il certificato, specificandone l'ambito e le condizioni di validità.
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.
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.
Livello (di garanzia) di valutazione	Uno dei sette pacchetti di garanzia ben formati (da EAL1 a EAL7) definito nella sezione 4.4 di [CC5].
Funzioni di Sicurezza	Le contromisure 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 l'OC dell'Agenzia nel rilascio dei certificati di cybersicurezza.
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.
Addendum di mantenimento	Una nota di dominio pubblico che integra il certificato di un ODV. L'addendum di mantenimento elenca le versioni dell'ODV mantenute. Non implica l'emissione di un certificato aggiornato.
Rapporto di Analisi di Impatto (RAI)	Il rapporto che relaziona i risultati dell'analisi dell'impatto delle modifiche apportate all'ODV certificato. Il RAI viene generato dal Committente (o Sviluppatore) che richiede di aggiornare l'addendum di mantenimento per un ODV.
Rapporto di mantenimento	Il rapporto pubblico che descrive le modifiche apportate all'ODV certificato accettate e certificate nell'ambito del processo di mantenimento.
Rapporto di aggiornamento dell'analisi di vulnerabilità	Il rapporto che identifica la versione dell'ODV, la lista di guide operative applicabili e il livello di garanzia AVA_VAN raggiunto dall'ODV come esito dell'aggiornamento dell'analisi di vulnerabilità. Può essere reso pubblico in base alle scelte del committente della valutazione.
Livello di garanzia di riferimento	È costituito dall'insieme delle attività svolte dal valutatore e dal Committente (o Sviluppatore) che si concludono con la certificazione dell'ODV, registrate o inviate in forma di evidenza.
Evidenze dello Sviluppatore	Sono tutte le evidenze messe a disposizione dei Valutatori a supporto di una valutazione dell'ODV (anche nell'ambito di un processo di mantenimento del certificato) da parte del Committente (o Sviluppatore).
Mantenimento	Il processo utilizzato per riconoscere che una o più modifiche apportate all'ODV certificato (o ad aspetti del suo ambiente di sviluppo o l'aggiunta di un componente della

	famiglia ALC_FLR) non abbiano un impatto negativo sulle garanzie offerte dalle funzioni di sicurezza dell'ODV.
Rivalutazione	Il processo attivato nei casi in cui le modifiche apportate ad un ODV certificato (o ad altre misure di garanzia) richiedano di eseguire nuovamente le attività di valutazione per definire un nuovo livello di garanzia di riferimento. Il processo di rivalutazione, per quanto possibile, riutilizza i risultati della precedente valutazione dell'ODV certificato.
Aggiornamento dell'analisi di vulnerabilità di un ODV certificato	Il processo di aggiornamento dell'analisi di vulnerabilità della valutazione e certificazione iniziale del prodotto, eseguita allo stesso livello di garanzia richiesto dal TDS della certificazione originaria, incluse, ove necessario, prove di intrusione. Può essere eseguito in modo asincrono o su base periodica. Può essere considerato un caso particolare di rivalutazione nei casi in cui non è cambiato l'ODV ma si ritiene necessario valutare le modifiche rispetto al panorama di minacce e di attacchi possibili per l'ODV al fine di confermare che le sue funzioni mantengano lo stesso livello di resistenza agli attacchi verificato durante la certificazione originaria.
Ambiente di sviluppo	È l'ambiente che racchiude tutte le misure e procedure relative allo sviluppo, alla consegna, alla messa in esercizio e alla correzione di difetti dell'ODV. Comprende tutti i concetti presi in esame dai requisiti di garanzia dalla classe ALC, insieme alla famiglia AGD_PRE.
Sottoinsieme di attività di valutazione	Un sottoinsieme di attività di valutazione è applicabile laddove modifiche all'ODV e/o all'ambiente di sviluppo siano classificabili come cambiamenti minori e siano riferite in modo specifico ad azioni di valutazione da condurre. Un Laboratorio di Valutazione della Sicurezza Informatica (LVS) identifica i componenti di garanzia su cui hanno impatto le modifiche all'ambiente di sviluppo e riesegue le attività di valutazione unicamente per tali componenti di garanzia alla luce delle modifiche apportate, producendo un Rapporto Finale di Valutazione (RFV) parziale. Un sottoinsieme delle attività di valutazione copre anche le azioni di valutazione da eseguire a seguito dell'aggiunta di un componente di garanzia della famiglia ALC_FLR al livello di garanzia di riferimento.
Rapporto Finale di Valutazione Parziale	È il risultato prodotto dal completamento del sottoinsieme di attività di valutazione. Viene creato dall'LVS che ha eseguito il sottoinsieme delle attività di valutazione e fornisce, per i componenti di garanzia su cui le modifiche hanno un impatto, un livello di dettaglio commisurato alle sezioni corrispondenti del rapporto finale di valutazione per l'ODV certificato.

15. Oneri dovuti all'OCSI

Le attività dell'OC richieste da un Committente o LVS sono svolte a titolo oneroso dall'OC sulla base delle tariffe stabilite dal decreto ([DM)], nelle more dell'adozione del decreto di cui all'art. 13, comma 1, del [DLGS]. In particolare, all'articoli 1 del [DM] si individuano come attività da rimborsare a titolo oneroso all'OC:

- le attività di verifica di competenza per gli LVS,
- la supervisione dei processi di valutazione ed emissione dei certificati di cybersicurezza.

L'articolo 3 dello stesso decreto individua per le attività dell'OC i seguenti elementi di costo per calcolare il rimborso dovuto all'OC:

- *costo del personale dell'OC impiegato* da calcolarsi in base ad una tariffa oraria pari a 60 euro l'ora,
- *costi di missioni* eventualmente sostenuti per le attività dell'OC,
- *spese generali* del 20% da applicarsi alle suddette componenti di costo.

Sulla base dei suddetti elementi, l'OC, in risposta ad una istanza di abilitazione per un LVS oppure ad una istanza di certificazione di un prodotto o profilo di protezione, emette un preventivo con il calcolo dei costi da rimborsare per accettazione da parte del richiedente.

15.1. Impegno richiesto all'OCSI per le attività di abilitazione

In Tabella 2 si riportano i valori di riferimento in termini di ore di impegno stimate per l'abilitazione di un LVS comprensive degli esami di abilitazione dei singoli valutatori da integrare assieme ai valori di riferimento per l'integrazione di valutatori addizionali successivamente all'abilitazione.

Denominazione attività	Riferimento	Ore
Abilitazione LVS	LG2 – sezione 6.5	7,5 OP fissi + 2,5 ore per l'esame di ciascun candidato valutatore da integrare.
Esami di integrazione valutatori addizionali successivi all'abilitazione dell'LVS	LG2 – sezione 6.7	2,5 ore per l'esame di ciascun candidato valutatore da integrare

Tabella 2 – Ore per le attività di abilitazione

15.2. Impegno richiesto all'OCSI per le attività di certificazione

In Tabella 3 sono riportati invece i valori di riferimento per i procedimenti di certificazione che richiedono l'emissione di un certificato e/o di un rapporto, i costi del personale sono calcolati in base ad una stima dei giorni/persona (7,5 ore al giorno pari a 450 euro giornaliere) necessari per lo svolgimento dell'attività richiesta all'OC. Di seguito si forniscono le stime di giorni/persona necessari per le diverse tipologie di attività eseguite dall'OC.

Denominazione attività	Riferimento	Giorni/persona (G/P)
Certificazione standard	LG3 – sezioni dalla 7 alla 11	10 G/P fissi + 8% dei G/P stimati dall'LVS nel PDV
Mantenimento	LG3 – sezione 12.3	5 G/P fissi + eventuale 8% dei G/P stimati dall'LVS nel PDV se LVS impiegato.
Aggiornamento dell'analisi di vulnerabilità dell'ODV	LG3 – sezione 12.6	5 G/P fissi + 8% dei G/P stimati dall'LVS nel PDV se LVS impiegato.

Tabella 3 – Giorni/persona (G/P) per le attività di certificazione

16. Riferimenti

[ACCR] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.

[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.

[CCRA] "Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security", July 2014

[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»).

[CVCN] Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54, Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[DD] Decreto del Direttore Generale dell'Agenzia per la cybersicurezza nazionale, "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".

[DLGS] Decreto Legislativo 3 agosto 2022 , n. 123, "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".

[DPCM1] Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 (c.d. DPCM 1) - Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[DPCM2] Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81 (c.d. DPCM 2) - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.

[DPCM3] Decreto del Presidente del Consiglio dei ministri 15 giugno 2021 (c.d. DPCM 3) - Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[DPCM4] Decreto del Presidente del Consiglio dei ministri 18 maggio 2022, n. 92 (c.d. DPCM 4) -Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[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).

[LG1-CA] Linea Guida NCCA N. 1– Attività di vigilanza nazionale e autorizzazione per il sistema EUCC (art. 5, art. 8 cc. 3-4 d.lgs. 123/2022).

[LG1-OC] Linea Guida OCSI N. 1– Sistema EUCC: le caratteristiche generali e gli attori del processo di certificazione dell'OCSI (art. 4 c. 2, art. 11 cc. 3-4 d.lgs. 123/2022).

[LG2-OC] Linea Guida OCSI N. 2 – Abilitazione dei laboratori per la valutazione della sicurezza per il sistema EUCC (art. 8 c. 4 d.lgs. 123/2022).

[LG3-OC] Linea Guida OCSI N. 3 – Attività di valutazione ed emissione dei certificati per il sistema EUCC (art. 6 d.lgs. 123/2022).

[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".

[TRNSF] Decreto del Presidente del Consiglio dei ministri 15 giugno 2022 - "Definizione dei termini e delle modalità del trasferimento di funzioni, beni strumentali e documentazione dal Ministero dello sviluppo economico all'Agenzia per la cybersicurezza nazionale.

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

[SOA-OC] EUCC Scheme state-of-the-art document 'Accreditation of CBs for the EUCC', version 1.6b.

[UCSE] Decreto del Presidente del Consiglio dei ministri 11 aprile 2002 - Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato.

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

[17065] UNI/CEI EN ISO/IEC 17065, "Valutazione della conformità: requisiti per organismi che certificano prodotti, processi e servizi", 2012