the information security provider

Le certificazioni di sicurezza dei prodotti ICT: Common Criteria e CEM (Common Evaluation Methodology)

Roma, 26 Marzo 2024

Garibaldi Conte

Agenda

- DEFINIZIONI E CONCETTI BASE
- I PRINCIPALI STANDARD DI RIFERIMENTO
- LO STANDARD COMMON CRITERIA
- CONCLUSIONI

Definizioni e Concetti Base

Cosa è la certificazione di un prodotto ICT

"la certificazione è il risultato di una attività di valutazione eseguita da una terza parte indipendente (organismo di certificazione) sulla base di standards e metodologie riconosciute, e per le quali l'organismo di certificazione è stato preventivamente accreditato da un ente di accreditamento specifico"

Contesto Normativo

1. **Norma di riferimento**: individua «cosa» necessita di certificazione e in che modo.
2. **Schema di certificazione**: raccoglie e definisce l'insieme delle regole che devono essere utilizzate durante il processo di applicazione della norma di riferimento.
3. **Gestore dello schema**: entità super-partes locale che garantisce la corretta applicazione dello schema da parte di tutti i soggetti interessati. Ha anche il compito di negoziare accordi di mutuo riconoscimento con gli analoghi gestori in altri paesi.
4. **Il garante dello schema**: entità super-partes (spesso internazionale) che si fa carico di risolvere le controversie che coinvolgono il gestore dello schema.

Soggetti Coinvolti

1. **Ente Accreditatore**: si occupa dell'accreditamento iniziale dei Certificatori e/o dei Valutatori (o dei Laboratori di Valutazione) e del controllo periodico degli stessi.
2. **Certificatore**: si occupa dell'emissione dei certificati sulla base dei risultati ottenuti dai valutatori (o dai laboratori di valutazione) accreditati e assicura la corretta gestione dei certificati emessi.
3. **Valutatore**: esegue la valutazione di sicurezza; si occupa perciò di redigere la documentazione, ispezionare, testare l'oggetto della certificazione in modo da poter fornire al certificatore (in caso di verdetto di valutazione positivo) gli elementi necessari all'emissione dei certificati.
4. **Cliente**: costituisce l'owner dell'oggetto della valutazione/certificazione. Ingaggia direttamente un valutatore con la volontà di portare a certificazione un determinato prodotto
5. **Oggetto della Valutazione (e della certificazione)**: un prodotto che, unitamente alla sua documentazione, è sottoposto al processo di valutazione secondo i criteri e la metodologia adottati.
6. **Fruitore della certificazione**: rappresenta l'entità che potrà avvalersi della certificazione; può essere lo stesso Cliente, un fornitore o l'utente finale.

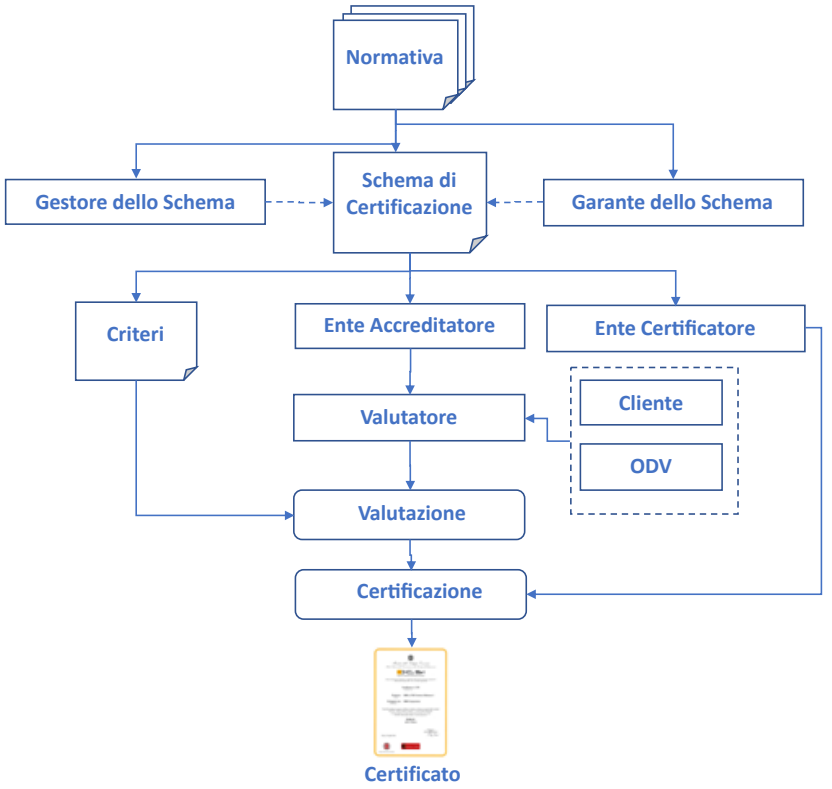
Certificazione di Sicurezza

"attività che in maniera probabilistica consente di rispondere circa le capacità di un sistema (assurance) di rispettare le specifiche di sicurezza che sono state stabilite in relazione al suo utilizzo/funzionamento."

Definizioni e Concetti Base

Certificazione: Caratteristiche

1. **Imparzialità**: l'accreditatore, il certificatore e il valutatore devono essere terza parte indipendente rispetto al fornitore/titolare del prodotto da certificare. In altre parole, deve essere possibile dimostrare che essi non abbiano interessi commerciali o finanziari legati all'esito della certificazione.
2. **Oggettività**: la valutazione deve essere condotta cercando di motivare (ove possibile) ogni affermazione con evidenze sperimentali. In altre parole, bisogna limitare il più possibile le considerazioni soggettive in modo da rendere la certificazione il più oggettiva possibile.
3. **Ripetibilità**: la valutazione deve essere condotta in modo da dimostrare che se effettuata una seconda volta sullo stesso oggetto, con gli stessi requisiti di sicurezza e dallo stesso valutatore, porterebbe ai medesimi risultati.
4. **Riproducibilità**: la valutazione deve essere condotta in modo da dimostrare che se effettuata una seconda volta sullo stesso oggetto, con gli stessi requisiti di sicurezza ma da un valutatore diverso porterebbe ai medesimi risultati.

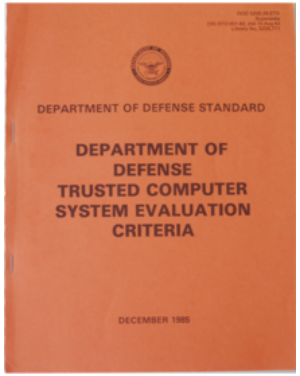


I PRINCIPALI STANDARD DI RIFERIMENTO

Trusted Computer Security Evaluation Criteria (TCSEC) - Orange Book

Trusted Computer Security Evaluation Criteria sono stati sviluppati dal **DoD americano nel 1985** e sono rimasti in uso fino a dicembre del 2000, sostituiti dai CC. Danno molto enfasi ai **requirement di tipo militare** e poca alle caratteristiche richieste in ambito commerciale. Più conosciuto con il nome di Orange Book, il documento introduce importanti ed innovativi concetti, che poi saranno ripresi da quasi tutti i moderni standard (inclusi i CC):

- **Valutazione di terza parte** (per TCSEC l'organismo era governativo)
- **Assurance**, ovvero la capacità del prodotto di soddisfare determinati criteri di sicurezza
- **Valutazione probabilistica**, non assoluta



I criteri di valutazione prevedono i seguenti argomenti:

- Security Policy
- Identification
- Labels
- Documentations
- Accountability
- Life Cycle Assurance
- Continous Protection

Livelli di Assurance

D: **Minimal Protection** - Non soddisfa i requisiti

C: **Discretionary Protection** - Discretionaty Access Control

C1: Discretionaty Security Protection

C2: Controlled Access Protection

B: **Mandatory Protection** - Mandatory Access Control, basato sul Bell-LaPadula.

B1: Labeled Security

B2: Structured Protection B3: Security Domains

A: **Verified Protection** - Analogo a B3, ma i controlli eseguiti sono più formali

Rainbow Series : Poichè l'Orange Book comprendeva la valutazione esclusivamente dei computer, il DoD decise di emettere altri documenti per coprire gli altri argomenti di sicurezza. Ognuno di essi aveva una copertina di un colore diverso (da qui l'arcobaleno)

I PRINCIPALI STANDARD DI RIFERIMENTO

Information Technology Security Evaluation (ITSEC)

Information Technology Security Evaluation Criteria, sviluppato in **ambito europeo da Francia, Germania, Regno Unito e Olanda**, è stato pubblicato in versione definitiva nel **giugno del 1991**, raccogliendo da subito il pieno consenso della Commissione della Comunità Europea. Per alcuni versi, ITSEC si può considerare come la risposta europea all'Orange Book (TCSEC).

ITSEC è da molti considerato il **progenitore dei moderni criteri di valutazione per prodotti e sistemi IT**; in effetti questo standard è stato il primo ad introdurre dei concetti di base, poi largamente riutilizzati, tra i quali:

- la considerazione per le **misure di sicurezza** non solo di carattere tecnico, ma anche organizzativo, ambientale (intendendo le caratteristiche di sicurezza dell'ambiente in cui il prodotto/sistema deve operare) e fisico;
- la possibilità di valutare gli aspetti di sicurezza di prodotti **hardware, software o firmware**, indistintamente;
- l'identificazione univoca del promotore della valutazione (denominato "**sponsor**");
- l'identificazione di enti preposti alla valutazione, formalmente accreditati per condurre le attività (nello Schema Nazionale sono i **Centri di Valutazione**, o CeVa e i **Laboratori per la Valutazione della Sicurezza**, o LVS);
- l'identificazione univoca dell'oggetto della valutazione (TOE, **Target Of Evaluation**, o in italiano ODV, Oggetto Della Valutazione);
- la definizione del **Security Target** (ST) (in italiano Traguardo di Sicurezza, TdS);
- la presenza di livelli di severità della valutazione flessibili (**Assurance Level**, AL).

Lo standard valuta 2 attributi fondamentali:

- Functionality: (F1 - F10)
- Assurance: (E0 - E6)

Per la sua **maggiore flessibilità** rispetto agli altri standard (e soprattutto a TCSEC) e per la sua natura Europea, ITSEC è stato accolto con largo favore ed utilizzato, negli anni 90, per la valutazione di sistemi e prodotti legati principalmente **all'ambito militare**. ITSEC è stato utilizzato spesso per la valutazione di sistemi e prodotti di **firma digitale**, nonostante il costo (in termini sia economici che di tempo) della valutazione non fosse assolutamente esiguo.

LO STANDARD COMMON CRITERIA

La Storia

- Gli **standard Common Criteria** (Standard ISO 15408 — Information technology — Security techniques — Evaluation criteria for IT security), hanno origine da un **progetto internazionale iniziato nel 1993 e durato circa 5 anni** che coinvolgeva **NIST e NSA per gli USA** e svariate organizzazioni per la sicurezza in **Canada, Francia, Germania, Olanda e Regno Unito**. Per lo sviluppo dei criteri fu istituito un gruppo di lavoro (anch'esso internazionale) denominato **Common Criteria Editorial Board (CCEB)**.
- L'obiettivo era quello di sviluppare una comune metodologia per la valutazione della sicurezza nel mondo dell'Informatica che fosse applicabile in campo internazionale e **superasse i limiti degli standard al momento in vigore** (TCSEC, ITSEC, …).

LO STANDARD COMMON CRITERIA

Cosa sono

- Sono una metodologia per specificare e valutare la sicurezza informatica.
  - Permettono una **convalida formale** (ad esempio matematica) della sicurezza.
  - Dopo il superamento della valutazione viene rilasciato un certificato.
- Sono applicabili sia a **prodotti software che hardware**.
- Non specificano di cosa ha bisogno un cliente o quali funzionalità di sicurezza deve fornire un prodotto. I Common Criteria funzionano per **diverse esigenze e diverse tipologie di prodotti.**
- Non sono una metodologia di progettazione o sviluppo.
- Si tratta di una valutazione basata sulle evidenze.

I CC è uno standard internazionale e sono composti da:

- Part 1: Introduction and general model
- Part 2: Security functional requirements
- Part 3: Security assurance requirements
- CEM: CC evaluation methodology
- La versione corrente è: 3.1 Release 5 (emessa in aprile 2017)
- Sito Web (c.d. CC Portal):
- https://www.commoncriteriaportal.org/

- Il **14 novembre 2022** è stata approvata la **nuova versione dei CC (versione CC 2022 rev 1).**
- La versione **CC 3.1 Release 5** potrà essere utilizzata per le attività di valutazione **fino al 30 giugno 2024**

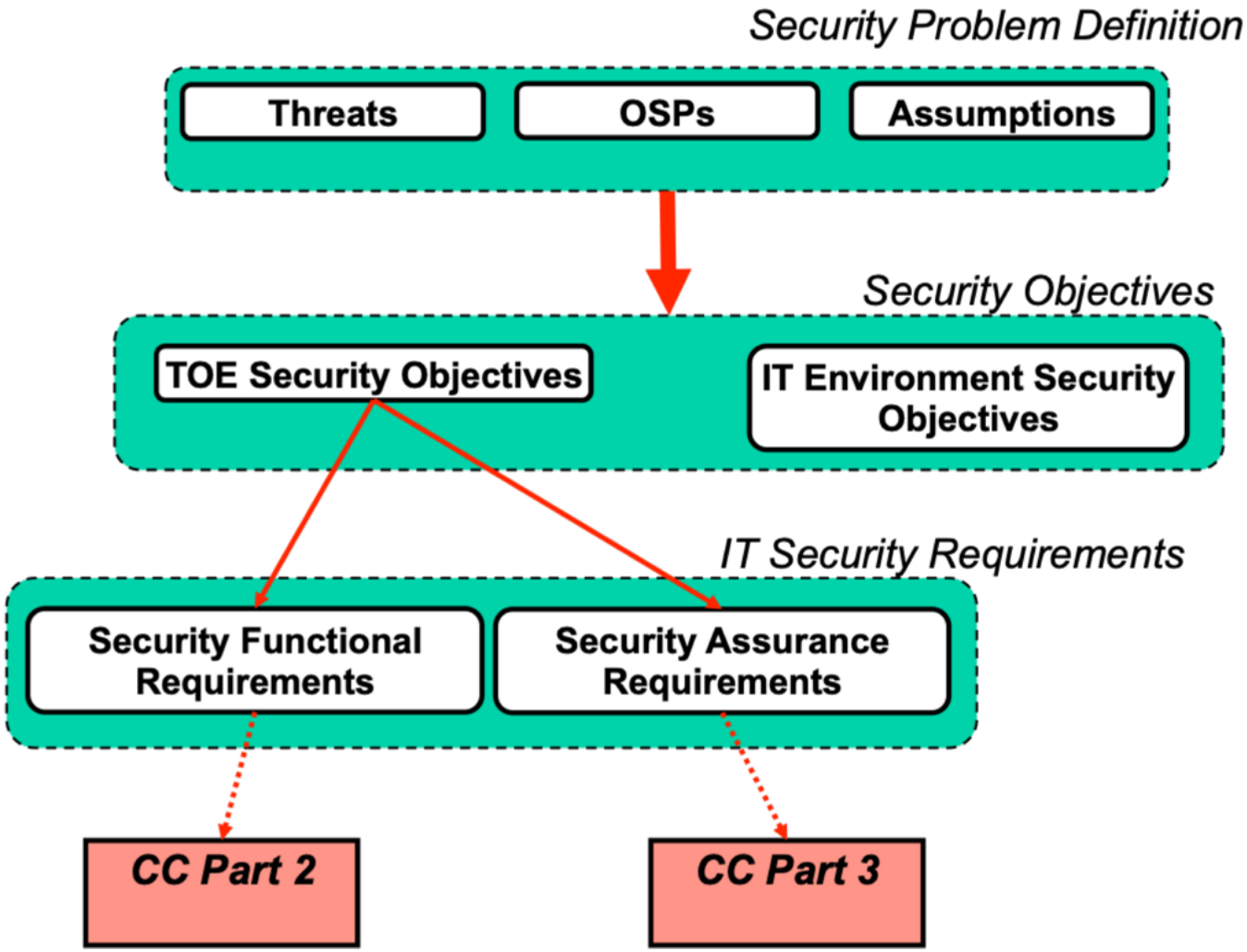
LO STANDARD COMMON CRITERIA

Terminologia

- **Target of Evaluation (TOE)** / Oggetto Della Valutazione (ODV)
  - *Il prodotto o il subset del prodotto da valutare (OS, applicazioni, DB, librarie, dispositivi di rete, dispositivi mobili,…)*
  - *Confine del TOE : Il confine che separa la parte che viene valutata (TOE) e la parte che non viene valutata (Ambiente Operativo - Operational Environment).*
- **Operational Environment (OE)**
  - *Componenti da cui il TOE dipende per funzionare*
  - *Se il TOE è un Server Application:*
    - *dipende come minimo da un Sistema Operativo e un hardware*
    - *Potrebbe dipendere da DB, LDAP, cloud, DNS, librerie di terze parti, ecc.*
    - *Potrebbe richiedere una GUI remota, web browser, CLI, ecc.*
- **Security Problem Definition**
  - *Minacce (le minacce che afferiscono al TOE)*
  - *Assumptions (le assumptions di sicurezza riguardo l'ambiente operativo (OE))*
  - *Policies di sicurezza dell'organizzazione (OSP) (le policies di sicurezza che l'organizzazione potrebbe dover applicare affinché il TOE funzioni in modo sicuro)*
- **Objectives**
  - *Obiettivi del TOE (gli obiettivi di sicurezza che il TOE intende raggiungere)*
  - *Obiettivi dell'ambiente operativo (OE) (gli obiettivi di sicurezza che l'ambiente deve soddisfare)*
- **Security Functional Requirements (SFRs)**
  - *Definiscono i requisiti di sicurezza applicati dall'ODV.*
  - *I requisiti sono indipendenti dal livello delle prove/assurance effettuate per la certificazione.*
- **Security Assurance Requirements (SARs)**
  - *Definiscono il livello di rigore e i test utilizzati per valutare i SFRs del TOE*
  - *I CC raggruppano SARs negli Evaluation Assurance Levels (EALs).*
  - *Il livello utilizzato per valutare il TOE sarà riportato sul certificato.*

LO STANDARD COMMON CRITERIA

Struttura



LO STANDARD COMMON CRITERIA

Il Security Target

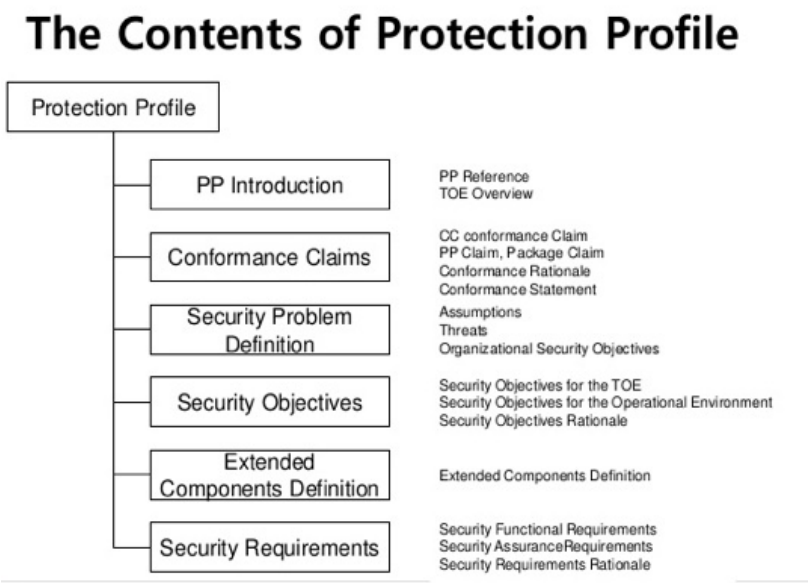
Il documento **Security Target** (ST) / Traguardo Di Sicurezza (TDS) descrive le dichiarazioni di valutazione del TOE, dell'OE e dei CC
Contiene:

- Panoramica sul TOE e sull'OE
- Dichiarazioni di conformità a EAL e/o PP/cPP (Protection Profile/collaborative Protection Profile).
- SPD (Security Problem Definition).
- Obiettivi del TOE e dell'OE.
- SFR (Security Functional Requirements).
- SAR (Security Assurance Requirements).
- TSS (TOE Summary Specification) : descrive in che modo il TOE soddisfa i requisiti.
- Richiesto per tutte le valutazioni Common Criteria.

LO STANDARD COMMON CRITERIA

I Protection Profile

- Il **Profilo di Protezione** è un documento, generalmente creato dal Cliente (utente o comunità di utenti) definisce un insieme di caratteristiche di garanzie e funzioni che identificano una particolare classe di un singolo prodotto/sistema o di una famiglia di prodotti/sistemi.
- Dal punto di vista del **fornitore/produttore del TOE** l'utilizzo di questo documento può essere duplice. Da un lato, esso può decidere di implementare e certificare prodotti che **rispettano le specifiche di sicurezza imposte da uno o più PP**. Dall'altro il documento può essere inteso come un **template per generare un nuovo PP** sulle basi dei requisiti di sicurezza espressi per la classe di prodotti, magari ampliandone lo spettro.
- Dal punto di vista **dell'utente**, invece, un PP può essere utilizzato come **criterio per selezionare il tipo particolare di prodotto che soddisfa maggiormente la sua particolare esigenza**, sulla base di quanto in esso espresso (requisiti di sicurezza).
- Dal punto di vista strutturale un **PP è per molti versi analogo ad un ST**, in particolare per quanto riguarda la descrizione dell'Ambiente di sicurezza del TOE, degli Obiettivi di sicurezza, dei Requisiti di sicurezza IT e le motivazioni legate a questi aspetti.
- Quello che invece **non è previsto** in un PP riguarda le **parti direttamente connesse con il TOE** (e solo con esso), come il sommario delle specifiche di questo, la conformità ad un eventuale altro PP e le motivazioni che dimostrano l'adeguatezza delle funzioni di sicurezza e garanzia che permettono di soddisfare i requisiti di sicurezza.
- I **due documenti, inoltre, potrebbero essere utilizzati congiuntamente**: un ST potrebbe essere dichiarato conforme ad un PP, ereditandone direttamente i requisiti funzionali e di garanzia. In questi casi è possibile solo fare riferimento al PP e dettagliare le eventuali differenze con questo.



LO STANDARD COMMON CRITERIA

Functional Classes (SFR)

- **FAU – Security Audit** : Generazione, memorizzazione, analisi, revisione, risposta di audit degli eventi di sicurezza.
- **FCO – Communication** : Verifica dell'origine (non ripudio).
- **FCS - Cryptographic support** : Gestione di chiavi e operazioni crittografiche.
- **FDP - User data protection** : Policies di controllo degli accessi, policies di controllo flussi di informazioni, data authentication, data export, protezione delle informazioni residuali, rollback, ecc.
- **FIA - Identification and authentication** : Identificazione, autenticazione, attributi degli user, robustezza password, failure handling dell'autenticazione, user-subject binding.
- **FMT - Security management** : Gestione delle funzionalità di sicurezza e attributi, ruoli e revocation.
- **FPR – Privacy** : Anonymity, pseudonymity, unlinkability, unobservatility
- **FPT - Protection of the TSF (TOE Security Functionality)** : Fail secure, export dei TSF data, trusted recovery, replay detection, time stamps, trasferimento dati interni all'ODV TSF, self test, ecc.
- **FRU - Resource utilisation** : Fault tolerance, priorità del servizio, allocazione delle risorse.
- **FTA - TOE access** : Session locking, ODV access banners, limitazione su sessioni concorrenti, creazione della sessione.
- **FTP - Trusted path/channels** : Trusted path, trusted channel

LO STANDARD COMMON CRITERIA

Assurance Classes (SAR)

- **ASE – Security Target Evaluation** : Verifica della idoneità delle specifiche di sicurezza.
- **ADV – Development** : Verifica della correttezza e completezza della documentazione progettuale e di realizzazione.
- **AGD – Guidance documents** : Verifica che i manuali siano appropriati per messa in opera sicura.
- **ALC – Life cycle support** : Verifica che l'ambiente di sviluppo fornisca misure di sicurezza sufficienti ed efficaci.
- **ATE – Tests** : Verifica che le funzioni di sicurezza dell'ODV funzionino come previsto.
- **AVA – Vulnerability assessment** : Verificare che non ci siano vulnerabilità sfruttabili.

LO STANDARD COMMON CRITERIA

Assurance Packages

- La tabella riassume il numero di componenti per ogni famiglia di ogni classe da verificare all'aumentare del livello di assurance da EAL1 a EAL7.
- Le aree grigie sono famiglie che possono essere usate, per esempio, per creare un livello di assurance aumentato (EALX+).

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

LO STANDARD COMMON CRITERIA

Evaluation Assurance Levels

Livello	Nome	TCSEC	ITSEC
EAL1	Functionally Tested		
EAL2	Structurally Tested	C1: Discretionary security protection	E1: Informal architectural design
EAL3	Methodically Tested & Checked	C2 — Controlled access protection	E2: E1 + informal detailed design & test documentation
EAL4	Methodically Designed, Tested & Reviewed	B1 - Labeled security protection	E3: E2 + Source code or hardware drawing & evidence of testing
EAL5	Semiformally Designed & Tested	B2 — Structured protection	E4: E3 + Semiformal architectural design & formal model of security policy
EAL6	Semiformally Verified Designed & Tested	B3 — Security domains	E5: E4 + Correspondence between detailed design & source code
EAL7	Formally Verified Designed & Tested	A1- Verified design	E6: E5 + Formal description & detailed architectural design

LO STANDARD COMMON CRITERIA

Utilizzo dello Standard

- Ognuna delle parti dei CC è studiata per esser utilizzata in modo distinto da tre tipologie di utenza, i **valutatori** (evaluators), gli **sviluppatori** (developers) e **consumatori** (consumers).

	Consumatori	Sviluppatori	Valutatori
Parte 1 *Introduction and general model*	Utilizzo a scopi informativi di base, come riferimento, o come guida per i PPs	Utilizzo a scopi informativi di base e come riferimento per lo sviluppo di requisiti e per la formulazione delle specifiche di sicurezza per i TOEs	Utilizzo a scopi informativi di base, come riferimento, o come guida per i PPs
Parte 2 *Security functional requirements*	Utilizzo come guida di riferimento per la redazione delle espressioni dei requisiti per le funzioni di sicurezza	Utilizzo come riferimento nell'interpretazione delle espressioni relative ai requisiti funzionali e nella redazione delle specifiche funzionali per i TOEs	Utilizzo come riferimento obbligatorio per l'espressione dei criteri di valutazione nella determinazione del corretto soddisfacimento da parte del TOE dei requisiti funzionali dichiarati.
Parte 3 *Securitu assurance requirements*	Utilizzo come guida nel determinare i livelli di assurance richiesti	Utilizzo come riferimento nell'interpretazione delle espressioni relative ai requisiti di assurance e nella determinazione di come i TOEs affrontino questi aspetti.	Utilizzo come riferimento obbligatorio per l'espressione dei criteri di valutazione nella determinazione dell'assurance del TOE e nella valutazione di TSs e PPs

LO STANDARD COMMON CRITERIA

Principali Accordi Internazionali - CCRA

- **Common Criteria Recognition Arrangement (CCRA)**
  - 30 Paesi membri (ad oggi)
  - 18 sono emittenti di certificati.
  - 12 sono utilizzatori di certificati.
  - Mutuo riconoscimento fino a EAL2 o fino a EAL4 per i cPP1.
  - I certificati restano pubblicati per 5 anni sul sito web CC Portal.
  - https://www.commoncriteriaportal.org/ccra/

(1): Collaborative Protection Profile: nome dato ai PP creati da International Technical Community (iTC) creati su specifici argomenti e riconosciuti dal CCRA

LO STANDARD COMMON CRITERIA

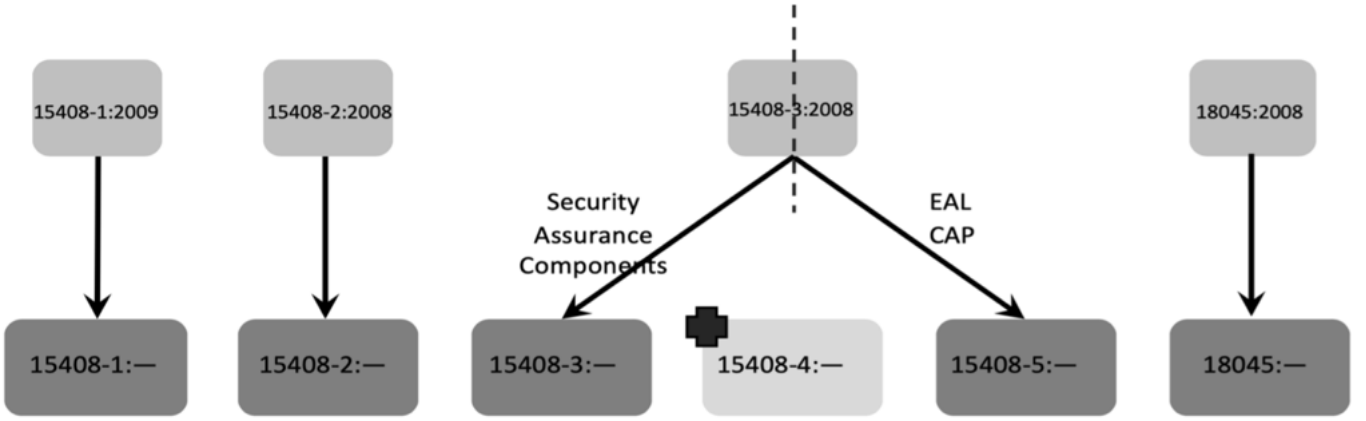
Principali Accordi Internazionali – SOG-IS

- **Senior Officials Group Information Systems Security** (SOGIS)
  - 17 Paesi Europei membri
  - https://www.sogis.org/
  - Mutuo Riconoscimento fino a CC EAL4
  - Livelli superiori possono essere riconosciuti in base ad accordi speciali.

Il SOG-IS è stato recepito nell'**EUCC** e viene superato alla **entrata in vigore** di quest'ultimo (**27 febbraio 2025**)

LO STANDARD COMMON CRITERIA

La versione CC:2022



Le principali modifiche introdotte nella nuova versione CC:2022 sono le seguenti:

- Lo standard è stato **ri-strutturato introducendo 2 parti nuove**: la 4 e la 5. La prima, completamente nuova, introduce i concetti inerenti i metodi di valutazione e le attività di valutazione, mentre la parte 5 eredita dalla parte 3 i pacchetti predefiniti dei requisiti di sicurezza introducendone dei nuovi.
- In tutto lo standard sono state introdotte delle **modifiche tecniche** e la **terminologia è stata rivista e aggiornata**.
- Sono stati introdotti **nuovi requisiti funzionali** e **nuovi requisiti di *assurance***.
- È stato introdotto il **concetto di *exact conformance*** che affianca quello di *Strict conformance* e *Demonstrable conformance* già presenti nella versione attuale.
- Sono stati introdotti i **PP *direct rationale*** (logica diretta) che affiancano i PP con basso livello di *assurance* (PP con livello di assurance pari a EAL-1).
- Sono state introdotte le **valutazioni multi-assurance** e le **valutazioni composite**.

LO STANDARD COMMON CRITERIA

La versione CC:2022

Vantaggi

- Valore aggiunto riconosciuto a livello internazionale
- Valutazione eseguita da una terza parte accreditata
- Prevenzione degli incidenti di sicurezza ICT
- Possibilità di esprimere in forma standardizzata le funzionalità di sicurezza e i requisiti di assurance
- Possibilità di utilizzare uno dei Profili di Protezione a valenza generale messi a disposizione dallo standard

Svantaggi

- Lunghi tempi di valutazione/certificazione
- Quantità rilevante di documentazione richiesta
- Processo di mantenimento della certificazione complesso
- Elevati costi di valutazione/ certificazione

CONCLUSIONI

- La Certificazione dei prodotti ICT rappresenta un **elemento chiave** in ambito Cyber Security per garantire i livelli di sicurezza richiesti per i sistemi e le applicazioni IT
- La scelta delle **metodologie di valutazione** rappresenta un driver importante in quando devono:
  - Garantire che la **valutazione sia efficace** e raggiunga gli obiettivi di sicurezza richiesti
  - Essere **specializzate in maniera verticale** sulla base della tecnologia valutata
  - Consentire la **valutazione a diversi livelli di sicurezza** rendendo la certificazione accessibile al maggior numero di vendor e, nel contempo, fornire alle Autorità Nazionali degli **strumenti utili per le certificazioni obbligatorie**
- Un aspetto rilevante per le certificazioni è lo sviluppo da parte dei vendor/laboratori di **tool automatici per l'automatizzazione delle fasi più onerose della certificazione** quali, ad esempio, l'esecuzione dei test e delle analisi di vulnerabilità. In tale ambito, uno strumento essenziale è la disponibilità di Protection Profile per categorie omogenee di prodotti.
- Altro punto importante è quello relativo alla **procedura di manutenzione** della certificazione che deve garantire la gestione nel tempo delle nuove vulnerabilità

Grazie per l'attenzione

Garibaldi Conte

garibaldi.conte@atsec.com