

Common criteria



Il progetto di sicurezza di
un sistema di servizi



Common Criteria



Il progetto di sicurezza
di un sistema di servizi

All'origine...

TCSEC - trusted computer system evaluation criteria - sviluppato negli U.S.A. nel 1980 e pubblicato ufficialmente nel 1983 (Orange Book)

Interoperabilità dei
certificati di valutazione

altri

ITSEC - information technology security evaluation criteria - sviluppato in europa da UK, F, D e NL, nel 1991e pubblicato ufficialmente nel 1993 (blu-white-red book)

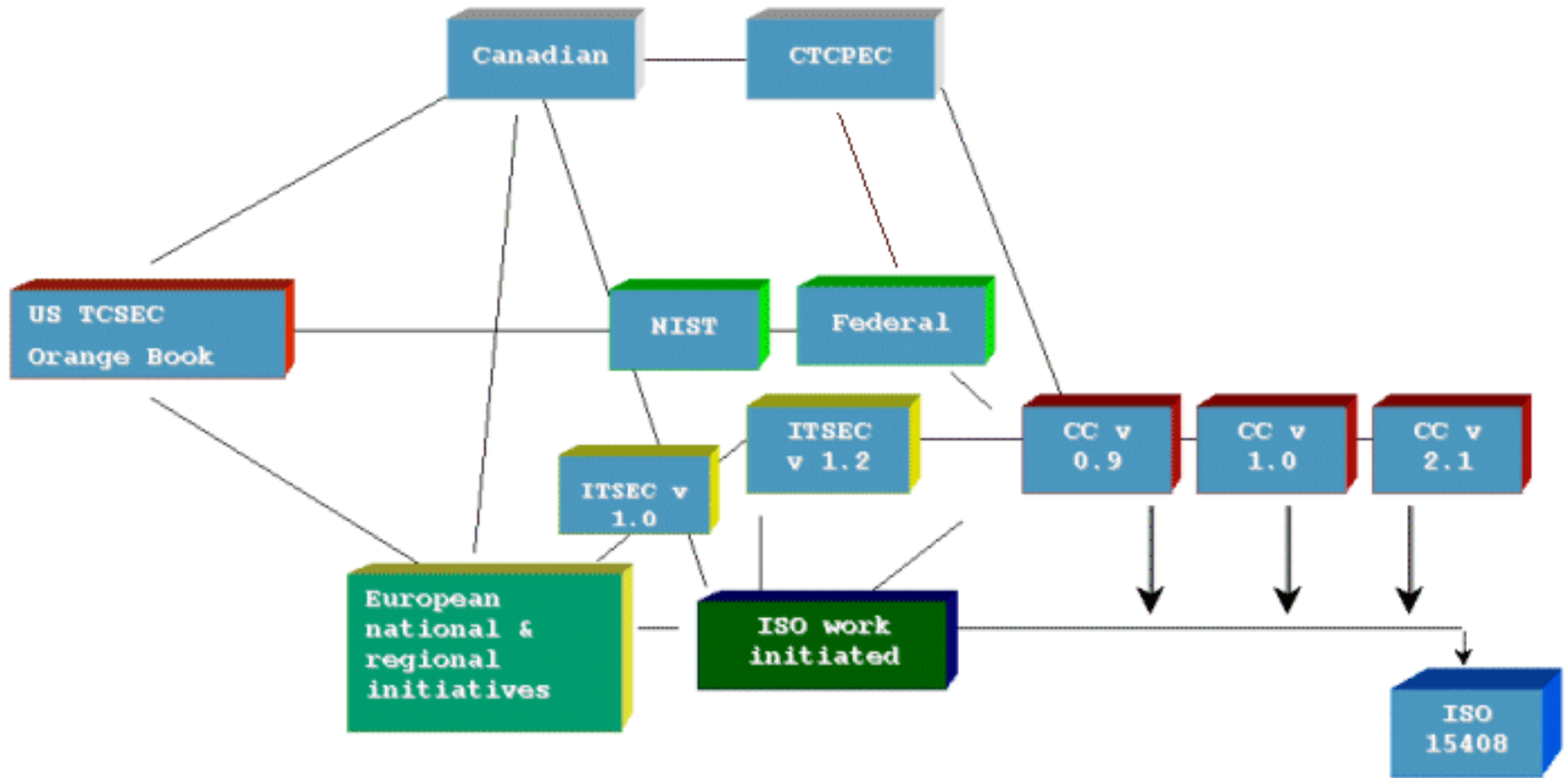


Common Criteria

Common Criteria -

iniziato nel 1193 e

All'origine...

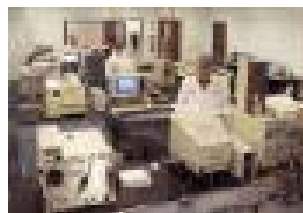


I laboratori...



Accredited Evaluation Laboratories within each country:

 <u>Australia and New Zealand</u>	 <u>Canada</u>
 <u>France</u>	 <u>Germany</u>
 <u>United Kingdom</u>	 <u>United States</u>





L'esigenza primaria

- Individuare metodi e strumenti in grado di permettere una valutazione misurabile della sicurezza di un sistema e/o di un prodotto.
- Rilasciare una valutazione della sicurezza internazionalmente riconosciuta e confrontabile (interoperabile) con valutazione già pre-esistenti di sistemi e/o prodotti.
- Permettere ai consumatori, agli sviluppatori ed ai certificatori di parlare un linguaggio comune e di potersi confrontare su schemi e modelli comuni.

Target of evaluation (TOE)



Prodotto o sistema corredato della sua documentazione utente (user guide) che è alla base della valutazione.

TOE resource: qualsiasi oggetto usabile o consumabile all'interno del TOE

TOE security policy (TSP): insieme di regole che dicono come gli oggetti del TOE devono essere manipolati

TOE security policy model: rappresentazione strutturata della TSP.

TOE security functions (TSF): hw, sw e firmware che devono essere disponibili per il corretto sviluppo della TSP.

TOE security functions interface (TSFI): insieme di interfacce interattive o programmi sw attraverso le quali sono acceduti gli oggetti del TOE attraverso le TSF.

Protection Profile (PP)



- Insieme di requisiti, regole di sicurezza che una categoria di prodotti e di sistemi (categoria TOE) devono verificare indipendentemente dalla loro implementazione fisica.

Si tratta quindi della definizione di standard funzionali che permettono poi di ricavare le specifiche del prodotto e/o del sistema.

Esistono PPs per firewall, database, router, ...

Security Target (ST)



- Insieme di requisiti, regole di sicurezza ed obiettivi che sono alla base per la valutazione di un TOE.

Il ST quindi definisce le misure funzionali e di sicurezza da effettuare affinché un TOE incontri i requisiti del suo PP.

Evaluation assurance level (EAL)



Il progetto di sicurezza
di un sistema di servizi

Insieme consistente di elementi di sicurezza (descritti nella parte 3 dei CC) che rappresentano un punto sulla scala di valutazione dei CC. Sono 7:

- **EAL 1:** functionally tested
- **EAL 2:** structurally tested
- **EAL 3:** methodically tested and checked
- **EAL 4:** methodically designed, tested and reviewed
- **EAL 5:** semiformally designed and tested
- **EAL 6:** semiformally verified design and tested
- **EAL 7:** formally verified design and tested



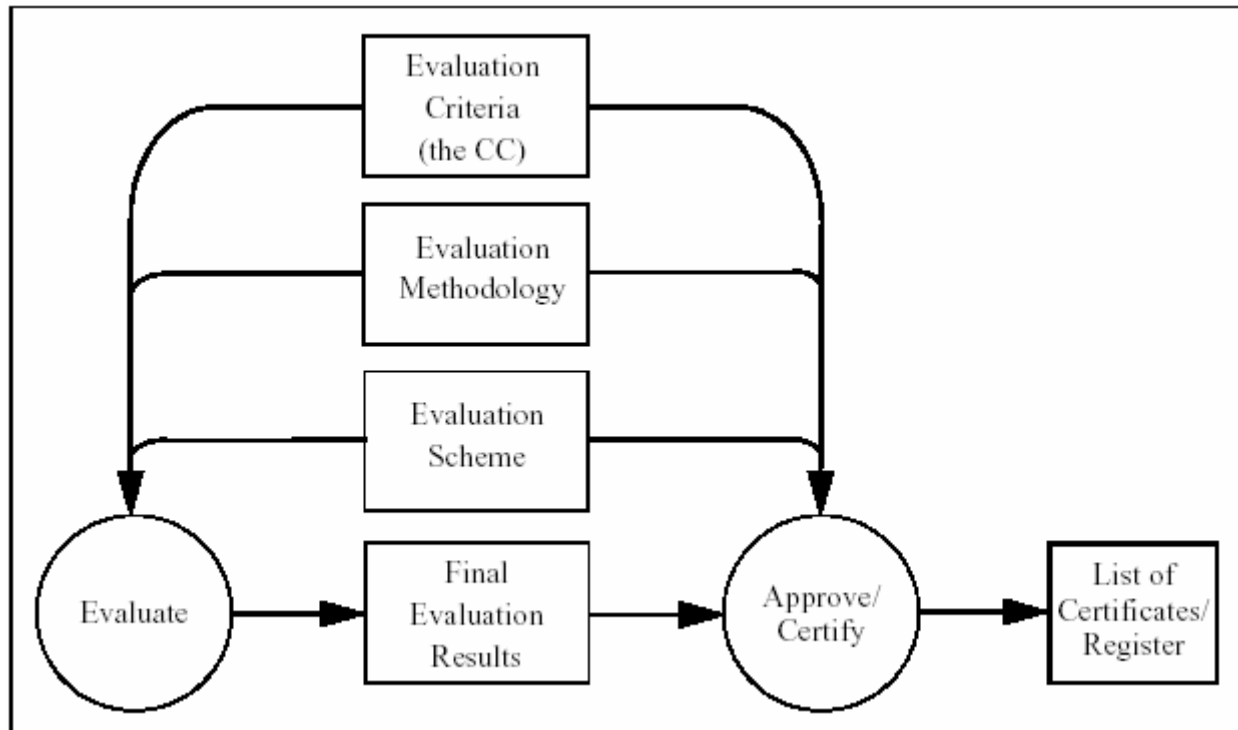
EAL e gli altri

CC	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	-	E1	E2	E3	E4	E5	E6
TCSEC	-	C1	C2	B1	B2	B3	A1



Contesto della valutazione

I CC forniscono soltanto i criteri della valutazione del TOE e devono essere supportati da una metodologia che permette la valutazione del TOE a fronte del quale viene emesso un certificato che sarà pubblicato nella Centralised Certifies Product List (CCPL)



*



Il programma di sicurezza di un sistema di servizi

Product	Assurance Level	Supplier	Status	caveat?
Oracle 8 Release 8.0.5	EAL4	Oracle Corporation	certified 2000/10	
ATMEL AT05SC1604R integrated	EAL4+	ATMEL Smartcards ICs	certified 2002/03	
Oracle 7 Release 7.2.2.4.13	EAL4	Oracle Corporation	certified 1998/09	
Oracle Government Database Management System Protection Profile	EAL3	Oracle Corporation	certified 1998/10	
Oracle 8 Release 8.1.7	EAL4	Oracle Corporation	certified 2001/07	
Oracle Commercial Database Management System Protection Profile	EAL3	Oracle Corporation	certified 1998/09	
Entrust RA and Entrust/Authority from Entrust/PKI 5.1	EAL3	Entrust Technologies Limited	certified 2001/02	
Entrust/RA and Entrust/Authority from Entrust/PKI 5.0	EAL3	Entrust Technologies Limited	certified 2000/03	
Entrust/PKI 4.0a	EAL3	Entrust Technologies Limited	certified 2000/01	
TeleWall System	EAL2+	SecureLogix Corporation	certified 2000/10	



L'organizzazione dei CC

I CC sono descritti in tre documenti ufficiali:

Parte 1: introduction and general model che è l'introduzione ai CC e permette di scrivere specifiche di alto livello per prodotti e sistemi da valutare (TOE);

Parte 2: security functional requirements: dove c'è la catalogazione di un insieme di componenti funzionali, famiglie e classi;

Parte 3: Security assurance requirements: dove vengono definiti i criteri di valutazione per i PPs e STs.



Roadmap dei CC

	Consumers	Developers	Evaluators
Part 1	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for security functions.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Use as mandatory statement of evaluation criteria when determining whether a TOE effectively meets claimed security functions.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use as mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.