

# I Common Criteria nell'ambito dello Schema Nazionale per la tutela delle informazioni classificate

Autori: Stefano Ramacciotti (CISSP), Luciano Porcelli



*Clusit*  
*Education*

# L'evoluzione dei Common Criteria fino alla versione 3.1R3Final







Autore: Luciano Porcelli, Capo Sezione Metodologie di Valutazione - Centro di Valutazione della Difesa



*Clusit*  
*Education*



# Come siamo giunti ai CC

						
1983	TCSEC					
1985	TCSEC	← ORANGE BOOK				
1989		CTCPSC	CETIT	UKITSEC	CCDDCSI	
1991			ITSEC			
1992	FC					
1993		CTCPSC	ITSEM			
1996	CC Vers. 1.0					
1998	CC Vers. 2.0					
1999	ISO 15408:1999	CC Vers. 2.1			CEM Vers. 1.0	
2004	ISO 15408:2004	CC Vers. 2.2		ISO 18045:2004	CEM Vers. 2.2	
2005	ISO 15408:2005	CC Vers. 2.3		ISO 18045:2005	CEM Vers. 2.3	
2009	ISO 15408:2009	CC Vers. 3.1R3final		ISO 18045:2009	CEM Vers. 3.1R3	

# Livelli di assurance da EAL1 a EAL4

## Common Criteria (ISO 15408)

<b>EAL1</b>	Functionally Tested	E' richiesta una certa fiducia nel corretto funzionamento. EAL1 richiede solo un <b>LAST</b> e potrebbe essere condotto <b>con successo senza assistenza da parte degli sviluppatori del TOE</b> . L'analisi è sostenuta da una ricerca di potenziali vulnerabilità di dominio pubblico, per <b>potenziale di attacco Basic e test indipendenti</b> (funzionali e di penetrazione) della TSF.
<b>EAL2</b>	Structurally Tested	Richiede la <b>collaborazione dello sviluppatore</b> in termini di consegna delle informazioni e risultati dei test, ma non deve imporre maggiori sforzi da parte degli sviluppatori rispetto a ciò che è coerente con una buona pratica commerciale. EAL2 fornisce garanzia grazie ad un <b>ST completo</b> e un'analisi delle SFR indicate nel ST. L'analisi è supportata da una <b>conferma</b> selettiva indipendente dei risultati dei <b>test degli sviluppatori</b> , e una analisi della vulnerabilità per potenziale di attacco Basic.
<b>EAL3</b>	Methodically Tested & Checked	EAL3 è applicabile nel caso in cui gli sviluppatori o gli utenti richiedono un moderato livello di sicurezza garantito indipendentemente, e richiedono un <b>esame approfondito del TOE</b> e del suo sviluppo <b>senza</b> una sostanziale <b>re-ingegnerizzazione</b> . EAL3 fornisce garanzia grazie ad una descrizione dell'architettura del progetto del TOE. L'analisi è sostenuta da una analisi della vulnerabilità per potenziale di attacco Basic.
<b>EAL4</b>	Methodically Designed, Tested & Reviewed	Permette ad uno sviluppatore di ottenere la massima garanzia da una <b>positiva ingegnerizzazione in termini di sicurezza</b> basata su buone pratiche di sviluppo commerciale. <b>EAL4 è il più alto livello</b> per il quale sia <b>economicamente fattibile il retrofit</b> di una linea di prodotti esistenti. EAL4 prevede descrizione dei moduli e della implementazione. L'analisi è supportata da una analisi della vulnerabilità per <b>potenziale di attacco pari a Enhanced-Basic</b> . EAL4 fornisce garanzia grazie anche attraverso l'uso di <b>ambienti di sviluppo controllati</b> .



# Livelli di assurance da EAL5 a EAL7

## Common Criteria (ISO 15408)

<b>EAL5</b>	Semiformally Designed & Tested	EAL5 permette ad uno sviluppatore di ottenere la massima garanzia basata su una rigorosa prassi commerciale di sviluppo supportata da una <b>moderata applicazione di tecniche di ingegneria di sicurezza specializzate</b> . L'analisi è sostenuta da analisi indipendenti delle vulnerabilità che dimostrano la resistenza alla penetrazione di attaccanti con un <b>moderato potenziale di attacco</b> . Questo EAL rappresenta un significativo aumento della garanzia da EAL4 imponendo una <b>descrizione progettuale semiformale</b> .
<b>EAL6</b>	Semiformally Verified Designed & Tested	EAL6 permette agli sviluppatori di ottenere alta garanzia dalla applicazione di tecniche di ingegneria della sicurezza a un ambiente di sviluppo rigoroso, al fine di produrre un <b>TOE adeguato per la protezione di beni di alto valore contro rischi significativi</b> . L'analisi è supportata da verifiche che dimostrano la resistenza alla penetrazione di attaccanti con un <b>elevato potenziale di attacco</b> . Questo EAL richiede un'analisi più approfondita, una rappresentazione strutturata della implementazione, una maggiore strutturazione dell'architettura (ad esempio a strati), <b>una più completa e indipendente analisi della vulnerabilità</b> , e una <b>gestione della configurazione migliorata</b> e controlli sull'ambiente di sviluppo.
<b>EAL7</b>	Formally Verified Designed & Tested	EAL7 è applicabile per lo sviluppo della sicurezza di TOE per applicazioni in <b>situazioni di rischio estremamente elevato e / o dove l'elevato valore dei beni giustifica i costi maggiori</b> . EAL7 fornisce garanzie grazie ad una <b>presentazione strutturata della implementazione</b> per capire il comportamento di sicurezza. La garanzia è inoltre acquisita attraverso un <b>modello formale di selezione delle politiche di sicurezza</b> del TOE e una presentazione semiformale delle specifiche funzionali e del progetto del TOE. E' anche necessario un <b>disegno della TSF modulare, stratificato e semplice</b> . L'analisi è supportata da test indipendenti e una analisi indipendente delle vulnerabilità che dimostra la resistenza alla penetrazione di attaccanti con un <b>elevato potenziale di attacco</b> .

# Composed assurance packages (CAP)

1° livello  
EAL1

## Common Criteria (ISO 15408)

**CAP-A**  
≤ EAL2

Structurally  
composed

CAP-A è applicabile quando un TOE composto è integrato ed è richiesta la fiducia nel corretto funzionamento della sicurezza del composto risultante. Ciò richiede la **collaborazione dello sviluppatore del componente dipendente (DC)** in termini di consegna delle informazioni progettuali e dei test risultanti dalla certificazione del DC, **senza che sia richiesto l'intervento dello sviluppatore del BC**. Le **SFR nel ST** del TOE composto sono analizzate **utilizzando i risultati delle valutazioni dei componenti del TOE**. L'analisi è supportata da **test indipendenti delle interfacce del BC che sono invocate dal DC**. L'analisi è sostenuta anche da una **revisione** da parte del valutatore della **vulnerabilità del TOE composto**

**CAP-B**  
≤ EAL3

Methodically  
composed

CAP-B consente ad uno sviluppatore coscienzioso di ottenere la massima garanzia dalla comprensione, **a livello di sottosistema**, degli effetti delle interazioni tra i componenti del TOE e del suo sviluppo senza una sostanziale reingegnerizzazione. CAP-B fornisce garanzia mediante l'analisi di un **ST completo** per il TOE composto. L'analisi è sostenuta anche da una analisi delle vulnerabilità da parte del valutatore del TOE composto per dimostrare la resistenza agli aggressori con un **potenziale di attacco pari a Basic**

**CAP-C**  
≤ EAL4

Methodically  
composed,  
tested and  
reviewed

**CAP-C non richiede l'accesso completo a tutte le prove di valutazione del BC**. CAP-C è quindi applicabile nel caso in cui gli sviluppatori o gli utenti sono disposti a sostenere **costi aggiuntivi specifici per la ingegnerizzazione** della sicurezza. CAP-C fornisce garanzia anche mediante **l'analisi del progetto del TOE descrivendo i moduli delle TSF**. L'analisi è supportata anche da una analisi della vulnerabilità per dimostrare la resistenza agli aggressori con un **potenziale di attacco pari a Enhanced-Basic**



# CC ver. 2.3 vs 3.1R2

Gestione del “versioning” delle applicazioni	No
Sviluppo non integrato nel processo	//
Quadro complesso (spesso “incomprensibile” per gli utenti)	≈
Troppi “documenti cartacei”	≈
Miglioramento della terminologia	Un po’
Concetto di “ <b>composizione</b> ” di due o più prodotti già certificati (sviluppo di ulteriori entità IT non incluso)	Sì
Concetto di “riduzione dello sforzo” (processo troppo lungo e costoso che influisce sui tempi di rilascio sul mercato)	Un po’
◆ Rimozione delle ridondanze	Sì
◆ Disallineamento fra valutazioni di “bassa garanzia” e lo sforzo	Sì
◆ Scala di valutazione EAL migliorata (agg. <b>CAP</b> )	Sì
◆ Nuovo concetto per il TOE design più vicino alla realtà	Sì

# CC vers. 3.1R2 in vigore dal 1/4/08 vers. 3.1R3 in vigore dal 1/7/09

Official CC/CEM versions - The Common Criteria Portal - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti ?

http://www.commoncriteriaportal.org/thecc.html

Horde :: Entra Gmail: f'email di Google Ubuntu -- Software P... Posta :: Webmail Mini... MMI Outlook Web Ac...

## Common Criteria

- ABOUT THE CCRA 01
- THE COMMON CRITERIA 02
- OTHER PUBLICATIONS 03
- CERTIFIED PRODUCTS 04
- PROTECTION PROFILES 05

### LAST UPDATES

- Products 10-March-2008
- PPs 03-March-2007
- Supp. Documents 2-Apr-2008
- Laboratories 06-March-2008
- Schemes 06-March-2008
- CCRA members 12-Feb-2008

### The Common Criteria

The member organisations of the CCRA declare that defined assurance levels (EALs) between versions of the criteria are equivalent and can therefore be used without restrictions for composition activities.

#### CC v2.3

CC v2.3 is based on version 2.2, updated with a number of [interpretations](#) and further editorial changes that do not affect their technical content. These standards have also been published as ISO/IEC 15408:2005 and ISO/IEC 18045:2005. This version is the last of the 2.\* series, to be used until March 2008, and maintenance based in this version during further 18 months, i.e., until September 2009.

CC v2.3 consists of three parts:

Part 1: Introduction and general model	PDF <a href="#">ccpart1v2.3.pdf</a>
Part 2: Security functional requirements	PDF <a href="#">ccpart2v2.3.pdf</a>
Part 3: Security assurance requirements	PDF <a href="#">ccpart3v2.3.pdf</a>

CEM v2.3 consists of one part:

CEM	PDF <a href="#">cemv2.3.pdf</a>
-----	------------------------------------

For previous versions of the CC and CEM please click [here](#)  
For unofficial versions of the CC and CEM please click [here](#)

Completato

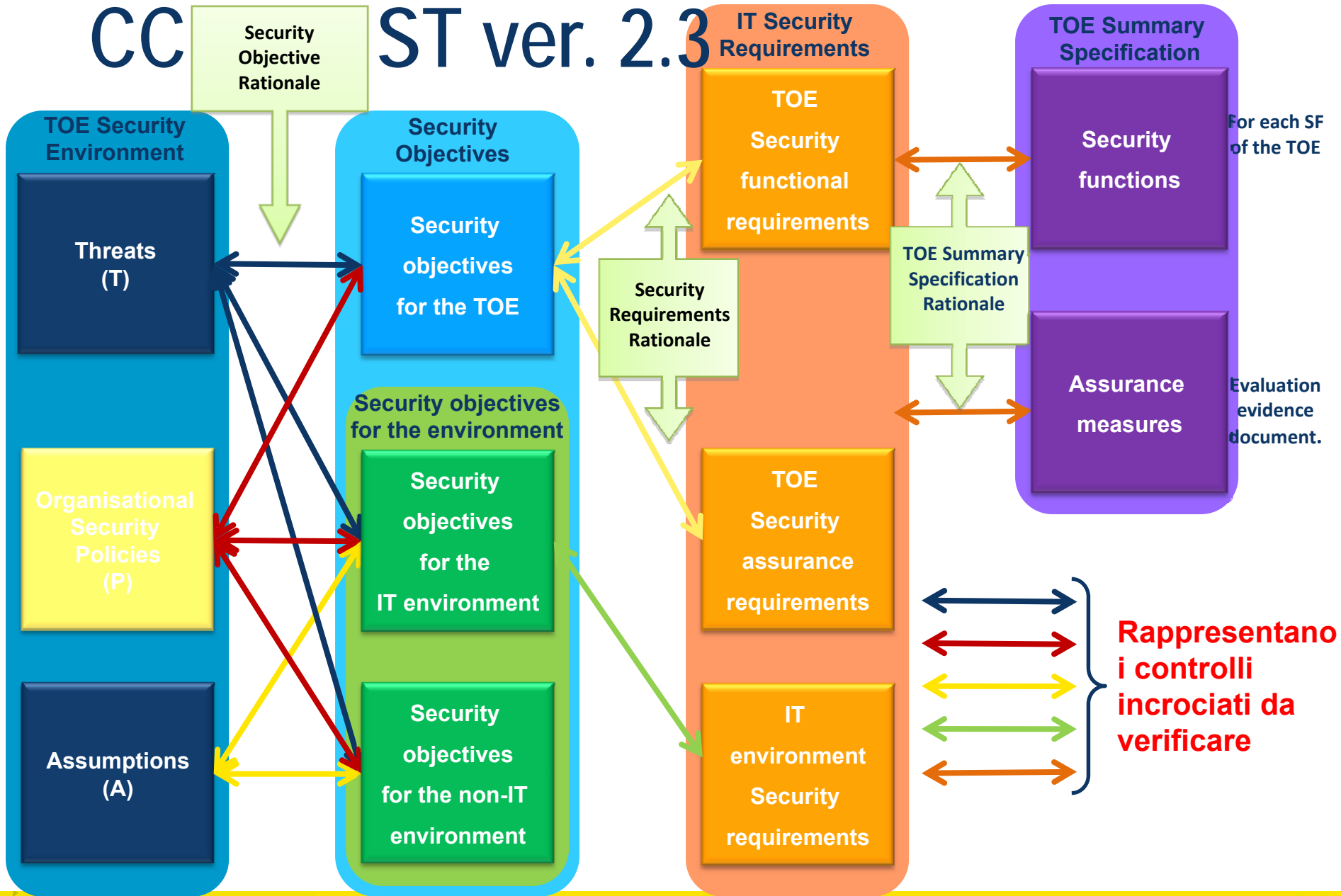


## CC v2.3

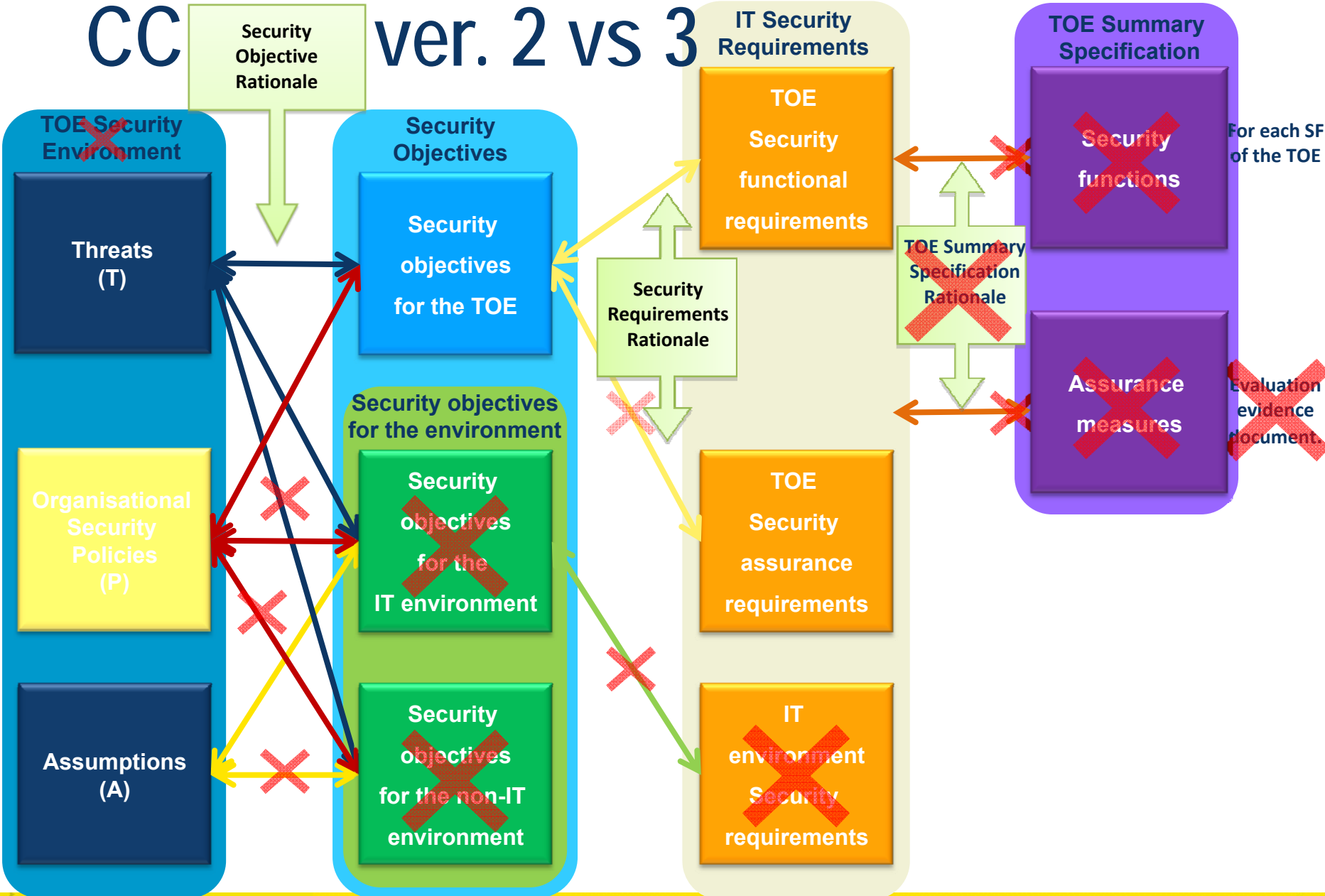
I CC v2.3 si basano sulla versione 2.2, aggiornata con una serie di interpretazioni e ulteriori modifiche che non incidono sul loro contenuto tecnico. Tali norme sono state pubblicate anche come ISO / IEC 15408:2005 e ISO / IEC 18045:2005.

**Questa versione è l'ultima della serie 2.\*, e può essere eventualmente utilizzata per valutazioni che siano iniziate prima di marzo 2008...**

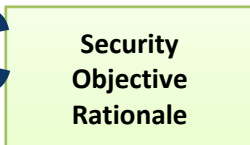
# CC ST ver. 2.3



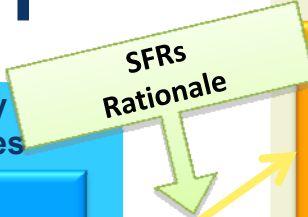
# CC ver. 2 vs 3



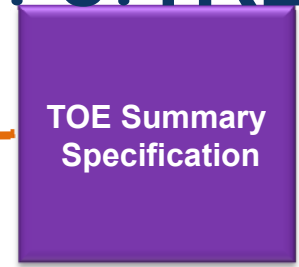
CC



ST



ver. 3.1R2



Per ogni SF del TOE



Vds Nota

**Nota:**  
 Secondo la fig. 7 a pagina 62 dei CC Part 1 non ci sono collegamenti tra SAR e Sec. Obj. per il TOE, ma questo non è da considerare obbligatorio

**Rappresentano i controlli incrociati da verificare**

# Differenze nei ST vers. 2.3 e vers. 3.1R2

Security Target ver. 2.3	Security Target ver. 3.1R2
<ol style="list-style-type: none"><li>1. ST introduction<ol style="list-style-type: none"><li>a. ST identification</li><li>b. ST overview</li><li>c. <b>CC conformance</b></li></ol></li><li>2. TOE description</li><li>3. TOE Security environment<ol style="list-style-type: none"><li>a. Assumptions</li><li>b. Threats</li><li>c. Organizational security policies</li></ol></li><li>4. Security objectives<ol style="list-style-type: none"><li>a. Security objectives for the TOE</li><li>b. Security objectives for the environment</li></ol></li><li>5. IT security requirements<ol style="list-style-type: none"><li>a. Security requirements for the IT environment</li><li>b. TOE security requirements<ul style="list-style-type: none"><li>▪ TOE security functional requirements</li><li>▪ TOE security assurance requirements</li></ul></li></ol></li><li>6. TOE summary specification<ol style="list-style-type: none"><li>a. TOE security functions</li><li>b. <b>Assurance measures</b></li></ol></li><li>7. <b>PP claims</b><ol style="list-style-type: none"><li>a. <b>PP reference</b></li><li>b. <b>PP tailoring</b></li><li>c. <b>PP additions</b></li></ol></li><li>8. Rationale<ol style="list-style-type: none"><li>a. Security objectives rationale</li><li>b. Security requirements rationale</li><li>c. <b>TOE summary specification rationale</b></li><li>d. <b>PP claims rationale</b></li></ol></li></ol>	<ol style="list-style-type: none"><li>1. ST introduction<ol style="list-style-type: none"><li>a. ST reference</li><li>b. <b>TOE reference</b></li><li>c. TOE overview</li><li>d. <b>TOE description</b></li></ol></li><li>2. Conformance claim<ol style="list-style-type: none"><li>a. CC conformance claims</li><li>b. PPs claims and/or packages claims</li><li>c. Conformance Rationale</li></ol></li><li>3. Security problem definition<ol style="list-style-type: none"><li>a. Threats,</li><li>b. Organizational security policies</li><li>c. Assumptions</li></ol></li><li>4. Security objectives<ol style="list-style-type: none"><li>a. Security objectives for the TOE</li><li>b. Security objectives for the operational environment of the TOE</li><li>c. Security objectives rationale</li></ol></li><li>5. Extended components definition<ol style="list-style-type: none"><li>a. Extended functional components</li><li>b. Extended assurance components</li></ol></li><li>6. Security requirements<ol style="list-style-type: none"><li>a. Security functional requirements</li><li>b. Security assurance requirements</li><li>c. Security requirements rationale</li></ol></li><li>7. <b>TOE summary specification</b></li></ol>

**In ROSSO: non inclusi nei Protection Profile (PP)**

# Security Problem Definition

## Security Problem Definition

Threats  
(T)

Organisational  
Security  
Policies  
(P)

Assumptions  
(A)

Minacce	Politiche di sicurezza dell'Organizzazione	Ipotesi
<p><b>Potenziale di abuso su beni protetti (entità alle quali qualcuno ha attribuito un valore). Una minaccia è descritta in termini di:</b></p> <ul style="list-style-type: none"> <li>➢ <b>agenti di minaccia</b> (entità che possono agire contro un bene), espressi in termini di:           <ul style="list-style-type: none"> <li>▪ competenza</li> <li>▪ risorse disponibili</li> <li>▪ motivazione</li> </ul> </li> <li>➢ <b>un bene</b>, espressi in termini di:           <ul style="list-style-type: none"> <li>▪ metodi di attacco</li> <li>▪ ogni vulnerabilità sfruttabile</li> <li>▪ opportunità</li> </ul> </li> <li>➢ <b>azioni effettuate da un agente di minaccia su un bene</b></li> </ul>	<p><b>Una o più :</b></p> <ul style="list-style-type: none"> <li>➢ <b>norme di sicurezza</b></li> <li>➢ <b>procedure</b></li> <li>➢ <b>linee guida</b></li> </ul> <p><b>imposte (o che si presume essere imposte) ora e / o in futuro da parte di una reale o ipotetica organizzazione nell'ambiente operativo</b></p>	<p>Descrive gli aspetti di sicurezza dell'ambiente operativo in cui il TOE sarà utilizzato o è destinato ad essere utilizzato. Ciò dovrebbe includere:</p> <ul style="list-style-type: none"> <li>➢ <b>informazioni sulle intenzioni d'uso del TOE :</b> <ul style="list-style-type: none"> <li>▪ ipotesi fisiche</li> <li>▪ ipotesi sul personale</li> <li>▪ ipotesi sugli aspetti di collegamento</li> </ul> </li> <li>▪ <b>ma anche:</b> <ul style="list-style-type: none"> <li>▪ applicazioni designate</li> <li>▪ potenziale valore dei beni</li> <li>▪ eventuale limitazioni d'impiego</li> </ul> </li> </ul> <p><i>Nota: durante la valutazione queste ipotesi sono considerate vere, cioè non sono verificate in alcun modo.</i></p>

# Security Problem Definition (esempi)

## Security Problem Definition

Threats  
(T)

Organisational  
Security  
Policies  
(P)

Assumptions  
(A)

Minacce (threats)	Politiche di sicurezza dell'Organizzazione	Ipotesi (assumptions)
<p>•Per minacce al TOE:</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> T.FACCINT, possono essere non rilevati i tentativi di accesso non autorizzato ai dati del TOE o alle SF</li> </ul> <p>•Per minacce alla parte Op. Env.:</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> T.MISACT, può verificarsi attività dannosa, come l'introduzione di trojan, su un sistema informatico monitorato dal TOE</li> </ul>	<p>•Per OSP del TOE:</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> P.PASSWD, la password deve essere di 8 caratteri</li> </ul> <p>•Per OSP dell'OP. Env.:</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> P.MANAGE, il TOE deve essere gestito da utenti autorizzati</li> </ul>	<p>•Per ipotesi fisiche:</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> A.PROTECT, HW ed il SW del TOE critico per l'applicazione della politica di sicurezza saranno protetti da ...</li> </ul> <p>•Per ipotesi sul personale:</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> A.NOEVIL, il SysAdm è attento e rispettoso delle norme</li> </ul> <p>•Per ipotesi sugli aspetti di collegamento':</p> <ul style="list-style-type: none"> <li>• <b>ad es.:</b> A.STNDAL, non sarà fornita la connettività o l'accesso ...</li> </ul>



# Security Objectives

Security Objectives

Security objectives for the TOE

Security objectives for the environment

Obiettivi di sicurezza (contromisure)	Obiettivi di sicurezza per il TOE	Obiettivi per la sicurezza dell'ambiente operativo
<p>Dichiarazione di <i>intenti per contrastare le T individuate e/o soddisfare le OSP identificate e/o le A. Una minaccia può essere <b>contrastata</b> / <b>ridotta</b> / <b>mitigata</b> dal TOE, dal suo ambiente operativo, o da una combinazione dei due.</i></p>	<p>Consiste in una serie di obiettivi che il TOE deve raggiungere al fine di risolvere la sua parte del problema. Ogni obiettivo di sicurezza per il TOE traccia almeno una <b>T</b> o una <b>OSP</b></p> <p><i>ad es.: O.PROTECT</i>, il TOE deve difendersi da modifiche non autorizzate e l'accesso alle sue funzioni e dati</p> <p><i>ad es.: O.INTEGR</i>, il TOE deve garantire l'integrità di tutti gli audit e dati di sistema</p>	<p>Consiste in una serie di dichiarazioni che descrivono gli obiettivi che l'ambiente operativo dovrebbe raggiungere.</p> <p>Ogni obiettivo di sicurezza per l'ambiente operativo, se presente, traccia almeno una <b>T</b>, una <b>A</b> o una <b>OSP</b></p> <p><i>ad es.: OE.PROTECT</i>, l'ambiente operativo del TOE deve proteggere se stesso e il TOE da interferenze esterne o manomissione</p> <p><i>ad es.: OE.PHYSICAL</i>, l'ambiente operativo del TOE deve limitare l'accesso fisico alla TOE al personale amministratore e al personale addetto alla manutenzione accompagnato da personale amministratore</p>

# IT Security Requirements

## IT Security Requirements

TOE  
Security  
functional  
requirements

TOE  
Security  
assurance  
requirements

Requisiti funzionali di sicurezza (SFR):	Requisiti di garanzia di sicurezza (SAR):
<i>Dalla Parte 2<sup>a</sup> dei CC</i>	<i>Dalla Parte 3<sup>a</sup> dei CC</i>
<p>una traduzione degli obiettivi di sicurezza del TOE in un linguaggio standard. Questo è importante al fine di:</p> <ul style="list-style-type: none"> <li>• fornire una descrizione esatta <b>di ciò che è da valutare</b></li> <li>• consentire il confronto tra due ST</li> </ul> <p><b>ad es.: FIA_SOS.1 Verifica dei segreti</b>  <b>Gerarchica a:</b> nessun altro componente.  <b>Dipendenza:</b> nessuna dipendenza.                      Il FIA_SOS.1.1 TSF fornisce un meccanismo per verificare che i segreti soddisfino [assegnazione: Una lettera maiuscola, una lettera minuscola, un carattere speciale, e un numero per una password dell'utente di almeno 8 carattere].</p>	<p>una descrizione di come deve essere acquisita la garanzia che il TOE soddisfa le SFR. Questo è importante al fine di:</p> <ul style="list-style-type: none"> <li>• fornire una descrizione precisa <b>di come il TOE deve essere valutato</b></li> <li>• consentire il confronto tra due ST</li> </ul> <p><b>ad es.: ALC_DEL.1: Procedura di consegna</b>  <b>Dipendenza:</b> nessuna dipendenza.                      Il documento relativo alla consegna fornisce una descrizione delle procedure di sicurezza da attuate dalla consegna utilizzando GPG per proteggere il TOE dalle modifiche durante la consegna del prodotto al cliente.</p>
<p><b>Nota SFR:</b> non vi è alcuna traduzione richiesta nei CC per gli obiettivi di sicurezza per l'ambiente operativo, perché l'ambiente operativo non è valutato e non è pertanto necessaria una descrizione volta alla loro valutazione</p> <p><b>Nota relativa a "Gerarchica":</b> un componente è "hierarchical" ad un altro quando offre maggiore sicurezza</p>	<p><b>Nota SAR:</b> il ST contiene il fondamento logico dei requisiti di sicurezza che spiega il motivo per cui questa particolare serie di SAR è ritenuta opportuna. Non vi sono requisiti specifici per questa spiegazione: la spiegazione potrebbe variare da "Nessuno" a "perché il PP o una legge nazionale li prevede" a una dettagliata analisi del rischio del TOE e l'ambiente di sviluppo del TOE.</p>

# TOE Summary Specification

TOE Summary  
Specification

Per ogni SF  
del TOE

## TOE sintesi specifica *TOE Summary Specification (TSS)*

L'obiettivo per la TSS è quella di fornire ai potenziali utilizzatori dei TOE una descrizione di come il TOE soddisfa tutte le SFR. La TSS dovrebbe fornire i meccanismi tecnici generali che il TOE utilizza per questo scopo. Il livello di dettaglio di questa descrizione dovrebbe essere tale da consentire ai potenziali utilizzatori del TOE di comprendere la forma generale e l'implementazione del TOE stesso.

**ad es.:** se il TOE è un PC abilitato a Internet e le SFR contengono la FIA\_UAU.1 per specificare l'autenticazione, il TSS deve indicare in che modo questa autenticazione è fatta: password, token, controllo biometrico dell'iride, ecc.. Possono essere fornite anche ulteriori informazioni, come gli standard applicabili che il TOE utilizza per soddisfare le SFR, o descrizioni più dettagliate.

# CC

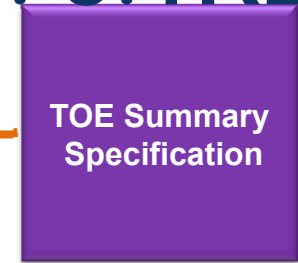
Security Objective Rationale

# ST

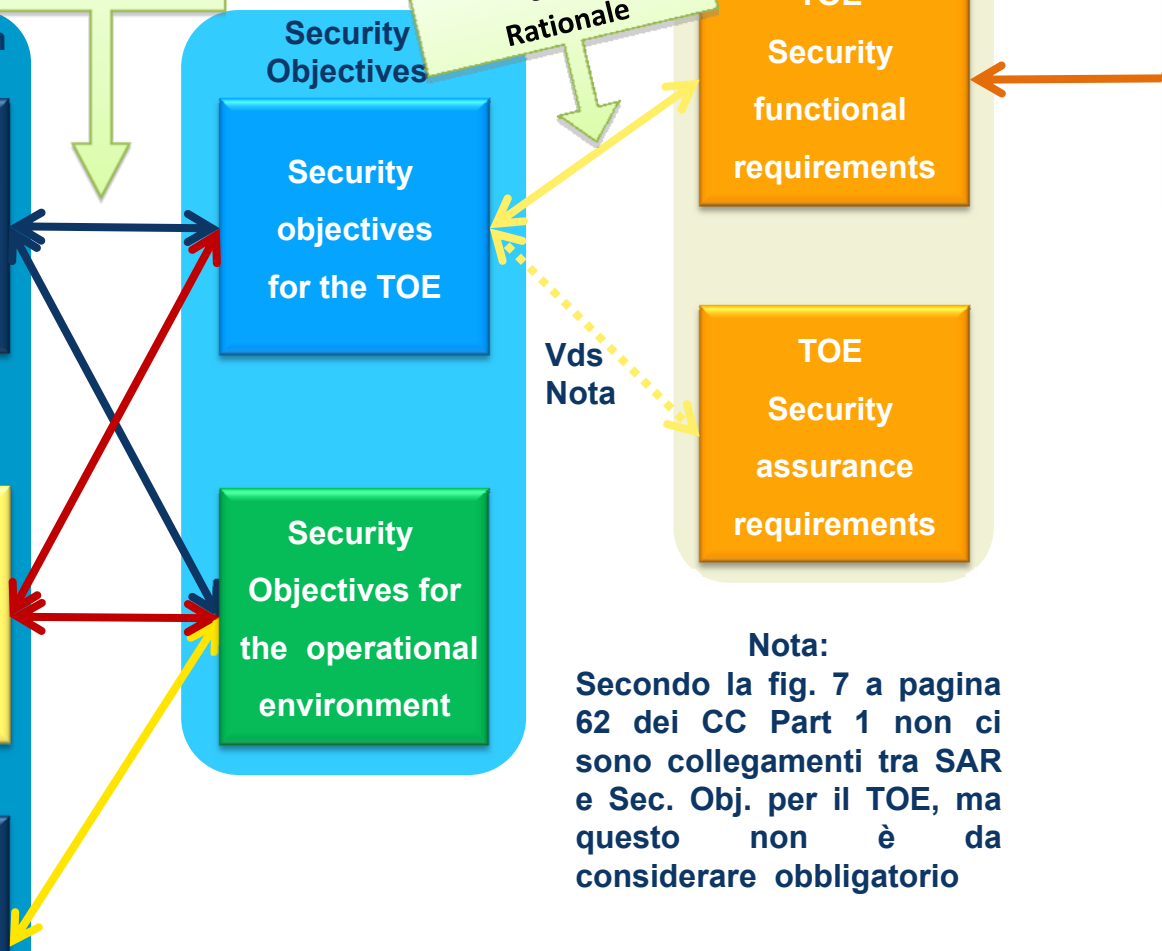
SFRs Rationale

## IT Security Requirements

# ver. 3.1R2

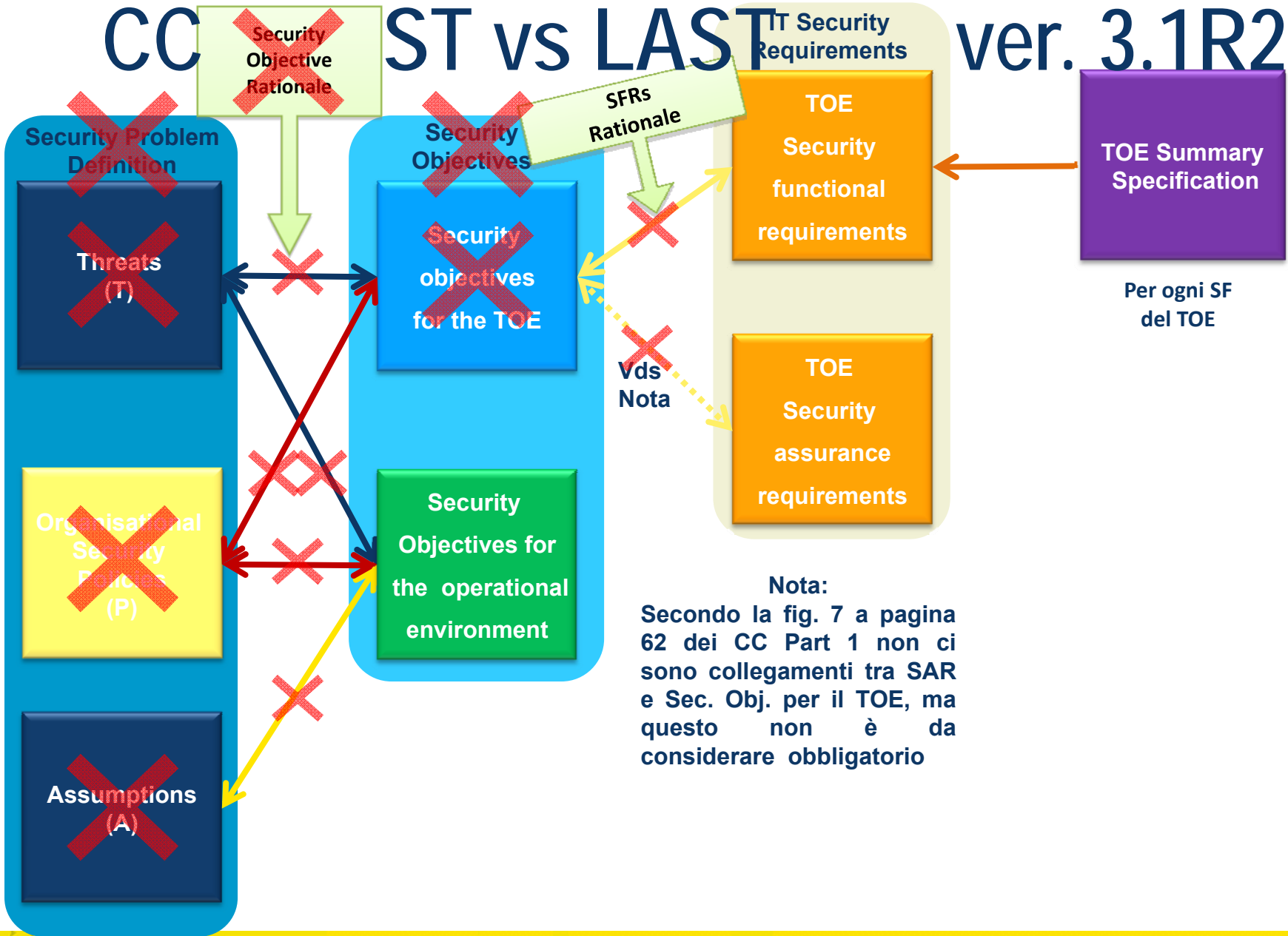


Per ogni SF del TOE



**Nota:**  
 Secondo la fig. 7 a pagina 62 dei CC Part 1 non ci sono collegamenti tra SAR e Sec. Obj. per il TOE, ma questo non è da considerare obbligatorio

# CC ST vs LAST IT Security Requirements ver. 3.1R2

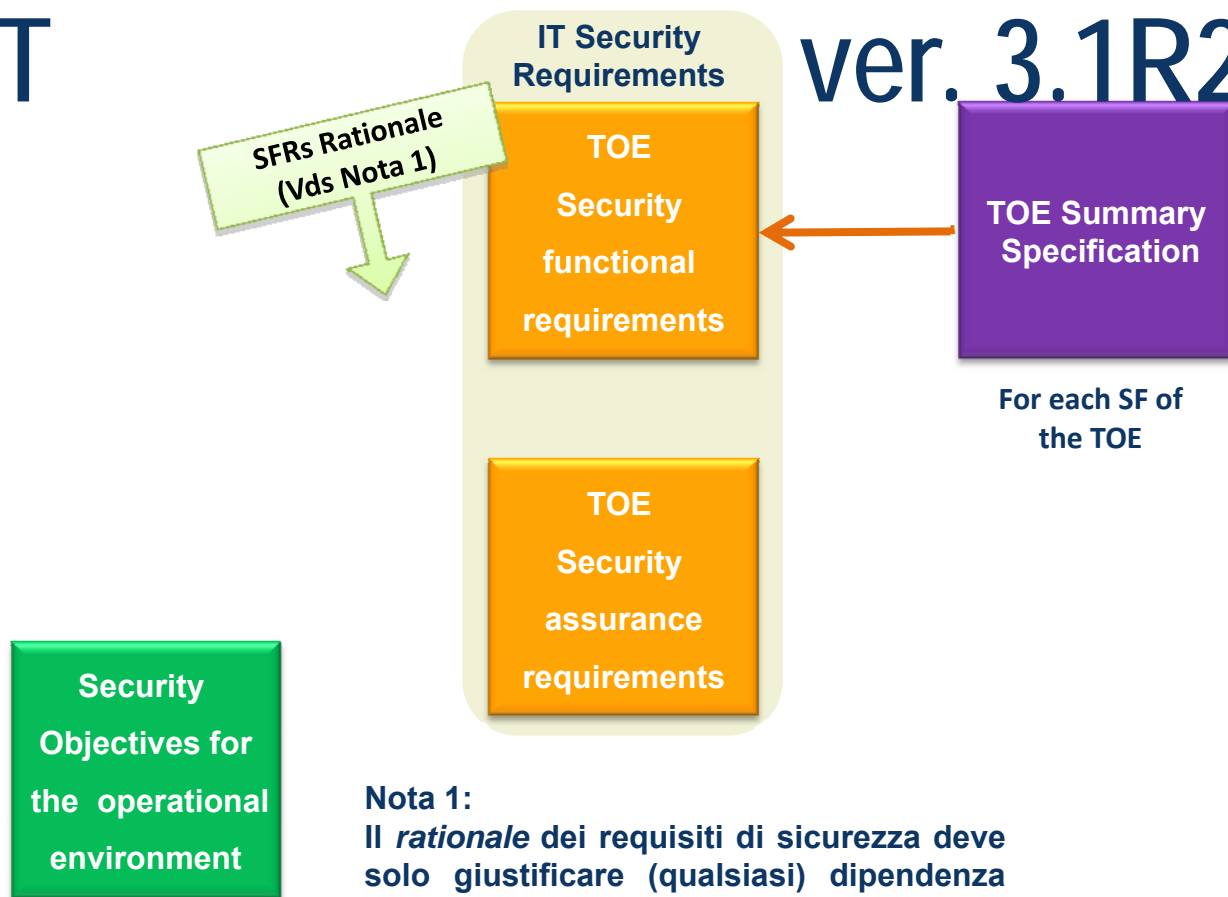


**Nota:**  
 Secondo la fig. 7 a pagina 62 dei CC Part 1 non ci sono collegamenti tra SAR e Sec. Obj. per il TOE, ma questo non è da considerare obbligatorio



# CC LAST

# ver. 3.1R2



### Nota 1:

Il *rationale* dei requisiti di sicurezza deve solo giustificare (qualsiasi) dipendenza non soddisfatta in quanto non ci sono obiettivi di sicurezza per il TOE nel ST

## Tipico di prodotti IT “da banco”

# Differenze tra LAST e ST (vers. 3.1R2)

Low assurance Security Target ver. 3.1R2 (EAL = 1/CAP = A)	Security Target ver. 3.1R2 (EAL ≥ 2/ CAP ≥ B)
<ul style="list-style-type: none"> <li>➤ ST introduction               <ul style="list-style-type: none"> <li>○ ST reference</li> <li>○ <b>TOE reference</b></li> <li>○ TOE overview</li> <li>○ <b>TOE description (physical &amp; logical scope)</b></li> </ul> </li> <li>➤ Conformance claim               <ul style="list-style-type: none"> <li>○ CC conformance claims</li> <li>○ PPs claims and/or packages claims</li> <li>○ Conformance Rationale</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>➤ ST introduction               <ul style="list-style-type: none"> <li>○ ST reference</li> <li>○ <b>TOE reference</b></li> <li>○ TOE overview</li> <li>○ <b>TOE description (physical &amp; logical scope)</b></li> </ul> </li> <li>➤ Conformance claim               <ul style="list-style-type: none"> <li>○ CC conformance claims</li> <li>○ PPs claims and/or packages claims</li> <li>○ Conformance Rationale</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>➤ Security objectives               <ul style="list-style-type: none"> <li>○ Security objective for the operational environment</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>➤ Security problem definition               <ul style="list-style-type: none"> <li>○ Threats,</li> <li>○ Organizational security policies</li> <li>○ Assumptions</li> </ul> </li> <li>➤ Security objectives               <ul style="list-style-type: none"> <li>○ Security objectives for the TOE</li> <li>○ Security objectives for the operational environment of the TOE</li> <li>○ Security objectives rationale</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>➤ Extended components definition               <ul style="list-style-type: none"> <li>○ Extended functional components</li> <li>○ Extended assurance components</li> </ul> </li> <li>➤ Security requirements               <ul style="list-style-type: none"> <li>○ Security functional requirements</li> <li>○ Security assurance requirements</li> <li>○ Security requirements rationale (to justifies only any dependency not satisfied)</li> </ul> </li> <li>➤ <b>TOE summary specification</b></li> </ul>	<ul style="list-style-type: none"> <li>➤ Extended components definition               <ul style="list-style-type: none"> <li>○ Extended functional components</li> <li>○ Extended assurance components</li> </ul> </li> <li>➤ Security requirements               <ul style="list-style-type: none"> <li>○ Security functional requirements</li> <li>○ Security assurance requirements</li> <li>○ Security requirements rationale</li> </ul> </li> <li>➤ <b>TOE summary specification</b></li> </ul>

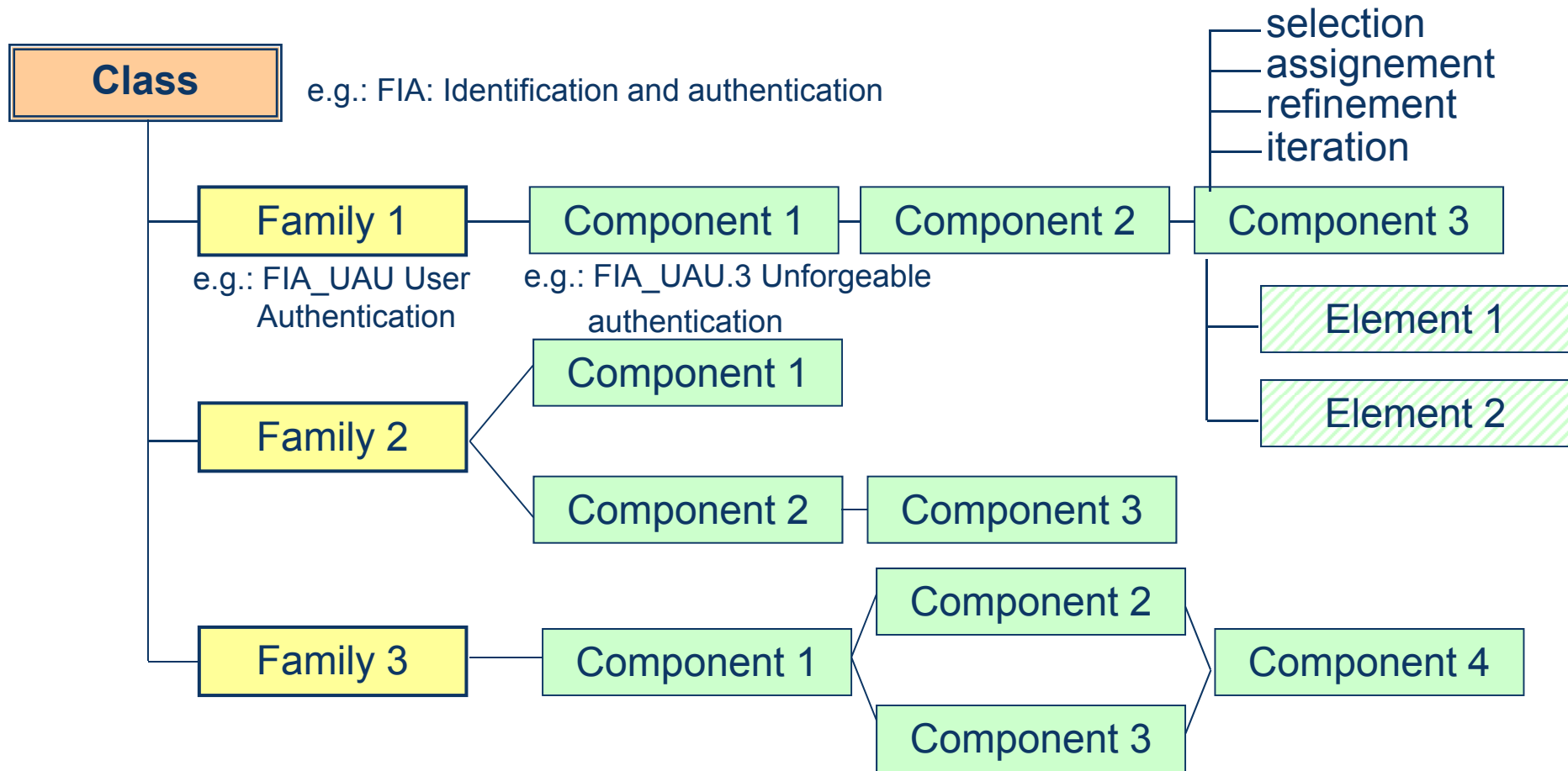
**In ROSSO: elementi non inclusi nei Protection Profile (PP)**

# SFRs (differenze minori tra 2.3 e 3.1)

	CLASSE	DESCRIZIONE
<b>FAU</b>	<b>Audit di sicurezza</b>	Controllo di sicurezza con il riconoscimento, la registrazione, la memorizzazione, l'analisi delle informazioni relative agli eventi significativi per la sicurezza. Le registrazioni sono essere esaminate per determinare gli eventi di sicurezza passati, e quale utente (se applicabile) è responsabile
<b>FCO</b>	<b>Supporto crittografico</b>	FCS si occupa della generazione di chiavi crittografiche, la distribuzione, l'accesso e la distruzione; e delle operazioni crittografiche svolte dal TOE (ad esempio, la cifratura, la decifrazione, le firme digitali, i checksums, gli hash sicuri, ecc.)
<b>FCS</b>	<b>Comunicazioni</b>	Fornisce due famiglie relative al non-ripudio da parte del mittente e del destinatario dei dati.
<b>FDP</b>	<b>Protezione dei dati utente</b>	Specifica i requisiti relativi alla protezione dei dati utente nel TOE durante l'importazione, l'esportazione e la memorizzazione, gli attributi di sicurezza relativi ai dati utente, memorizzazione off-line, importazione ed esportazione e comunicazioni inter-TSF
<b>FIA</b>	<b>Identificazione e autenticazione</b>	Identificazione utente (anche come alias) e autenticazione, fallimenti delle autenticazioni, attributi utente, qualità dei dati di autenticazione
<b>FMT</b>	<b>Gestione della sicurezza</b>	Gestione degli attributi della sicurezza, dei dati e delle funzioni della TSF, dei ruoli di sicurezza
<b>FPR</b>	<b>Privacy</b>	Questi requisiti forniscono protezione all'utente dalla scoperta e l'abuso di identità da parte di altri
<b>FPT</b>	<b>Protezione delle funzioni di sicurezza del TOE</b>	Questa classe contiene famiglie di requisiti funzionali, che riguardano l'integrità e la gestione dei meccanismi che costituiscono la TSF e l'integrità dei dati TSF
<b>FRU</b>	<b>Utilizzazione delle risorse</b>	Supporta la disponibilità delle risorse necessarie (capacità di lavorazione, capacità di memorizzazione). FRU tratta di: tolleranza ai guasti, priorità dei servizi, allocazione delle risorse.
<b>FTA</b>	<b>Accesso al TOE</b>	Questa famiglia specifica i requisiti funzionali per controllare la creazione di una sessione utente
<b>FTP</b>	<b>Canali/percorsi fidati</b>	Fornire i requisiti per un percorso fidato di comunicazione tra gli utenti e la TSF, e per un canale fidato di comunicazione tra la TSF e altri prodotti IT di fiducia



# Organizzazione dei requisiti



# Esempio di Classe (CC ver. 3.1R2)

FCS Class

**Cryptographic support**

**Cryptographic key management**

FCS\_CKM Family

**Cryptographic operation**

FCS\_COP Family

Cryptographic key generation

FCS\_CKM.1 Component

Cryptographic key distribution

FCS\_CKM.2 Component

Cryptographic key access

FCS\_CKM.3 Component

Cryptographic key destruction

FCS\_CKM.4 Component

Cryptographic operation

FCS\_COP.1 Component

# Corrispondenza fra EAL e requisiti di garanzia – CC ver. 2.3

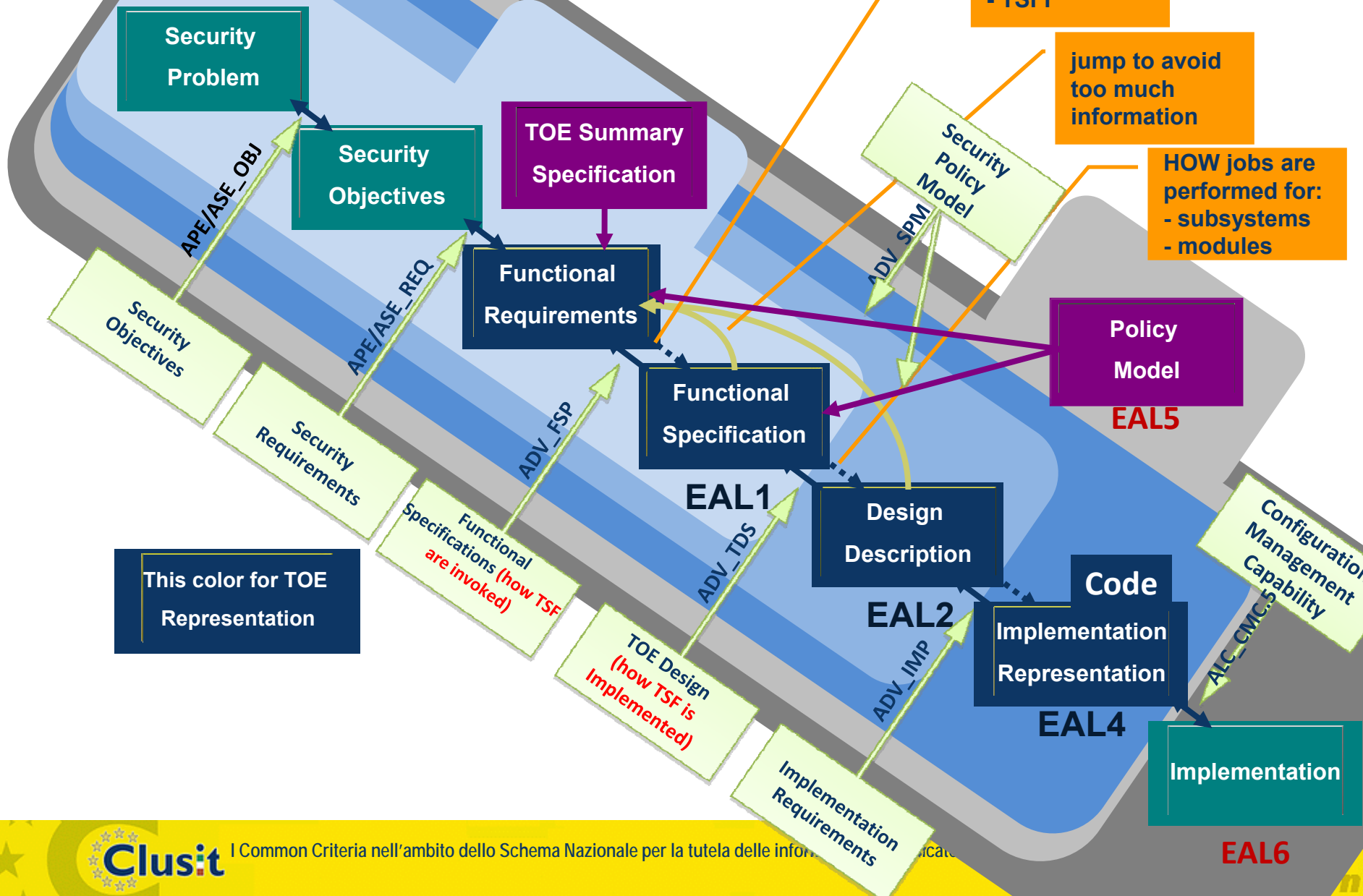
Assurance class	Assurance Family		Assurance components by Evaluation Assurance Level						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT	Automazione della gestione di configurazione				1	1	2	2
	ACM_CAP	Potenzialità della gestione della configurazione	1	2	3	4	4	5	5
	ACM_SCP	Limiti della gestione di configurazione			1	2	3	3	3
Delivery and operation	ADO_DEL	consegna		1	1	2	2	2	3
	ADO_IGS	Installazione, generazione e avvio	1	1	1	1	1	1	1
Development	ADV_FSP	Specifiche funzionali	1	1	1	2	3	3	4
	ADV_HLD	Progetto di alto livello		1	2	2	3	4	5
	ADV_IMP	Rappresentazione dell'implementazione				1	2	3	3
	ADV_INT	Struttura interna delle funzioni di sicurezza					1	2	3
	ADV_LLD	Progetto di basso livello				1	1	2	2
	ADV_RCR	Corrispondenza della rappresentazione	1	1	1	1	2	2	3
	ADV_SPM	Modello della politica di sicurezza				1	3	3	3
Guidance documents	AGD_ADM	Documentazione destinata agli amministratori	1	1	1	1	1	1	1
	AGD_USR	Documentazione destinata agli utenti	1	1	1	1	1	1	1
Life cycle support	ALC_DVS	Sicurezza del processo di sviluppo			1	1	1	2	2
	ALC_FLR	Correzione degli errori							
	ALC_LCD	Definizione del ciclo di vita				1	2	2	3
	ALC_TAT	Strumenti e tecniche				1	2	3	3
Tests	ATE_COV	Copertura dei test		1	2	2	2	3	3
	ATE_DPT	Profondità dei test			1	1	2	2	3
	ATE_FUN	Test funzionali		1	1	1	1	2	2
	ATE_IND	Test indipendenti	1	2	2	2	2	2	3
Vulnerability assesment	AVA_CCA	Analisi dei covert channel					1	2	2
	AVA_MSU	Abuso			1	2	2	3	3
	AVA_SOF	Valutazione della robustezza delle funzioni di sicurezza		1	1	1	1	1	1
	AVA_VLA	Analisi di vulnerabilità		1	1	2	3	4	4



# Corrispondenza fra EAL e requisiti di garanzia – CC ver. 3.1

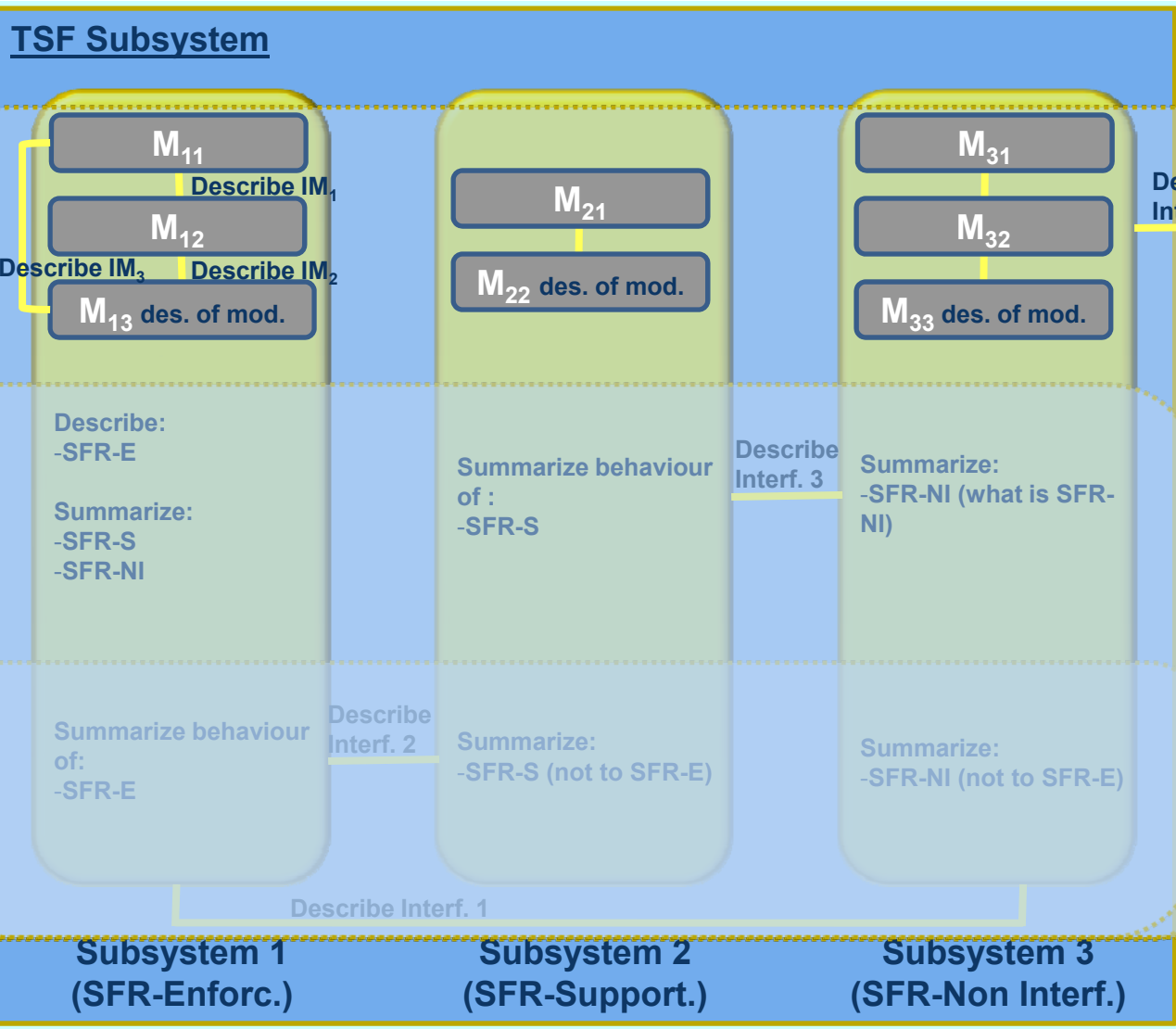
Assurance class	Assurance Family		Assurance compnents by Evaluation Assurace Level						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC	Architettura di sicurezza		1	1	1	1	1	1
	ADV_FSP	Specifiche funzionali	1	2	3	4	5	5	6
	ADV_IMP	Rappresentazione dell'implementazione				1	1	2	2
	ADV_INT	Struttura interna delle funzioni di sicurezza					2	3	3
	ADV_SPM	Modello della politica di sicurezza						1	1
	ADV_TDS	Disegno del TOE		1	2	3	4	5	6
Guidance documentents	AGD_OPE	Guida operativa per gli utenti	1	1	1	1	1	1	1
	AGD_PRE	Procedure di preparazione	1	1	1	1	1	1	1
Life cycle support	ALC_CMC	Proprietà della gestione della configurazioe	1	2	3	4	4	5	5
	ALC_CMS	Limiti della gestione della configurazione	1	2	3	4	5	5	5
	ALC_DEL	Distribuzione		1	1	1	1	1	1
	ALC_DVS	Sicurezza del processo di sviluppo			1	1	1	2	2
	ALC_FLR	Correzione degli errori							
	ALC_LCD	Definizione del ciclo di vita			1	1	1	1	2
	ALC_TAT	Strumenti e tecniche				1	2	3	3
Security Target evaluation	ASE_CCL	Dichiarazioni di conformità	1	1	1	1	1	1	1
	ASE_ECD	Definizione dei componenti estesi	1	1	1	1	1	1	1
	ASE_INT	Introduzione al ST	1	1	1	1	1	1	1
	ASE_OBJ	Obiettivi di sicurezza	1	2	2	2	2	2	2
	ASE_REQ	Requisiti di sicurezza	1	2	2	2	2	2	2
	ASE_SPD	Definizione del problema di sicurezza		1	1	1	1	1	1
	ASE_TSS	Specifiche sommarie del TOE	1	1	1	1	1	1	1
Tests	ATE_COV	Copertura dei test		1	2	2	2	3	3
	ATE_DPT	Profondità dei test			1	2	3	3	4
	ATE_FUN	Test funzionali		1	1	1	1	2	2
	ATE_IND	Test indipendenti	1	2	2	2	2	2	3
Vulnerability assesment	AVA_VAN	Analisi di vulnerabilità	1	2	2	3	4	5	5

# Costrutto ADV



# TDS picture (with $TDS.1 \subset TDS.2 \subset TDS.3$ )

**TOE**



**non-TSF Subsystem**

**Istruzioni:**

- 1 °: identificare ciò che fa e ciò che non fa parte della TDS (ADV\_TDS.2-2)
- 2 °: a causa della presenza di dominio di separazione tra TSF e non-TSF dovrebbe esservi una separazione fisica tra di loro

**NB:** il significato di "summarize" cambia in ogni w.u. del CEM. Leggere attentamente in ogni w.u. per comprendere ciò che significa

**TDS.3 (EAL4)**

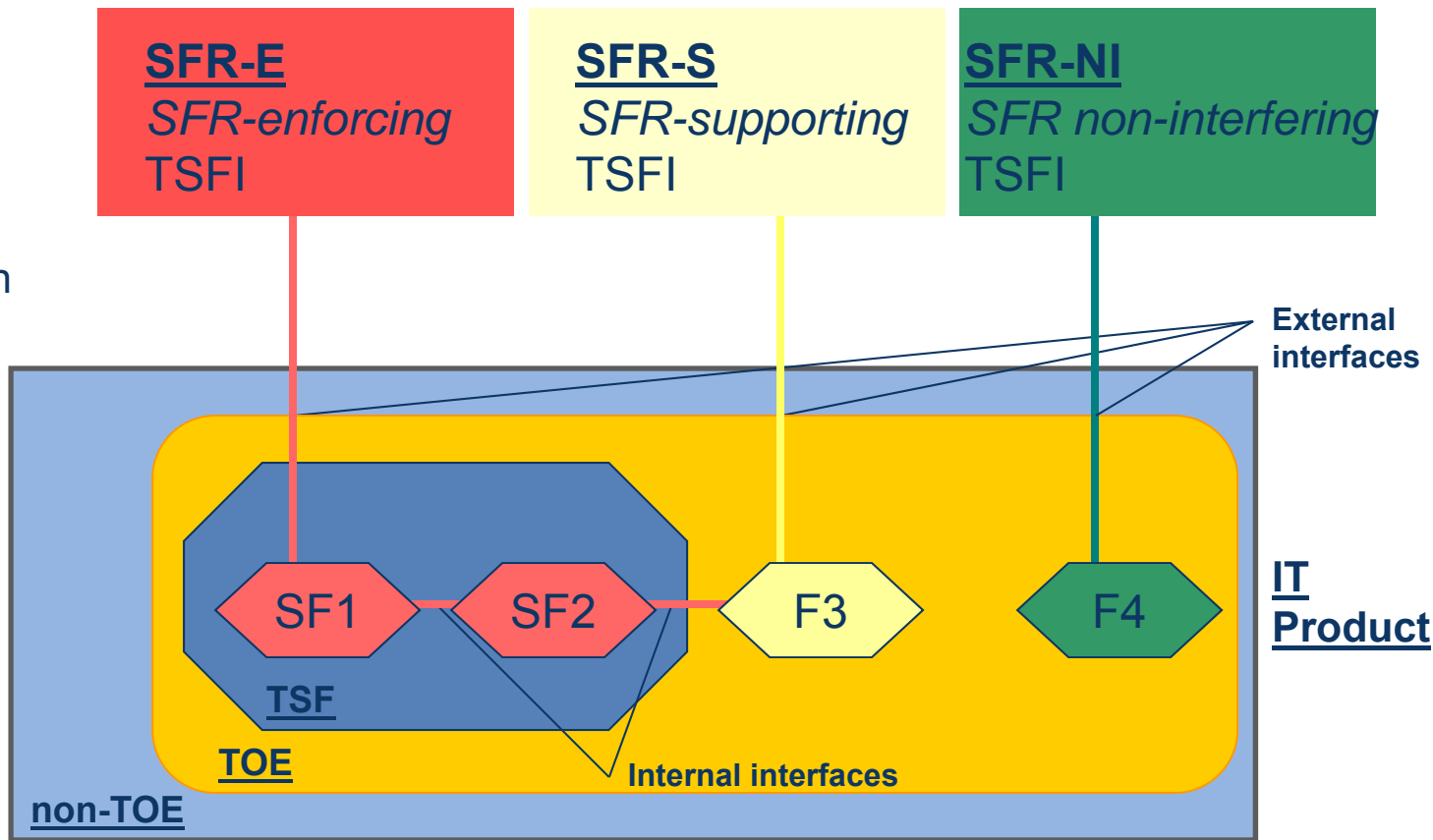
**TDS.2 (EAL3)**

**TDS.1 (EAL2)**

# TSFI (Target Of Evaluation Security Functionality Interface)

**SFR**  
Security Functional Requirements

**TSFI**  
Target of Evaluation Security Functionality Interface



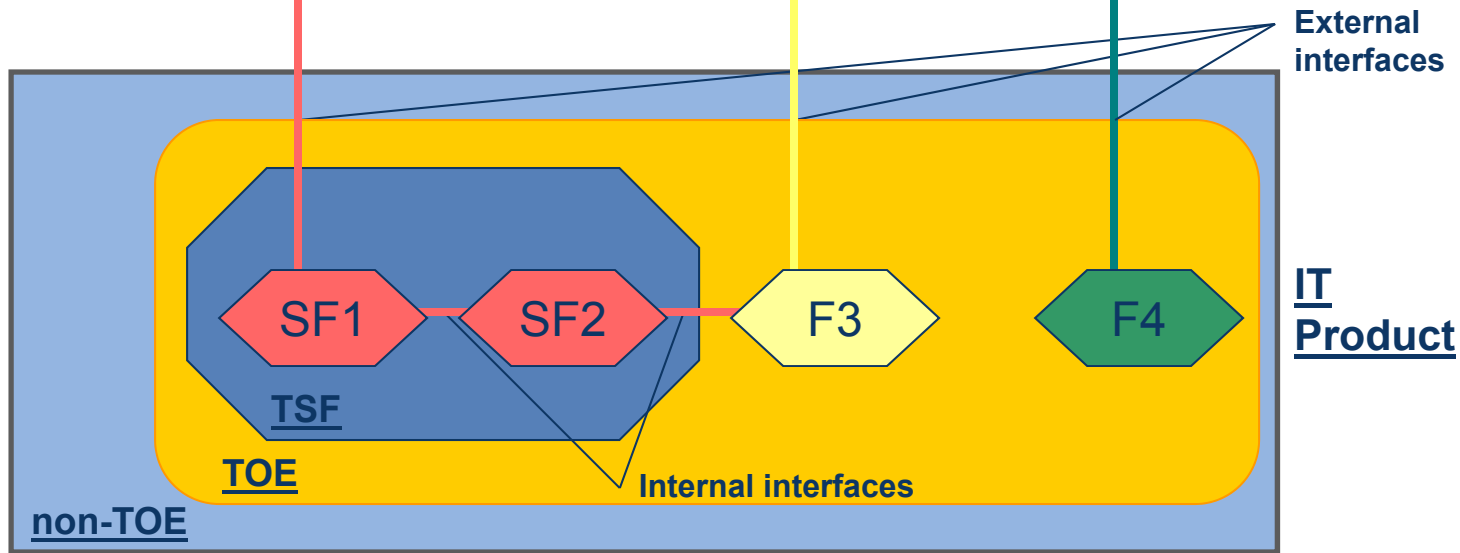
# FSP.1 (EAL1)

	<b>SFR-E</b>	<b>SFR-S</b>	<b>SFR-NI</b>
Purpose	State the purpose	State the purpose	Rationale of SFR-NI
Method of use	Is given	Is given	//
Parameters	Identification	Identification	//
Parameters description	//	//	//
Actions	//	//	//
Error messages descr.	//	//	//

- SFR-E**  
*SFR-enforcing TSFI*
- SFR-S**  
*SFR-supporting TSFI*
- SFR-NI**  
*SFR non-interfering TSFI*

**SFR**  
Security Functional Requirements

**TSFI**  
Target of Evaluation Security Functionality Interface



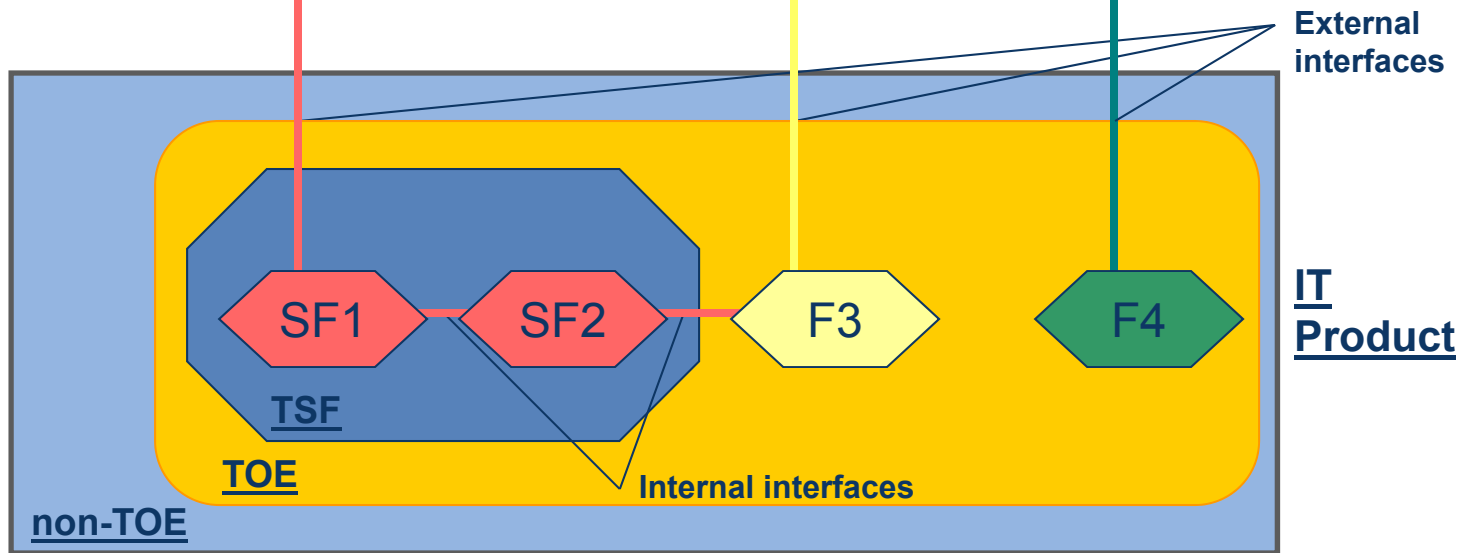
# FSP.2 (EAL2)

	<b>SFR-E</b>	<b>SFR-S</b>	<b>SFR-NI</b>
Purpose	State the purpose	State the purpose	State the purpose
Method of use	Is given	Is given	Is given
Parameters	Complete identification	Complete identification	Complete identification
Parameters description	Compl. & accurate descr.	Compl. & accurate descr.	Compl. & accurate descr.
Actions	Compl. & acc. descr. of SFR-E act.	//	//
Error messages descr.	Compl. & acc. descr. of SFR-E err.	//	//

- SFR-E**  
*SFR-enforcing TSFI*
- SFR-S**  
*SFR-supporting TSFI*
- SFR-NI**  
*SFR non-interfering TSFI*

**SFR**  
Security Functional Requirements

**TSFI**  
Target of Evaluation Security Functionality Interface



# FSP.3 (EAL3)

	<b>SFR-E</b>	<b>SFR-S</b>	<b>SFR-NI</b>
Purpose	State the purpose	State the purpose	State the purpose
Method of use	Is given	Is given	Is given
Parameters	Complete identification	Complete identification	Complete identification
Parameters description	Compl. & accurate descr.	Compl. & accurate descr.	Compl. & accurate descr.
Actions	Compl. & acc. descr. of SFR-E act.	Summarises SFR-S act.	Summarises SFR-S act.
Error messages descr.	Compl. & acc. descr. of SFR-E err. msgs & assoc. exceptions	//	//

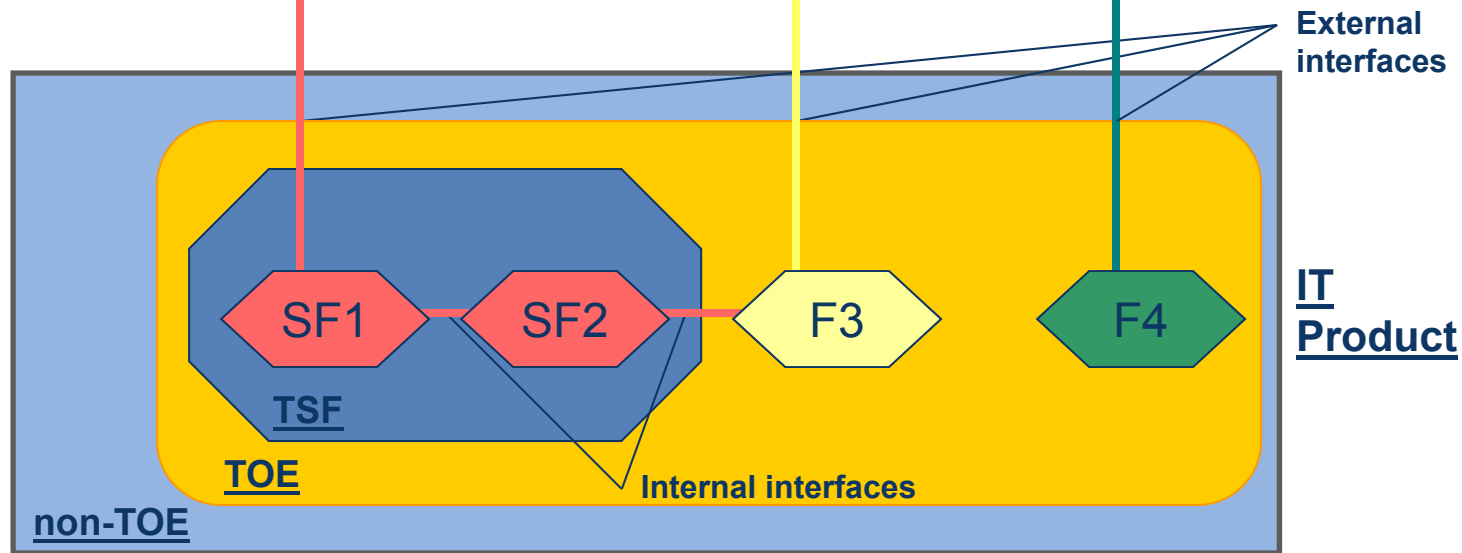
**SFR-E**  
SFR-enforcing TSFI

**SFR-S**  
SFR-supporting TSFI

**SFR-NI**  
SFR non-interfering TSFI

**SFR**  
Security Functional Requirements

**TSFI**  
Target of Evaluation Security Functionality Interface



# FSP.4 (EAL4)

	<u>SFR-E</u>	<u>SFR-S</u>	<u>SFR-NI</u>
Purpose	State the purpose	State the purpose	State the purpose
Method of use	Is given	Is given	Is given
Parameters	Complete identification	Complete identification	Complete identification
Parameters description	Compl. & accurate descr.	Compl. & accurate descr.	Compl. & accurate descr.
Actions	Compl. & acc. descr. of SFR-E act.	Compl. & acc. descr. of SFR-E act.	Compl. & acc. descr. of SFR-E act.
Error messages descr.	Compl. & acc. descr. + meaning of SFR-E err. msgs & assoc. exceptions	Compl. & acc. descr. + meaning of SFR-E err. msgs & assoc. exceptions	Compl. & acc. descr. + meaning of SFR-E err. msgs & assoc. exceptions

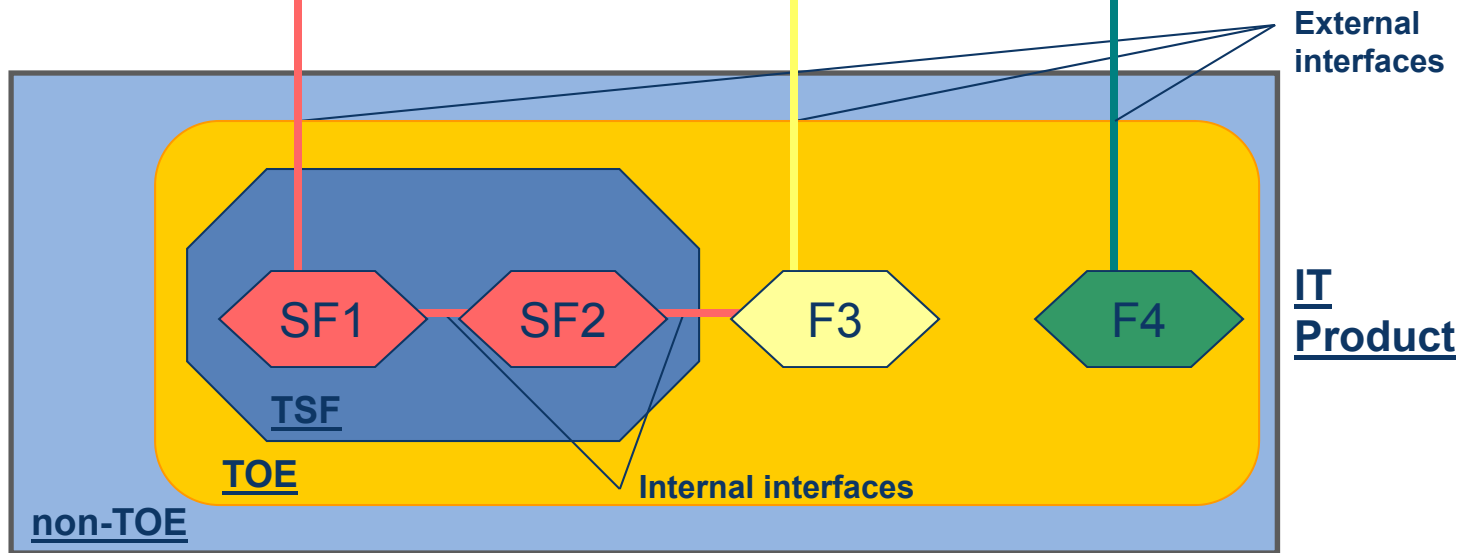
SFR-E  
SFR-enforcing TSFI

SFR-S  
SFR-supporting TSFI

SFR-NI  
SFR non-interfering TSFI

SFR  
Security Functional Requirements

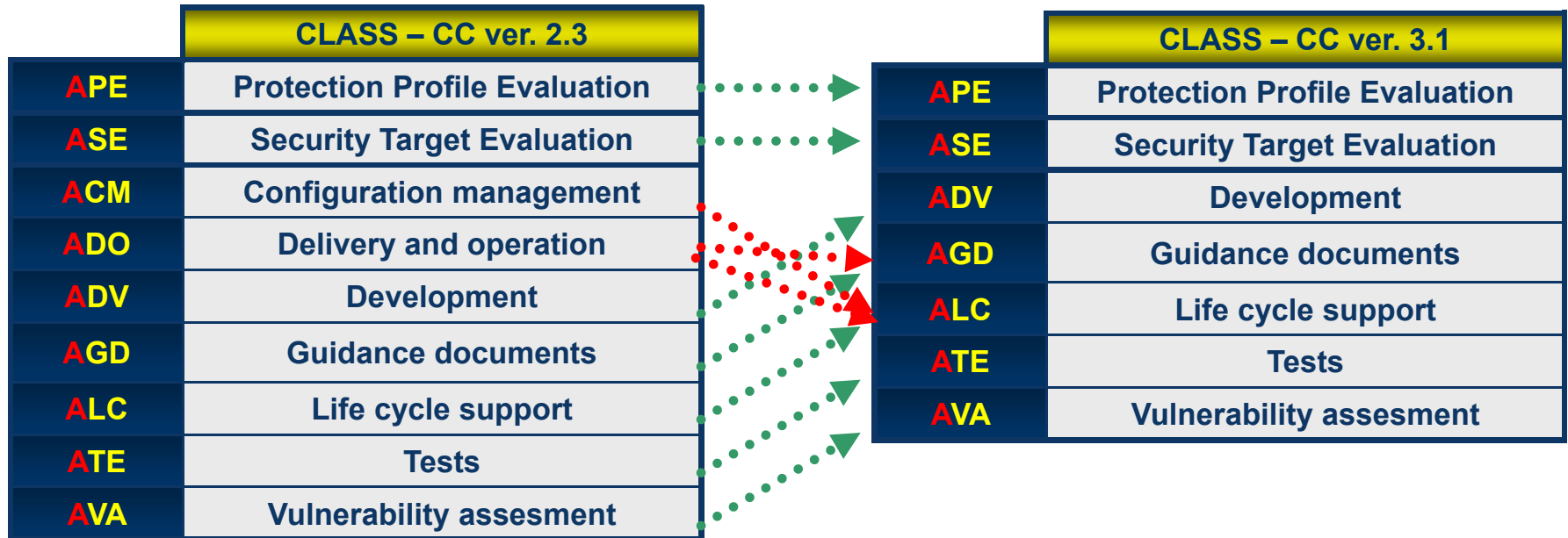
TSFI  
Target of Evaluation Security Functionality Interface



# Le 1+1+5+1 SAR – CC ver. 3.1

	CLASS	DESCRIPTION
<b>APE</b>	Valutazione del PP	Necessaria per dimostrare che il <b>PP è tecnicamente valido e internamente coerente</b> , e che il PP sia una, eventuale, corretta implementazione di questi PP e dei “ <i>packages</i> ”
<b>ASE</b>	Valutazione del ST	Richiesta per dimostrare quanto riportato sopra per l’APE. Queste proprietà sono necessarie perchè il ST sia <b>idoneo ad essere utilizzato come base per la valutazione di un TOE</b>
<b>ADV</b>	Sviluppo	L’obiettivo della attività di sviluppo è quello di valutare la documentazione di progetto in termini di adeguatezza <b>per capire come la TSF soddisfa le SFR</b> e come <b>l’implementazione di tali SFR non può essere manomessa o aggirata</b>
<b>AGD</b>	Documenti di supporto	Fornisce i requisiti per la documentazione di supporto per tutti i ruoli degli utenti. La classe relativa ai documenti di supporto è suddivisa in due famiglie che sono relative alla <b>guida utente per la preparazione</b> e alla <b>guida utente per l’utilizzo</b>
<b>ALC</b>	Supporto durante il ciclo di vita	Determinare <b>l’adeguatezza delle procedure relative a: modello del ciclo di vita utilizzato dagli sviluppatori</b> , gestione della configurazione, misure di sicurezza utilizzate durante lo sviluppo, gestione dei problemi di sicurezza, e attività di consegna
<b>ATE</b>	Verifiche	Determinare <b>se il TOE si comporta come descritto nel ST</b> . Le famiglie di questa classe sono attinenti all’ampiezza e alla profondità delle verifiche dello sviluppatore e ai requisiti per le verifiche indipendenti
<b>AVA</b>	Valutazione vulnerabilità	Determinare la <b>possibilità di sfruttare difetti o carenze del TOE nell’ambiente operativo</b> , basata sulle precedenti attività e su una ricerca di materiale pubblicamente disponibile, per finire con le prove di penetrazione
<b>ACO</b>	Composizione	L’analisi delle <b>vulnerabilità del TOE composto</b> sfrutta i risultati dell’analisi delle vulnerabilità delle valutazioni dei componenti

# Riorganizzazione classi di assurance

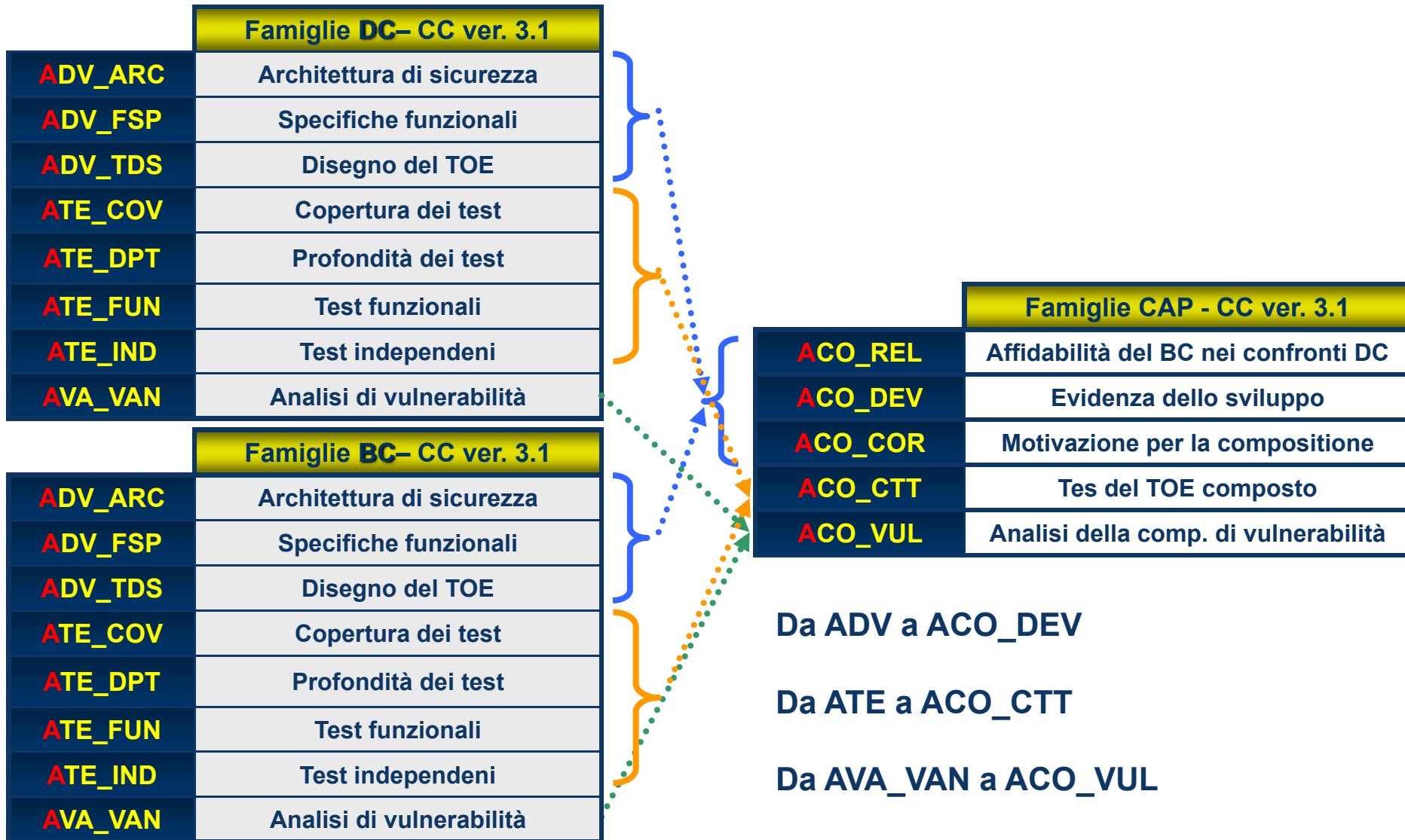




# Corrispondenza fra CAP e requisiti di garanzia – CC ver. 3.1

Assurance class	Assurance Family		Assurance compnents by Composed Assurance Packages		
			CAP-A	CAP-B	CAP-C
Composition	ACO_COR	Motivazione per la composizione	1	1	1
	ACO_CTT	Test del TOE composto	1	2	2
	ACO_DEV	Evidenza dello sviluppo	1	2	3
	ACO_REL	Affidabilità del BC nei confronti DC	1	1	2
	ACO_VUL	Analisi della comp. di vulnerabilità	1	2	3
Guidance documentents	AGD_OPE	Guida operativa per gli utenti	1	1	1
	AGD_PRE	Procedure di preparazione	1	1	1
Life cycle support	ALC_CMC	Proprietà della gestione della configurazione	1	1	1
	ALC_CMS	Limiti della gestione della configurazione	2	2	2
	ALC_DEL	Distribuzione			
	ALC_DVS	Sicurezza del processo di sviluppo			
	ALC_FLR	Correzione degli errori			
	ALC_LCD	Definizione del ciclo di vita			
	ALC_TAT	Strumenti e tecniche			
Security Target evaluation	ASE_CCL	Dichiarazioni di conformità	1	1	1
	ASE_ECD	Definizione dei componenti estesi	1	1	1
	ASE_INT	Introduzione al ST	1	1	1
	ASE_OBJ	Obiettivi di sicurezza	1	2	2
	ASE_REQ	Requisiti di sicurezza	1	2	2
	ASE_SPD	Definizione del problema di sicurezza		1	1
	ASE_TSS	Specifiche sommarie del TOE	1	1	1

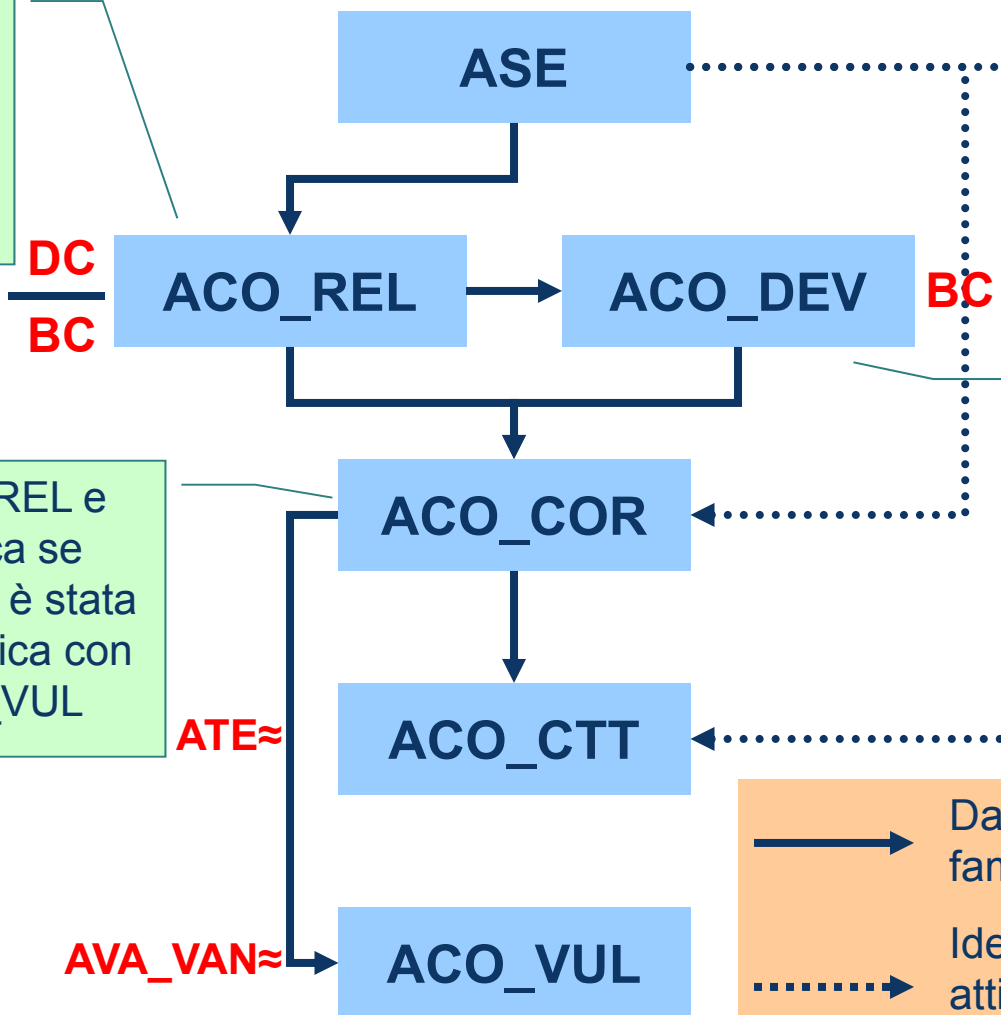
# Rapporto EAL (DC e BC) e CAP





# Assurance COmposition

Come la TSF del DC si protegge (da interfer. & tamper.) dal BC (punto di vista sviluppatore DC)



Comparando ACO\_REL e ACO\_DEV identifica se qualche specifica non è stata considerata e la verifica con ACO\_CTT e ACO\_VUL

Scopo TSF del BC Comport. HLD del BC Subsystem BC

→ Dati famiglia input per famiglia successiva  
..... Identifica quando una attività si riconduce alle SFR del TOE composto

# Domande?



# Centro di Valutazione della Difesa



**Ten. Col. Luciano PORCELLI**

*Capo Sezione Metodologia di  
Valutazione del Ce.Va. Difesa*

*Via della Bigattiera lato monte, 10  
c/o CISAM 56122 - San Piero a grado (PI)*

*Tel./Fax: 050.964.317*

*e-Mail: [ris.csmvceva@smd.difesa.it](mailto:ris.csmvceva@smd.difesa.it)  
[ceva.difesa@cisam.it](mailto:ceva.difesa@cisam.it)*