



CC Common Criteria

ISO/IEC 15408

Common Criteria: Caratteristiche



- Forniscono un'**istantanea** della sicurezza di un prodotto o di un sistema
- Il risultato è significativo quando il prodotto è **utilizzato nelle condizioni in cui è stato valutato**
- Il processo di valutazione ha **una durata commisurata al livello di severità**
- <http://www.commoncriteriaportal.org/>

Livelli di Sicurezza

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Livello di assurance crescente



- Sicurezza maggiore

- Componenti di livello gerarchico più elevato (numeri identificativi più grandi)



Common Criteria

- Scaricare documentazione da <http://www.commoncriteriaportal.org>
- CC v3.1 in tre parti
 - Parte 1 R1: Introduzione e modello generale
 - Parte 2.R2 : Requisiti funzionali di sicurezza
 - Parte 3.R2: Requisiti di assurance
- CEM Common Criteria Evaluation Methodology
- PP Protection Profile
- Esempi di Certificazioni

Gli attori interessati ai CC

	Consumers	Developers	Evaluators
Part 1	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference purposes. Development of 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 a TOE.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Use for reference when interpreting statements of functional requirements.
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 for reference when interpreting statements of assurance requirements.

Significato CC

- Ha senso certificare che un apparato ICT è sicuro solo se si specifica:
 - sicuro per fare cosa (obiettivi di sicurezza)
 - sicuro in quale contesto (ambiente di sicurezza)
 - sicuro a fronte di quali verifiche eseguite (soddisfacimento requisiti di assurance)

In altri termini: la valutazione della sicurezza secondo i CC ha lo scopo di offrire garanzie (assurances), che è possibile graduare, sulla capacità del TOE di soddisfare i propri obiettivi di sicurezza nell'ambiente di sicurezza per esso ipotizzato



Target Of Evaluation (TOE)

- Costituisce l'Oggetto Della Valutazione (ODV), può essere:
 - un prodotto, cioè un pacchetto IT che può essere acquistato e impiegato in svariati ambienti operativi
 - un sistema, cioè una specifica installazione IT per cui sono definiti a priori lo scopo e l'ambiente operativo



Target Of Evaluation (TOE). Esempi

- una applicazione software;
- un Sistema Operativo
- una Applicazione Software in un Sistema Operativo
- una Applicazione Software in un Sistema Operativo in una workstation;
- un circuito integrato di smartcard
- co-processor crittografico del circuito integrato di una smartcard
- una Local Area Network compresi terminali, server, dispositivi di rete e software:
- una applicazione di database con esclusione del client associato con tale applicazione



Target Of Evaluation (TOE/OdV).

Esempi

- ToE: una specifica CONFIGURAZIONE di SISTEMA OPERATIVO

Tipo di utenti

numero di utenti

tipo di connessioni esterne

tipo di connessioni consentite/non consentite

opzioni abilitate/disabilitate

- Un SOTTINSIEME di CONFIGURAZIONI puo' essere collettivamente considerato un ToE

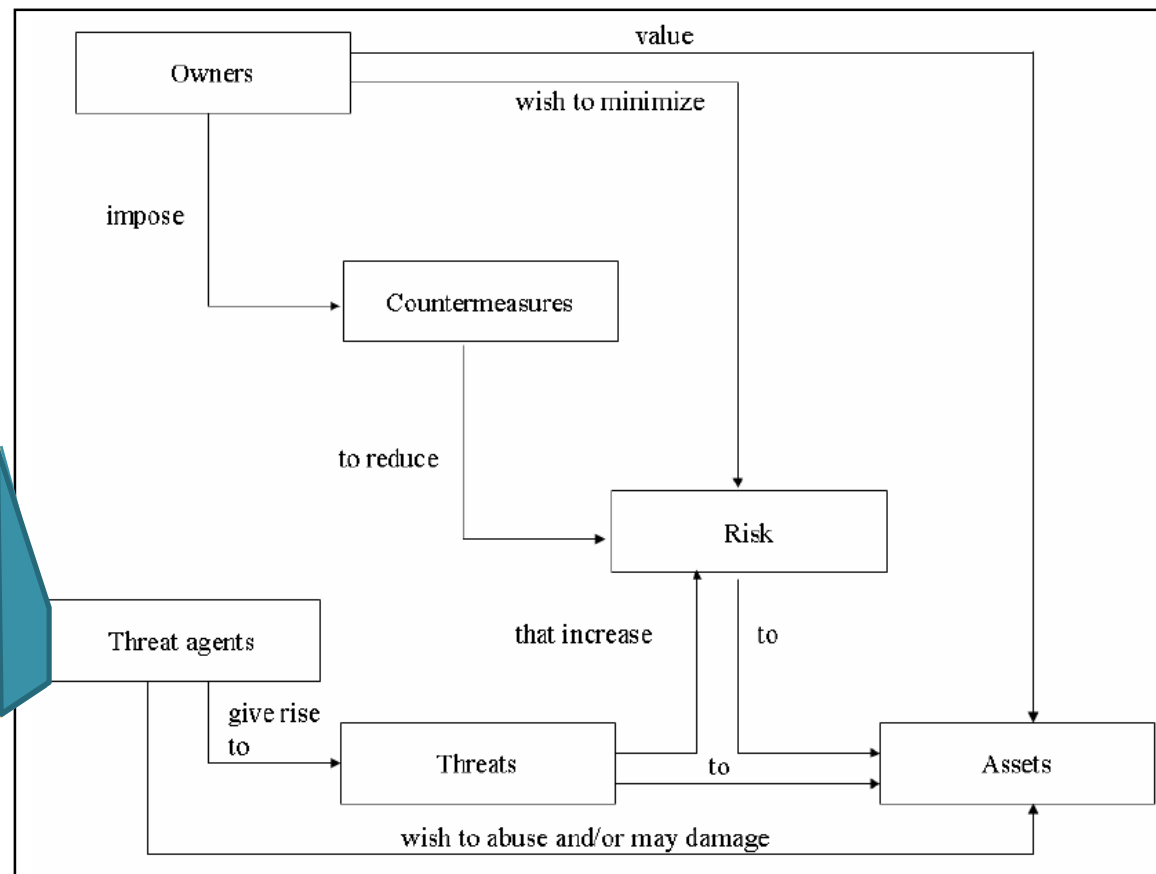


Asset & Ambiente Operativo

- Asset=entità cui viene dato valore, sono il “bene” da proteggere
- Esempi di asset
 - contents of a file or a server;
 - the authenticity of votes cast in an election;
 - the availability of an electronic commerce process
 - the ability to use an expensive printer;
 - access to a classified facility.
- Ambiente in cui l'asset e' collocato
- Esempi di ambienti operativi
 - the computer room of a bank;
 - connected to the Internet;
 - a LAN;
 - a general office environment.

Assets Owners: hanno interesse a proteggere gli asset

Hacker
Malicious users
Non malicious users (sbagli)
Processi
Incidenti





Contromisure per ridurre il Rischio

- Contromisure IT (smart card, firewall...)
- Contromisure non-IT (guardie, procedure...)
- Proprietà Contromisure
 - Sufficienti: se adottate neutralizzano le minacce
 - Corrette: realizzano cio' che promettono

Security Target (ST)

- E' un documento che definisce il Traguardo Di Sicurezza (TDS), in termini di:
 - Beni(asset)
 - Minacce agli asset
 - Ipotesi
 - Ambiente operativo
- Le contromisure sono descritte come:
 - Obiettivi di sicurezza(Security Objectives)
 - Obiettivi di sicurezza del ToE (che saranno oggetto della valutazione)
 - Obiettivi di sicurezza dell'ambiente operativo (che NON saranno oggetto di valutazione)
- Security Functional Requirements (SFRs) descritti in CC parte 2
 - Descrivono in dettaglio le funzionalita' di sicurezza richieste
- Il Security Target costituisce una base per dimostrare che:
 - Gli SFR corrispondono agli obiettivi di sicurezza del ToE
 - Gli obiettivi di sicurezza del ToE e dell'ambiente operativo contrastano le minacce
 - E quindi gli SFR e i security objective dell'ambiente operativo contrastano le minacce



TOE

- Dimostrare la sicurezza del TOE
 - Testare il TOE;
 - Controllarne il progetto a vari livelli
 - Controllare la sicurezza dell'ambiente di sviluppo
- ST fornisce un modo strutturato di specificare dei Security Assurance Requirements
- più forti sono i SAR più forte è il **livello di assurance**



La EVALUATION

- Valutazione del Security Target: valuta la sufficienza del TOE e dell'ambiente operativo sono sufficienti (utilizza il CC parte 3 capitolo ASE)
- Valutazione del TOE: valuta la correttezza del TOE (il TOE, ambiente di sviluppo, documenti di sviluppo, test)



Packages

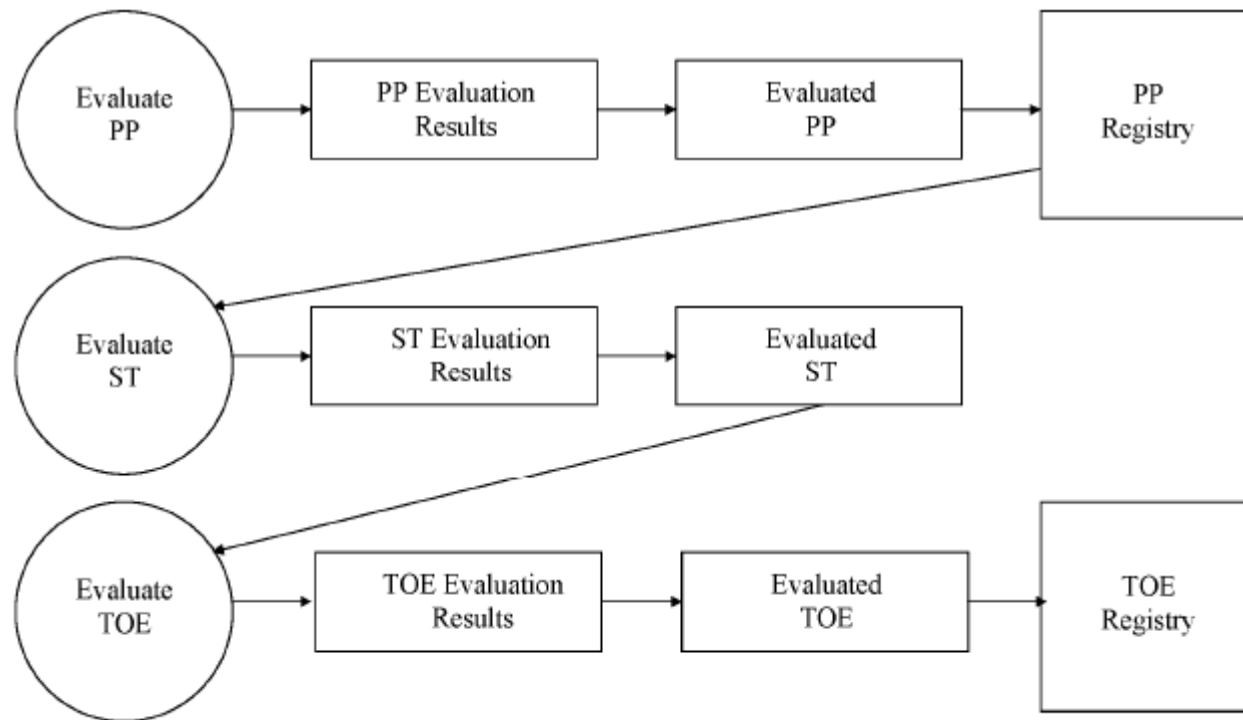
- Package funzionali, contengono solo SFR (CC part 2)
 - Non vi sono standard
- Assurance package contengono solo SAR (CC part 3)
 - gli Evaluation Assurance Level EAL sono esempi di package



Protection Profile (PP)

- Un Protection Profile è una specifica indipendente di requisiti di Sicurezza
- un ST descrive sempre un TOE specifico (e.s MinuteGap v18.5 Firewall)
- un PP descrive una classe di TOE (es.i firewall)
- Costituisce un modello/template di Security Target riusabile
- Normalmente è creato da una società o da un gruppo di utenti, agenzie governative (es.NSA) etc.
- un PP può essere valutato/certificato e quindi facilita il processo di valutazione di un ST

Il processo di valutazione



- il ST può anche essere basato su un PP non certificato/valutato

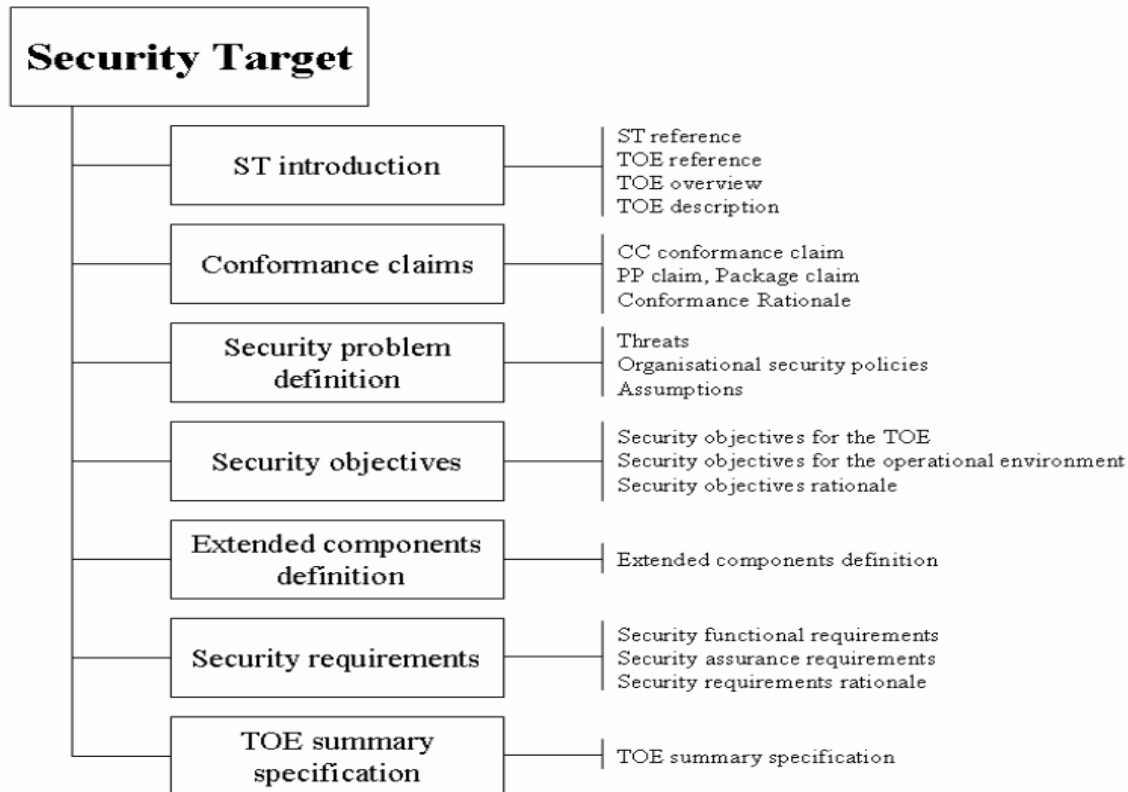


La Dichiarazione di Conformità CC

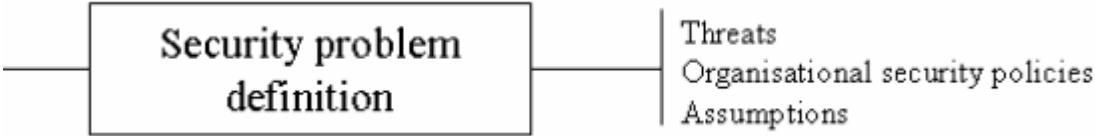
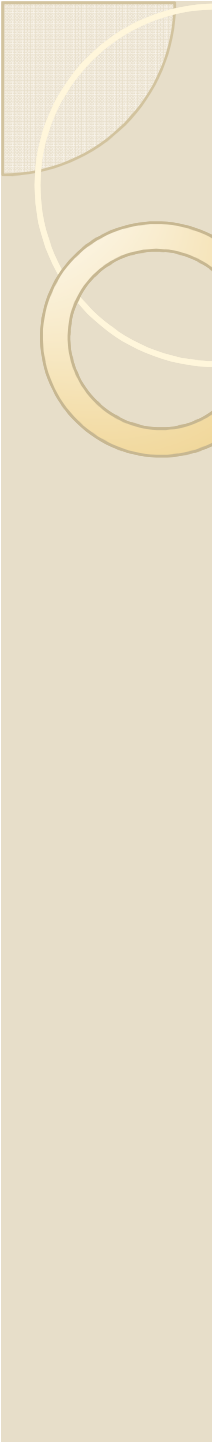
La *conformance claim* indica l'insieme di requisiti verificati dal PP o dall'ST che supera la valutazione deve dichiarare:

- **Versione dei CC di riferimento**
- **Conformità alla parte 2**
 - **CC part 2 conformant**, se tutti gli SFR sono basati solo su componenti funzionali descritti nella parte 2
 - **CC part 2 extended**, se almeno un SFR non è basato su componenti funzionali della parte 2
- **Conformità alla parte 3**
 - **CC part 3 conformant**, se tutti gli SAR sono basati solo su *assurance components* descritti nella parte 3
 - **CC part 2 extended**, se almeno un SAR non è basato su *assurance components* della parte 3
- **Conformità ad un package (es. EAL)**
 - **Package Name conformant**, se tutti gli SFR e gli SAR sono IDENTICI ai SFR/SAR del package
 - **Package Name augmented**, se tutti gli SFR e gli SAR sono IDENTICI ai SFR/SAR del package ma ve ne sono di *aggiuntivi o di gerarchicamente superiori*

Struttura di un Security Target



- **Deve definire a** (relativamente) **alto livello** cosa viene valutato
- **NON dovrebbe essere una descrizione dettagliata** di algoritmi, protocolli, meccanismi, operazioni dettagliate
- **NON dovrebbe essere una specifica completa** di tutto ma solo di elementi rilevanti alla sicurezza, sono da escludere se non rilevanti ad es. peso, voltaggio, dimensioni etc.



Security problem
definition

Threats
Organisational security policies
Assumptions

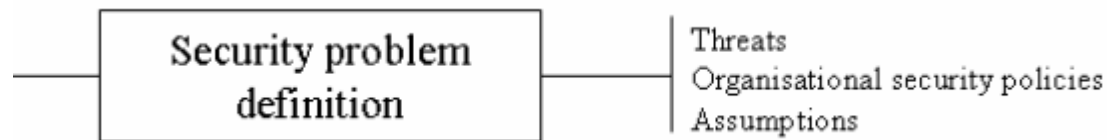
- **Minacce (Threats), esempi:**

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network;
- a worm seriously degrading the performance of a wide-area network;
- a system administrator violating user privacy;
- Someone on the Internet listening in on confidential electronic communication.

- **Politiche di Sicurezza, esempi:**

- All products that are used by the Government must conform to the National Standard for password generation and encryption;
- Only users with System Administrator privilege and clearance of Department Secret shall be allowed to manage the Department Fileserver.

- **Ipotesi (segue)**



• Ipotesi (Assumption) su:

aspetti fisici dell'ambiente operativo

- It is assumed that the TOE will be placed in a room that is designed to minimise electromagnetic emanations;
- It is assumed that the administrator consoles of the TOE will be placed in a restricted access area.
- Assumptions on personnel aspects of the operational environment:
 - It is assumed that users of the TOE will be trained sufficiently in order to operate the TOE;
 - It is assumed that users of the TOE are approved for information that is classified as NationalSecret;
 - It is assumed that users of the TOE will not write down their passwords.

connettività dell'ambiente operativo

- It is assumed that a PC workstation with at least 10GB of disk space available to run the TOE
- It is assumed that the TOE is the only non-OS application running on this workstation;
- It is assumed that the TOE will not be connected to an untrusted network.



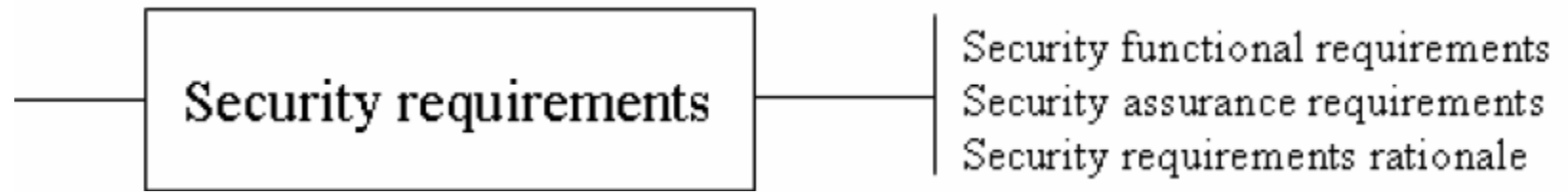
- **Security Objective for the TOE, descrizione in linguaggio naturale degli obiettivi, esempi:**
 - The TOE shall keep confidential the content of all files transmitted between it and a Server;
 - The TOE shall identify and authenticate all users before allowing them access to the Transmission Service provided by the TOE;
 - The TOE shall restrict user access to data according to the Data Access policy described in Annex 3 of the ST.
- **Sec.Objective per Ambiente Operativo**
 - The operational environment shall provide a workstation with the OS Inux version 3.01b to execute the TOE on;
 - The operational environment shall ensure that all human TOE users receive appropriate training before allowing them to work with the TOE;
 - The operational environment of the TOE shall restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel;
- **Sec.Obj.Rationale**
 - un collegamento che mostri quale Sec.Obj si riferisce a quale minaccia, policy(OSP), e ipotesi
 - un insieme di giustificazioni che dimostri che tutte le minacce/OSP/ e ipotesi sono efficacemente trattate dai security objective



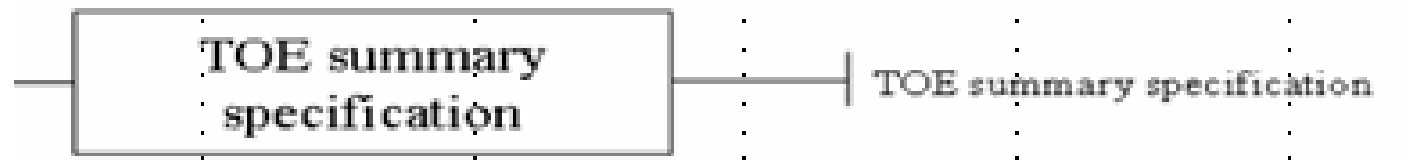
- Una minaccia può essere contrastata efficacemente:
 - Rimuovendola
 - Protezione definitiva, rimozione processo/hardware etc.
 - Diminuendola
 - Tramite deterrenti, restringendo gli accessi/opportunità
 - Mitigandone gli effetti
 - Es. frequenti backup
 - Assicurazione
 - Rilevazione e monitoraggio frequente



- Descrizione di eventuali componenti che non sono ne' in CC Part2 ne' in CC part 3



- **Sec.Funct Req.** traduzione dei TOE **security objectives** descritti secondo il linguaggio standard CC part2
 - Il SecReq “rationale” ne spiega le relazioni con i Sec.Obj.
- **Sec.Ass Req.** descritti secondo gli standard CC part 3, spiegano come il TOE deve essere valutato
 - dipendenze tra SAR, e operazioni su SAR(assegnamento, selezione, iterazione, raffinamento)
 - Il Sec Req. Rationale contiene le motivazione per i SAR



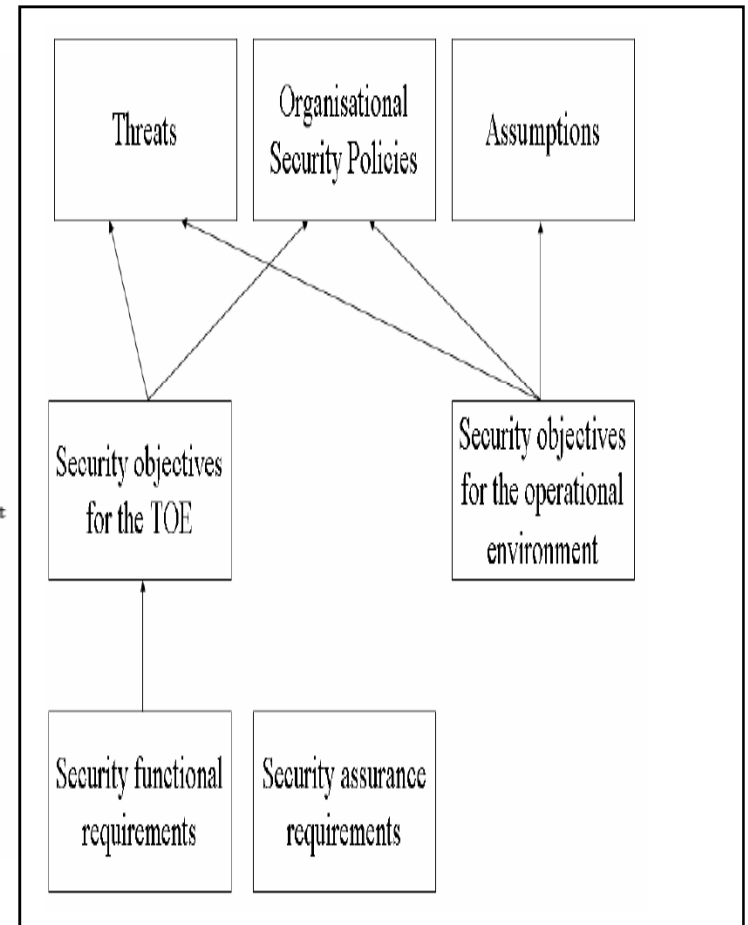
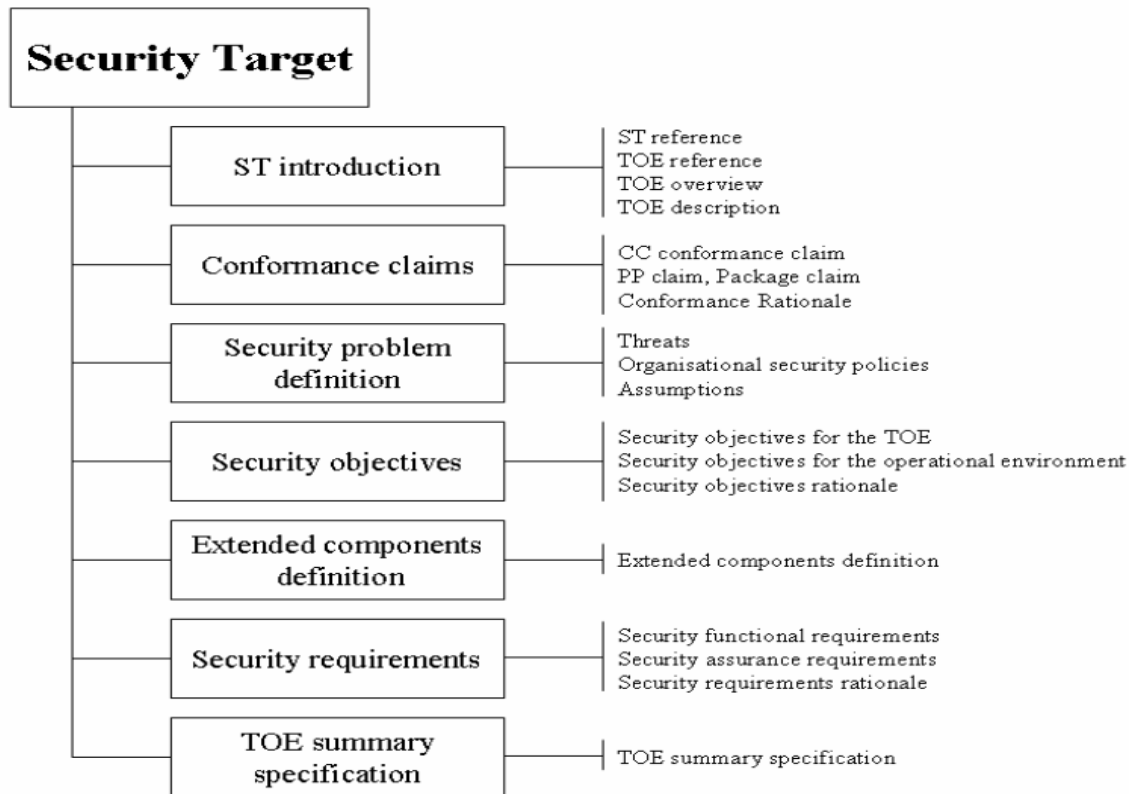
- ## TOE Summary Specification

Contiene una descrizione per utenti potenziali di come il TOE soddisfa tutti gli SFRs, descrive il meccanismo tecnico generale utilizzato dal TOE a questo scopo.

Il livello di dettaglio dovrebbe essere comprensibile all'utente.

- Es. Se c'è una SFR FIA_UAU.I per l'autenticazione il summary dovrebbe spiegare come avviene l'autenticazione

Security Target



Security Target: le domande a cui risponde

- Come trovare il ST/TOE giusto tra tanti? **TOE Overview**
- Questo TOE si adatta alla mia infrastruttura IT? **TOE overview**
identifica gli elementi hardware/firmware/software principali necessari;
- Questo TOE si adatta al mio ambiente operativo? **Security objectives**
per l'ambiente operativo, vincoli
- Cosa fa il TOE (interested reader)? Nella **TOE overview** c'è un breve sommario
- Cosa fa il TOE (potential consumer)? Nella **TOE description**
- Cosa fa il TOE (technical)? Nella **TOE summary specification** c'è una descrizione ad alto livello dei meccanismi usati dal TOE;
- Cosa fa il TOE (expert)? gli **SFRs** sono una descrizione astratta molto tecnica, la **TOE summary specification** fornisce ulteriori dettagli
- Il TOE risponde al problema come definito dal mio governo/organizzazione? Se il governo/organizzazione ha definito dei **packages e/o PPs** allora la risposta è nella **Conformance Claims section** che lista tutte le compatibilità con package e PP
- Il TOE risponde ai miei problemi di sicurezza(expert)? Quali sono le minacce contrastate dal TOE? Quali policy di sicurezza realizza? Quali ipotesi sull'ambiente operativo? **Security problem definition**;
- Quanta fiducia posso riporre nel TOE? **SARs** nella parte **security requirements**, fornisce il livello di assurance level usato per valutare il TOE, e quindi la fiducia che nella correttezza del TOE

