Managing IT security using Common Criteria

ISACA – CETIC Meeting

23 May 2007

Objectives

- Explain what are the Common Criteria
- Explain how to use them effectively
- Illustrate on examples
- Focus:
  - Security Requirements
  - Auditor point of view

2

Overview

- IT Security
- Security Evaluations
- The Common Criteria approach
  - A bit of history, actors, terminologies
  - Process description with examples
  - Document structure and justification
  - Assurance levels
- Model-based support
  - A requirements engineering approach
  - Document management
- Conclusions
- References

3

IT - Security

- process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption
- through the protection the confidentiality, integrity and availability of information
- Complements SAFETY = prevent errors caused by **<u>unintentional</u>** damage or malfunctions

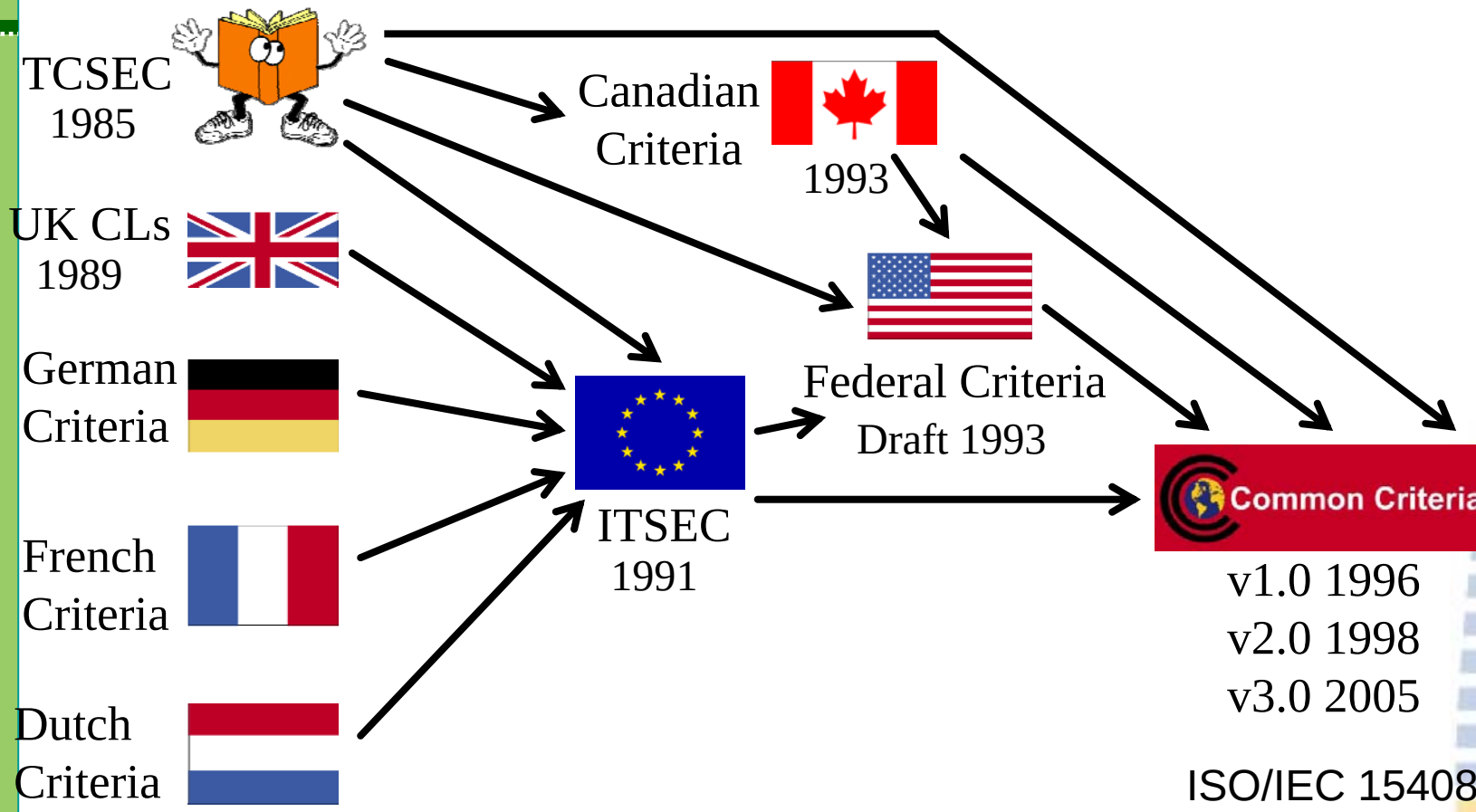
4

Security Evaluation

- Independent (third party) attestation of a developer's security claims against a defined security evaluation criteria.
- Evaluations result in **independent** measure of assurance, therefore build confidence in security.
- Secures development **process** and yields better product.
- Comprehensive security solutions cannot be evaluated by **simple examination**!

5

Evolution of Evaluations: towards the Common Criteria



Note: EBIOS

6

Common Criteria Purpose

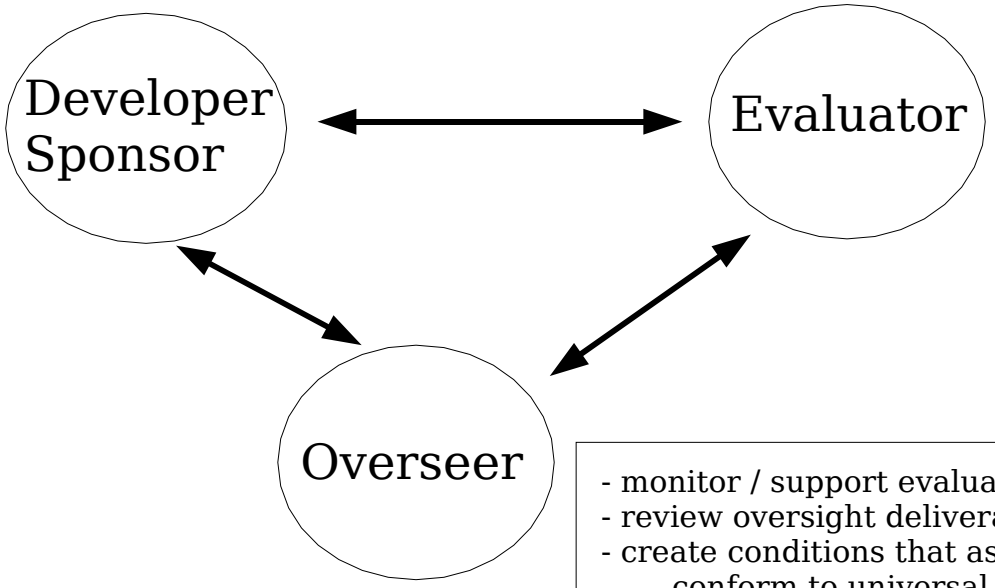
- From the User perspective:
  - A way to **define** Information Technology (IT) security **requirements** for some IT products:
    - Hardware
    - Software
    - Combinations of above
- From the Developer/Vendor perspective:
  - A way to **describe** security **capabilities** of their specific product
- From the Evaluator/Scheme perspective:
  - A tool to **measure** the **belief** we may attain about the security characteristics of a product.

7

Evaluation Parties

- establish agreements
- assure provision of evaluation deliverables
- support evaluation
- develop and maintain evaluation evidence

- perform CC evaluator actions
- request and receive support
- provide oversight deliverables
- document and justify verdicts



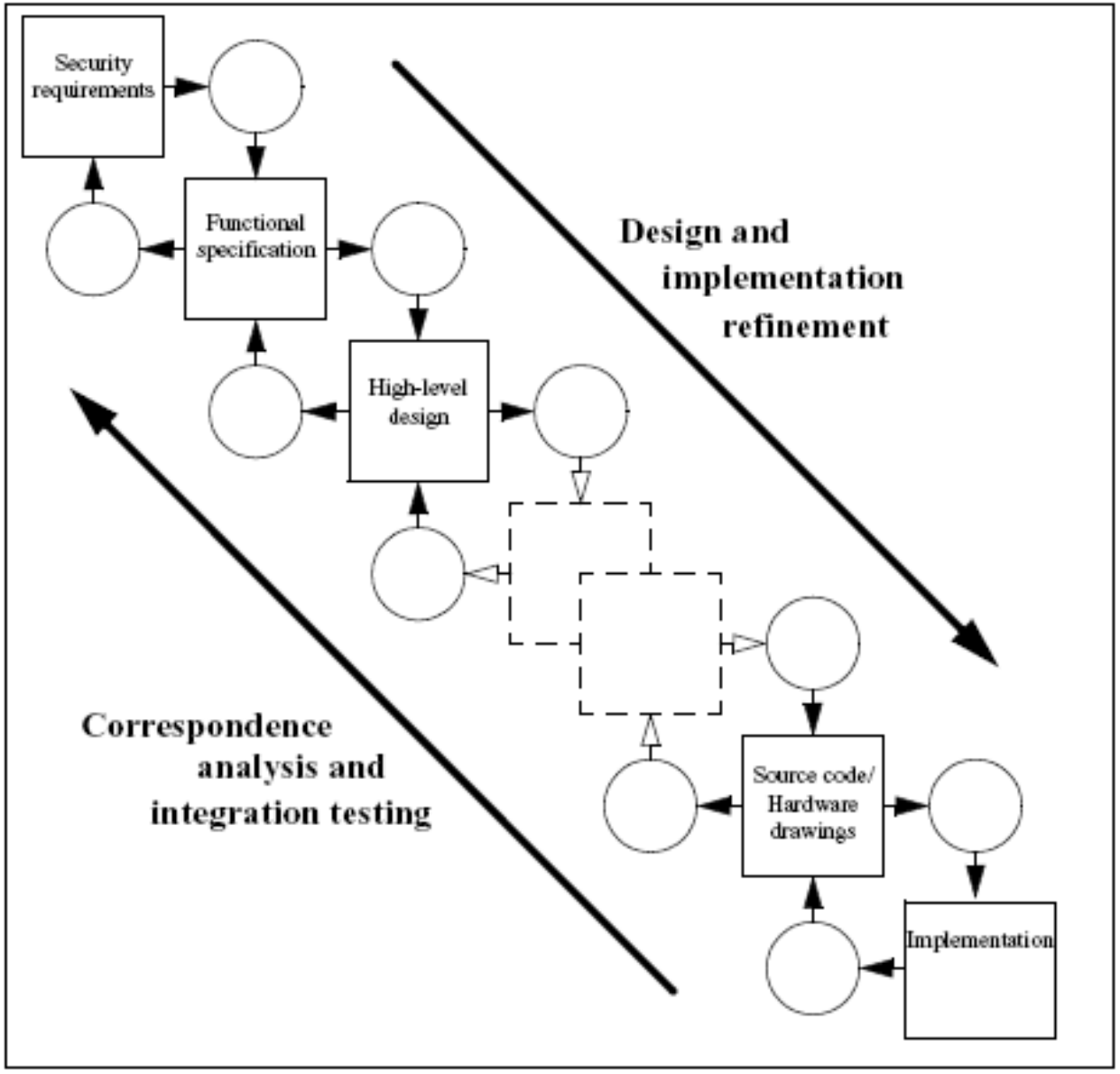
- monitor / support evaluations
- review oversight deliverables
- create conditions that assure evaluations conform to universal principles
- approve or disapprove the overall verdict
- document and justify the oversight verdict

8

Common Criteria (CC) Terminologies

- **TOE: target of evaluation** = the product or system that is the subject of the evaluation
- **SFRs: Security Functional Requirements** = specify individual security functions which may be provided by a product
- **PP: protection profile** = a document, typically created by a user or user community, which identifies security requirements relevant to that user for a particular purpose. **Implementation independent**
- **ST: security target** = the document that identifies the security **properties** of the target of evaluation. Each target is evaluated against the SFRs established in its ST, no more and no less
- **EAL: evaluation assurance level =** numerical rating (1-7) assigned to the target to reflect the assurance requirements fulfilled during the evaluation; each package of assurance requirements covers the complete development of a product, with a given level of strictness
- **SOF : Strength of Function =** a qualification of a TOE Security Function expressing the minimal efforts assumed to defeat its security mechanisms.

Development process (classical)



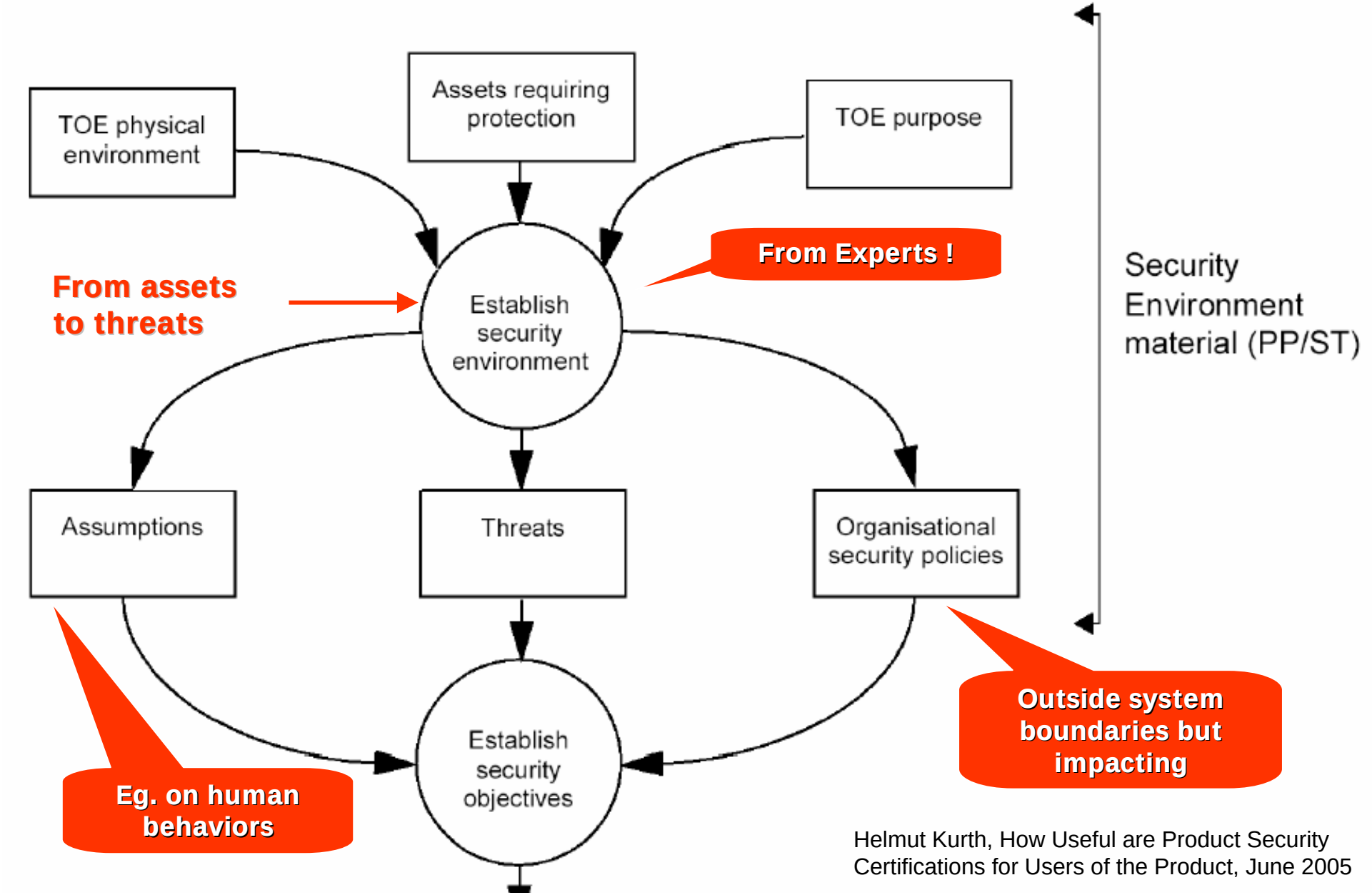
10

Lifecycle details

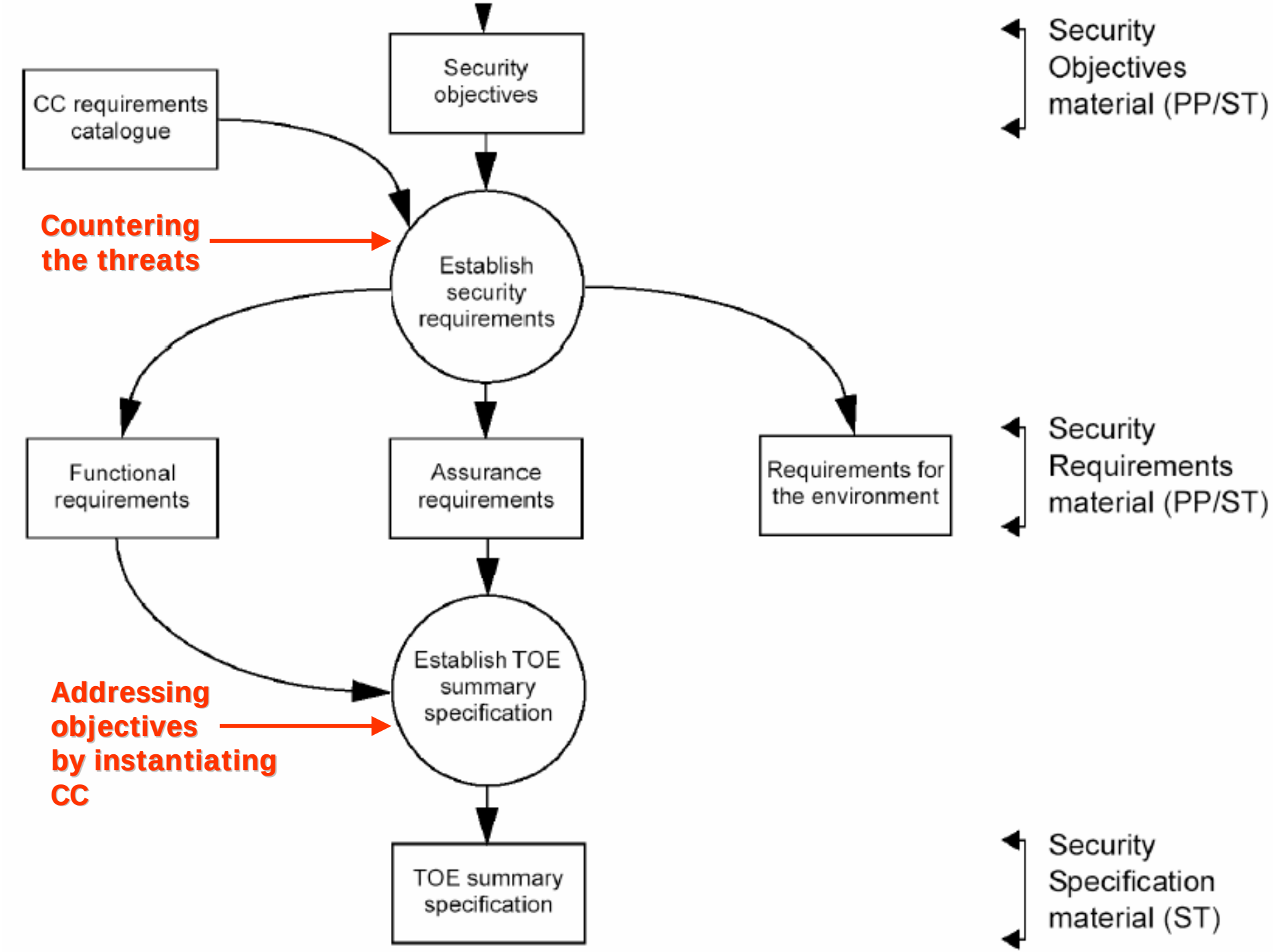
CC/CEM Artifacts and Activities	Generic System Lifecycle Phases	Generic Procurement Phases
none	Concept	Concept definition Feasibility studies, needs analysis Independent cost estimate
Protection Profile (PP) Security assurance activity: APE	Requirements analysis and specification	Request for proposal (tender) issued by customer
Security Target (ST) Security assurance activity: ASE	Design	Technical and cost proposals submitted by vendors Technical and cost proposals evaluated by customer
Target of Evaluation (TOE) developed by winning vendor Security assurance activities: ACM, ADV	Development	Contract award
Security assurance activities: ATE, AVA	Verification	Acceptance of delivery orders ECPs issued to correct deficiencies in requirements, design, or development
Security assurance activities: ADO, AGD	Validation, installation and checkout	Deployment
Security assurance activities: ALC, AVA, AMA	Operations and maintenance	Transition to maintenance contract
none	Decommissioning	Contract expiration

11

Common Criteria Process

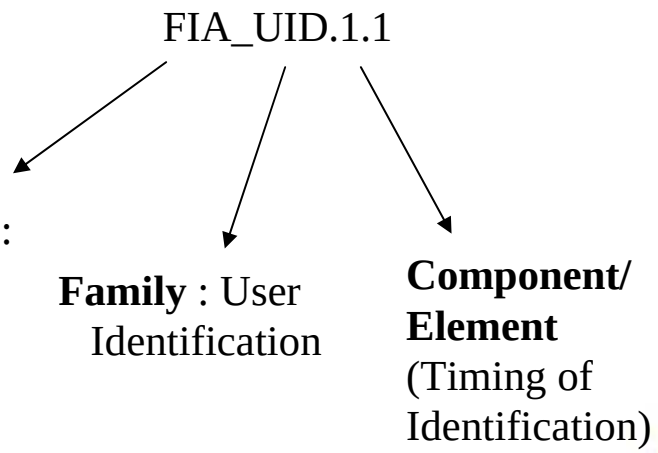


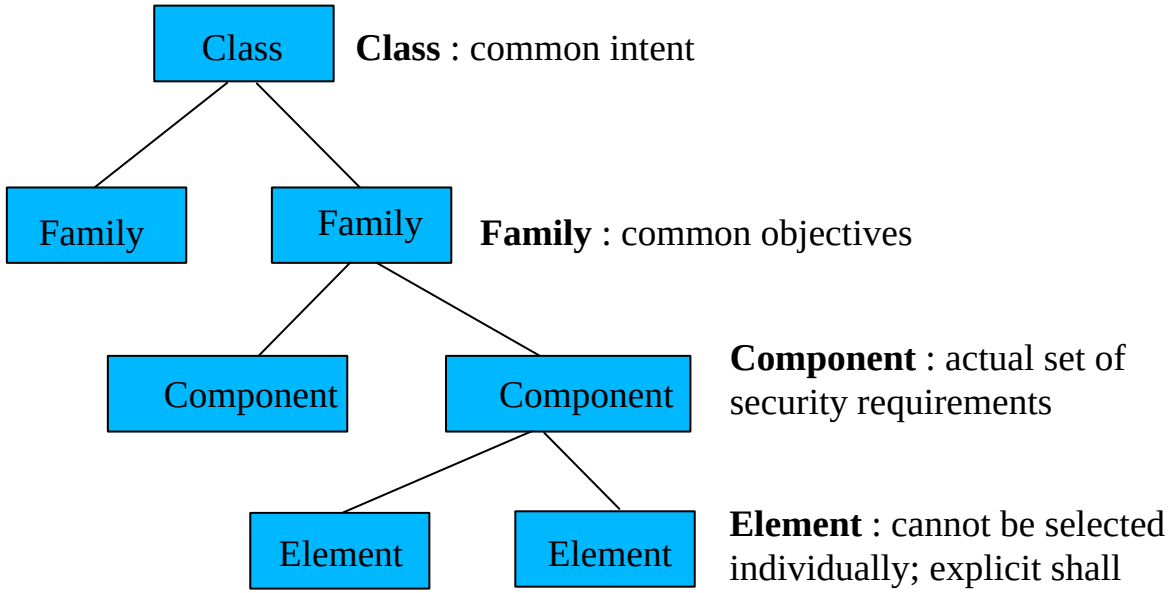
Helmut Kurth, How Useful are Product Security Certifications for Users of the Product, June 2005


Security objectives
CC requirements catalogue
Countering the threats
Establish security requirements
Functional requirements
Assurance requirements
Requirements for the environment
Addressing objectives by instantiating CC
Establish TOE summary specification
TOE summary specification
Security Objectives material (PP/ST)
Security Requirements material (PP/ST)
Security Specification material (ST)

Security Classes

- Tree-structured catalogue
- Notation convention





14

Security Classes

Short Name	Long Name	Purpose[20]
FAU	Security audit	monitor, capture, store, analyze, and report information related to security events
FCO	Communication	assure the identity of originators and recipients of transmitted information; nonrepudiation
FCS	Cryptographic support	manage and control operational use of cryptographic keys
FDP	User data protection	protect (1) user data, and the associated security attributes, within a TOE and (2) data that is imported, exported, and stored
FIA	Identification and authentication	ensure unambiguous identification of authorized users and the correct association of security attributes with users and subjects
FMT	Security management	manage security attributes, data, and functions and define security roles
FPR	Privacy	protect users against discovery and misuse of their identity
FPT	Protection of the TSF	maintain the integrity of the TSF management functions and data
FRU	Resource utilization	ensure availability of system resources through fault tolerance and the allocation of services by priority
FTA	TOE access	control user session establishment
FTP	Trusted path/channels	provide a trusted communication path between users and the TSF and between the TSF and other trusted IT products

15

CC Evaluation Example

Red Hat
Enterprise Linux 3
(running on specified
Dell and Hewlett-Packard hardware)

16

Target of Evaluation (TOE)

TOE Description

Introduction

Linux is a free computer operating system that was created in 1991 by Linus Torvalds, based on POSIX standards, and has grown through contributions from software developers all over the world.

Red Hat Enterprise Linux is a commercially supported distribution of the free Linux operating system that is easier to install and operate. Red Hat Enterprise Linux is designed for mission-critical enterprise computing, with support for the largest X86-compatible servers, used in departmental and datacentre server deployments.

The TOE assumes that responsibility for the safeguarding of the data protected by the TOEs security functions (TSF) can be delegated to the TOE users. All data are under the control of the TOE. The data are stored in objects, and the TSF can associate with each controlled object a description of the access rights to that object.

TOE Architecture

Red Hat Enterprise Linux (also referred to in this document as Linux) provides a multi-user, multi-tasking environment. The operating system may be viewed as a series of layers. At the lowest layer, the Linux kernel interacts with the hardware platform, providing a common set of services to application programs. These services include managing system memory, sharing access to the system processor(s), and opening and closing devices. In addition, the operating system provides other basic services, including:

- File systems organised within a hierarchy of directories;
- Device drivers providing interfaces to hardware devices
- User interfaces to run programs and access th
  graphical interfaces (GNOME and KDE) a
  Note that the graphical interfaces are

17

Evaluated Configuration

Evaluated Configuration

The TOE covers the following products, built around a common core:

- Red Hat Enterprise Linux AS 3 – supporting large commodity-architecture servers, for large departmental and datacentre server deployments;
- Red Hat Enterprise Linux ES 3 – suitable for medium scale departmental deployments;
- Red Hat Enterprise Linux WS 3 – the workstation product, suitable for software development or client applications.

The TOE is evaluated on the following hardware platforms:

HP D530	(Red Hat Enterprise Linux WS)
HP Proliant ML570	(Red Hat Enterprise Linux ES and AS)
Dell Precision 650	(Red Hat Enterprise Linux WS)
Dell PE 2650	(Red Hat Enterprise Linux ES)
Dell PE 6650 4 Processor	(Red Hat Enterprise Linux AS)

18

Evaluated Configuration

The following features are excluded from the scope of the TOE, and it is assumed that they are not used:

- Apache Web Server
- Kerberos
- Crypto IP Encapsulation
- Nmap
- LILO
- Network File System (NFS)
- Domain Naming System (DNS)
- Dynamic Host Configuration protocol (DHCP)
- Network Information System (NIS)
- Automatic Updating using Red Hat Up2date
- X-Windows Graphical Interface
- Support for AppleTalk
- Support for IPX
- Red Hat Cluster Manager

19

Security Environment

Security Environment

Threats

This ST has derived all security objectives from the statement of Organisational Security Policy found in the following section. Therefore, there is no statement of the explicit threats countered by the TOE.

Organisational Security Policies

An Organisational Security Policy is a set of rules or procedures imposed by an organisation upon its operations to protect its sensitive data. The organisational security policies described below apply to many DoD and non-DoD environments.

P.AUTHORISED_USERS
Only those users who have been authorised to access the information within the system may access the system.

P.NEED_TO_KNOW
The system must limit the access to, modification of, and destruction of the information in protected resources to those authorised users which have a “need to know” for that information.

P.ACCOUNTABILITY
The users of the system shall be held accountable for their actions within the system.

Security Objectives

Security Objectives

This section defines the security objectives of the TSF and its supporting environment. Security objectives, categorised as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organisational security policies identified. All of the identified threats and organisational policies are addressed under one of the categories below.

IT Security Objectives

The following are the TOE IT security objectives:

O.AUTHORIZATION
The TSF must ensure that only authorised users gain access to the TOE and its resources.

O.DISCRETIONARY_ACCESS
The TSF must control accessed to resources based on identity of users. The TSF must allow authorised users to specify which resources may be accessed by which users.

O.AUDITING
The TSF must record specified security relevant actions of users of the TOE. The TSF must present this information to authorised administrators.

O.RESIDUAL_INFORMATION
The TSF must ensure that any information contained in a protected resource is not released when the resource is recycled.

O.MANAGE
The TSF must provide all the functions and facilities necessary to support the authorised administrators that are responsible for the management of TOE security.

O.ENFORCEMENT
The TSF must be designed and implemented in a manner that ensures that the organisational policies are enforced in the target environment.

21

Security Objectives

Non-IT Security Objectives

The TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met. The following are the TOE non-IT security objectives:

O.INSTALL
Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives.

O.PHYSICAL
Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security objectives.

O.CREDEN
Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives.

22

Threats and risk analysis

#	Threat	Severity of Consequences (note 1)	Likelihood of Occurrence (note 2)	Risk Mitigation Priority
T1	An undetected compromise of assets may occur as a result of:			
T1a	an authorized user performing actions the individual is not authorized to perform	marginal to critical	occasional	high
T1b	an attacker (insider or outsider) masquerading as an authorized user and attempting to perform actions that individual is authorized to perform	marginal to critical	occasional	high
T1c	an attacker (insider or outsider) gaining unauthorized access to information or resources by impersonating an authorized user.	marginal to critical	occasional	high
T1d	an authorized or unauthorized user accidentally or intentionally blocking staff access to TOE devices	marginal to critical	occasional	high
T1e	an unauthorized user gaining control of the TOE	marginal to critical	remote	medium to high
T1f	an unauthorized user rendering the TOE inoperable	marginal to critical	remote	medium to high
T1g	an unauthorized person attempting to bypass security	Marginal to critical	frequent	medium to high
T1h	an unauthorized person repeatedly trying to guess identification and authentication data	marginal to critical	frequent	medium to high
T1i	an unauthorized person using valid identification and authentication data fraudulently	marginal to critical	probable	medium to high
T1j	an unauthorized person or external IT entity viewing, modifying, and/or deleting security relevant information transmitted to a remote authorized user or administrator	marginal to critical	occasional	medium to high
T2	An authorized user may access information or resources without having permission from the person who owns or is responsible for the information or resource	marginal to critical	remote	medium
T3	An attacker may eavesdrop on or otherwise capture data being transmitted across a network:			

23

Operations on requirements

- generic requirements which can be “instantiated” using 4 mechanisms:
  - Selection:
    - fill a placeholder with one/several proposed proposition
  - Assignment:
    - specify the policy to meet the security requirement
  - Iteration
    - multiple instantiation is possible
  - Refinement:
    - make requirement more concrete
    - rationale must be provided

24

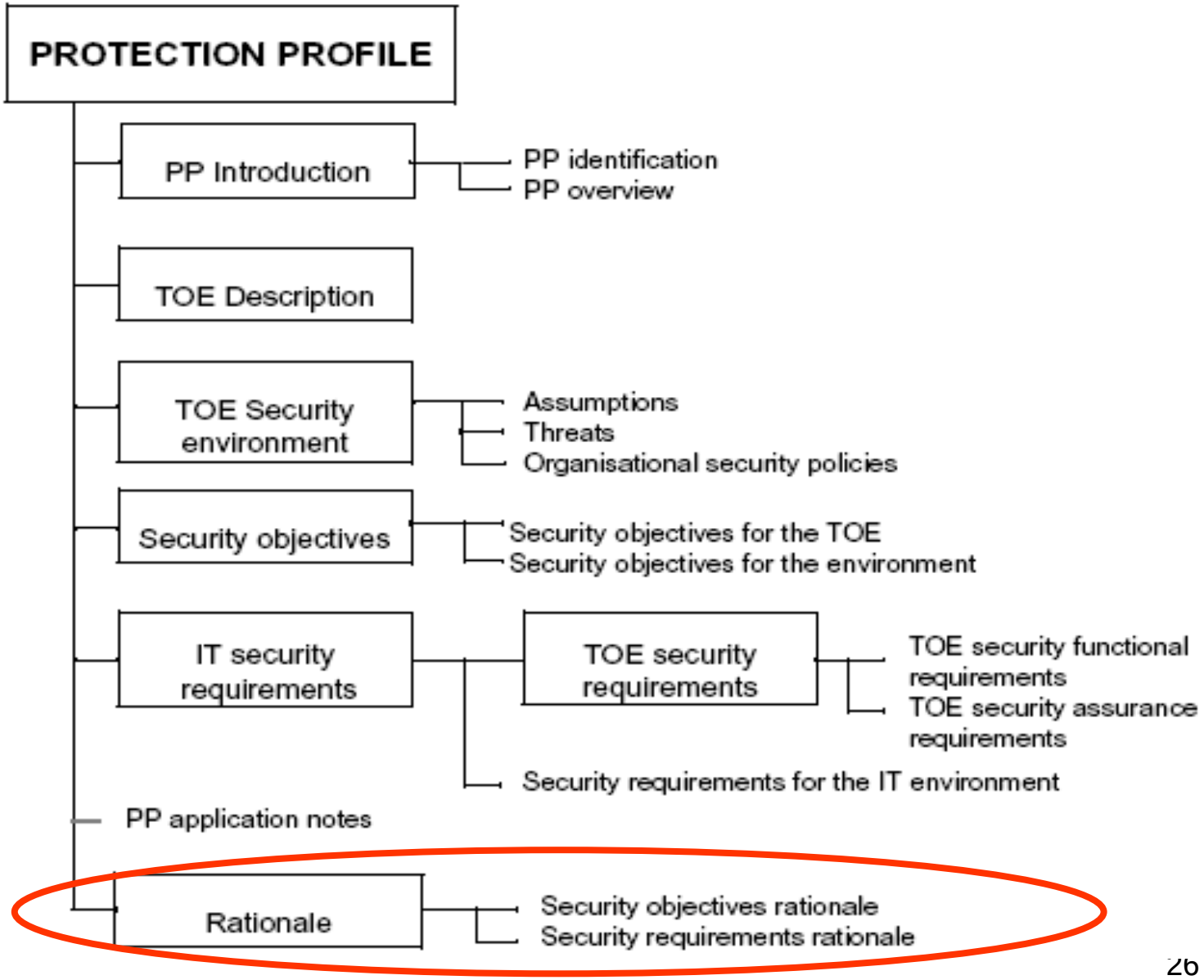
From Security Objectives to Security Requirements

- **Cryptography:**
  - **FCS_COP.1.1 -** The TSF shall perform **[assignment: *list of cryptographic operations*]** in accordance with a specified cryptographic algorithm **[assignment: *cryptographic algorithm*]** and cryptographic key sizes **[assignment: *cryptographic key sizes*]** that meet the following: **[assignment: *list of standards*].**
  - Concrete algorithms and key size ?
    - Not now: deferred to design phase
    - So CC left uninstantiated at the PP level

- **Integrity Testing:**
  - **FPT_TST.1.1 -** The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of the TSF.

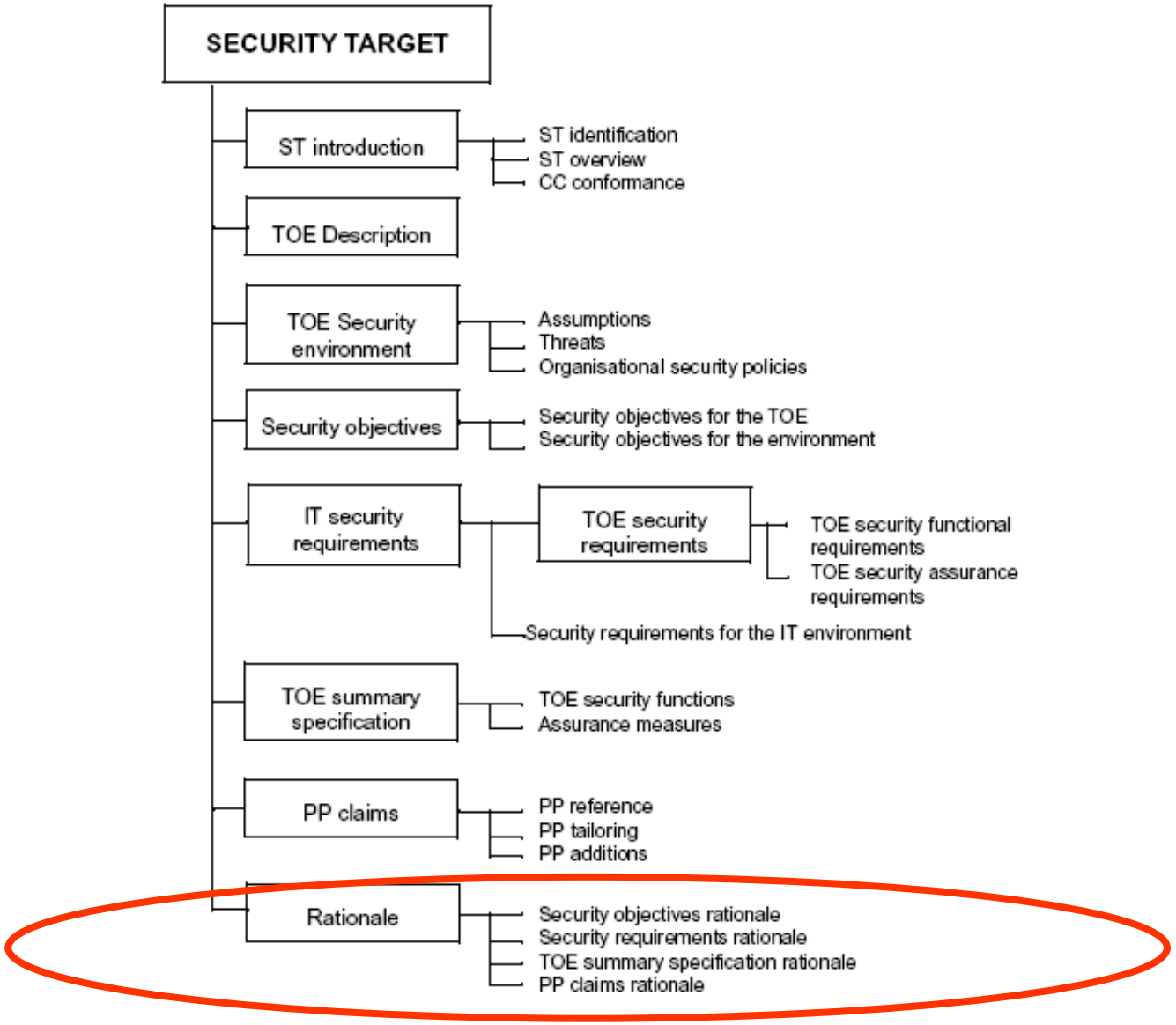
25

Document : PP Structure



26

Document: ST Structure



27

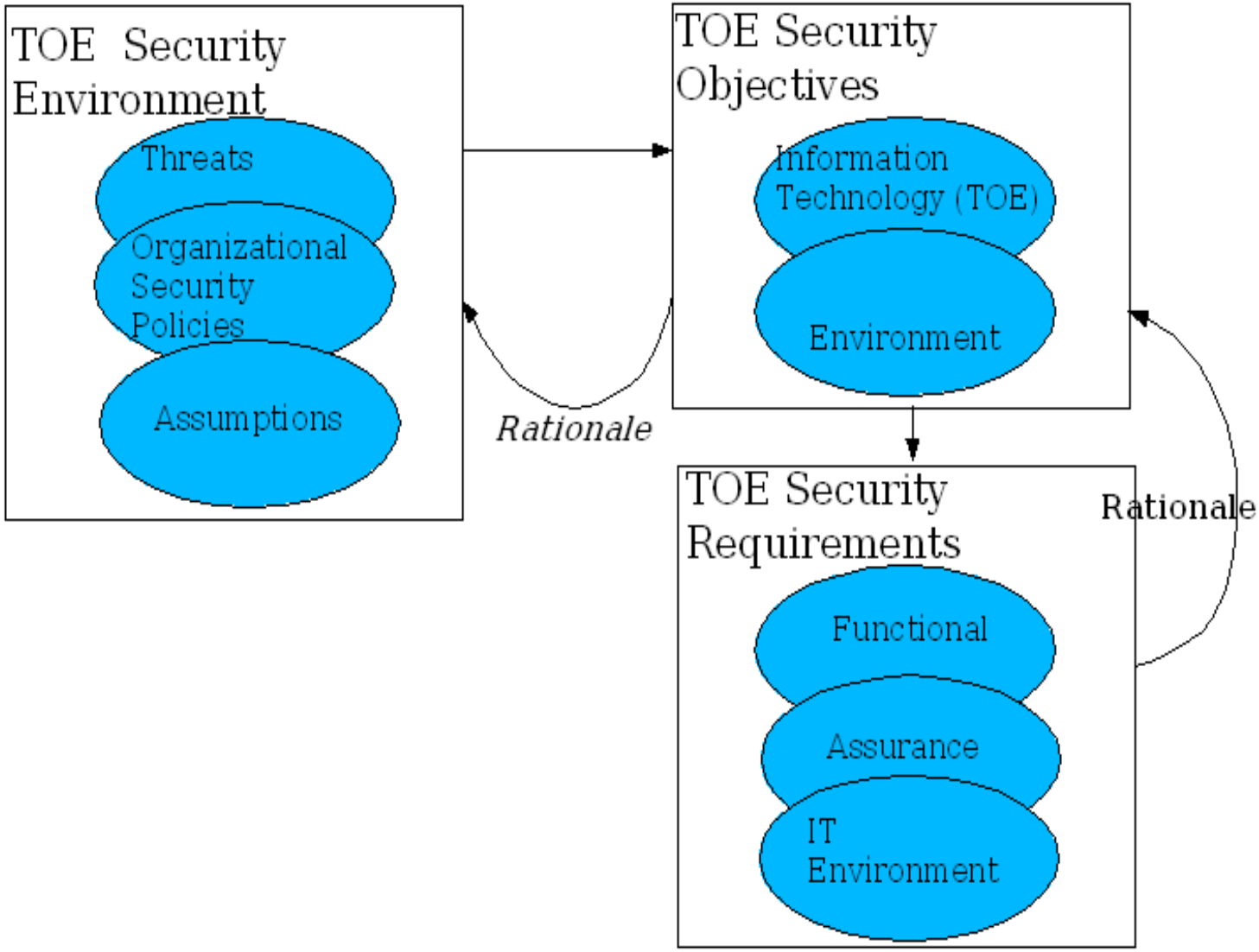
Rationale: essential !

- Do not just claim: justify !
- Analysis of a smart card protection profile

Part	Size (pages)
TOE description	5
Security Environment	10
Security Objectices	10
Security Requirementes	30
Rationales	40
Annexes	100

28

Main Rationales



29

A look at the PP, ST evaluation elements

- Developer Action elements
  - ASE_OBJ.1.2D - The developer shall provide the security objectives **rationale**.
  - ASE_PPC.1.2D - The developer shall provide the PP claims rationale for each provided PP claim.
  - ASE_REQ.1.2D - The developer shall provide the security requirements **rationale**.
  - ASE_SRE.1.2D - The developer shall provide the security requirements **rationale**.
  - ...
- Presentation of **evidence**:
  - ASE_OBJ.1.4C - The security objectives rationale shall demonstrate that the stated security objectives are suitable to **counter the identified threats** to security.
  - ASE_OBJ.1.5C - The security objectives rationale shall demonstrate that the stated security objectives are suitable to cover all of the identified organisational security policies and assumptions.
  - ASE_PPC.1.1C - Each PP claim shall identify the PP for which compliance is being claimed, including qualifications needed for that claim.
  - ASE_PPC.1.2C - Each PP claim shall identify the IT security requirements statements that satisfy the permitted operations of the PP or otherwise further qualify the PP requirements.
  - ...

30

A look at the Rationales (smart card PP)

Completeness, coverage: tabular format

Threat	Is Addressed By Objective(s)
T.P_Probe	O.D_Read, O.Phys_Prot
T.P_Alter	O.Phys_Prot
T.Flt_Ins	O.Flt_Ins
T.Forcd_Rst	O.Init
T.Inv_Inp	O.Log_Prot
T.Reuse	O.Reus
T.Brute-Force	O.Brut

Component	Depends On:	Which is:
FAU_ARP.1	FAU_SAA.1	included
"	(indirect) FAU_GEN.1	see Section 6.4.1.2
"	(indirect) FPT_STM.1	see Section 6.4.1.3
FAU_LST.1	no dependencies	not applicable
FAU_SAA.1	FAU_GEN.1	see Section 6.4.1.2
"	(indirect) FPT_STM.1	see Section 6.4.1.3
FAU_SEL.1	FAU_GEN.1	see Section 6.4.1.2
"	FMT_MTD.1	included
"	(indirect) FIA_UID.1	included
"	(indirect) FMT_SMR.1	see Section 6.4.1.4
"	(indirect) FPT_STM.1	see Section 6.4.1.3

32

Some Textual Rationales

- **Sufficiency:**
  - **T.P_Probe (Physical Probing of the IC)** deals with mechanical attacks on the structure of the TOEitself. It is countered directly by **O.Phys_Prot (Physical Protection)** which ensures that the TOE is constructed using such elements as (...)

- **Mutually supportive (=> not conflicting)**
  - The requirements represented in this protection profile were developed from a variety of sources including the direct experience of smart card security evaluations by major card associations. As such, the body of requirements has been indirectly shown to be **consistent and mutually supportive** through its successful application to major commercial systems. A further demonstration is presented below, showing that the security requirements work mutually so that each SFR is protected against bypassing, tampering and deactivation attacks by other SFRs.

33

More Textual Rationales

- **Refinement**: justify that:

  « Meeting the refined requirement will also meet the original requirement, so this refinement is not an extension of the stated CC requirement. »

- **Extensions**: eg. EAL4+
  - **AVA_VLA.3 Vulnerability Assessment - Vulnerability Analysis - Moderately resistant.** EAL4 requires vulnerability assessment through imposition of AVA_VLA.2. This dictates a review of identified vulnerabilities only.

34

Evaluation Assurance Levels

1. Functionally tested
2. Structurally tested
3. Methodically tested and checked
4. Methodically designed, tested, and reviewed

---

5. Semi-formally designed and tested
6. Semi-formally verified design and tested
7. Formally verified design and tested

35

Assurance (process level)

EAL level = maturity of assurance process

-Idea comparable to CMM

-Informal -> semiformal -> formal lgge

-1-2-3-4 = Basic

-5 = Medium

-6-7= High

-Maximal “commercial” EAL today: EAL 4+

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Class ACM: Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Class ADO: Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Class ADV: 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
Class AGD: Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Class ALC: Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Class ATE: 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
Class AVA: 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

Assurance Requirements

8.2 Assurance Measures

This section identifies the Configuration Management, Delivery/Operation, Development, Guidance Documents, Test, and Vulnerability Assessment measures applied to satisfy CC assurance requirements.

TABLE 2: Assurance measures

Assurance Measure	Security Assurance Requirement Met
Documentation for the Red Hat configuration management system shows how Red Hat identifies and labels configuration items.	ACM_CAP.2
Red Hat Enterprise Linux delivery procedures describe how the TOE is delivered via secure download from https://rhs.redhat.com, and by physical delivery on CD.	ADO_DEL.1
Instructions for installation are provided in the Red Hat Enterprise Linux 3 Installation Guide. This is supplemented by further guidance on achieving the evaluated configuration.	ADO_IGS.1
A functional specification is provided that describes all system calls, trusted commands and related configuration files. Much of the information is given by reference to man pages.	ADV_FSP.1
A high-level design is provided that describes the subsystems that provide the security functions of the product.	ADV_HLD.1

Assurance Requirements

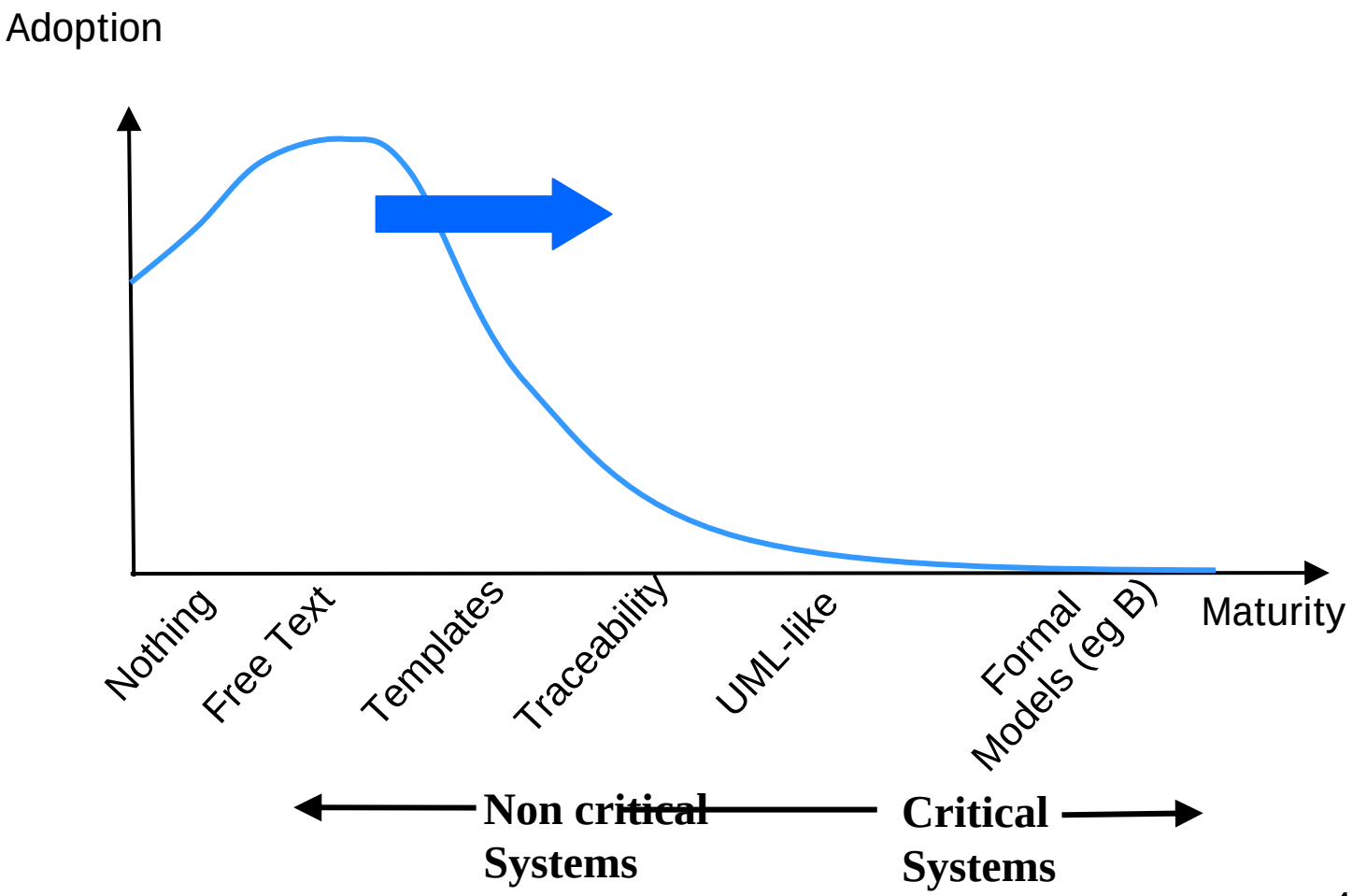
Correspondence information is provided that maps the security functions in the ST to the functional specification and the high-level design.	ADV_RCR.1
A set of reference manuals is provided with the product. These manuals are supported by comprehensive man files	AGD_ADM.1, AGD_USR.1
Test plans and procedures are provided for the TSF, documented to a level where tests can be repeated. Expected and actual test results are supplied. Hardware is provided to the evaluators to allow tests to be repeated and additional tests to be run.	ATE_COV.1, ATE_FUN.1, ATE_IND.2
A strength of function analysis is provided for the TOE authentication function.	AVA_SOF.1
A vulnerability analysis is provided that documents a search for vulnerabilities in the TOE. This search is based on available documentation and public domain sources.	AVA_VLA.1

The above table includes all of the assurance requirements for the target level of assurance EAL2. Documented evidence covering each of the detailed security assurance requirements in EAL2 will be provided in the supporting documentation listed above against each EAL2 component.

38

Model-based Support

A large spectrum of techniques



40

A model-based approach

- Modelling:
  - Capturing assets and essential security properties
  - Identifying and addressing threats
  - Capturing all rationales behind this
- Addressing the right EAL level
  - Textual, semi-formal, formal descriptions
  - Seamless refinement
- Tool support
  - Structuring models
  - Formalising models
  - Generating documents

41

A Requirements Point of View

Security using Common Criteria	Issues	Goal-Oriented Req. Eng.
Security		Goal Model
Security Threats	Finding/organizing threats ?	Anti-goals/Obstacles
Security Objectives	Addressing threats ?	“Mitigating” Goals
Security Requirements	Refining/Operationalizing ?	Requirements
		+ guidance
Documents (PP, ST)	Document management ?	
Rationale – Justification	Rationale generation ?	Rationale capture
Tool = word processor		**Model-based report generation**

42

Toy Example: a simple smart-card e-purse

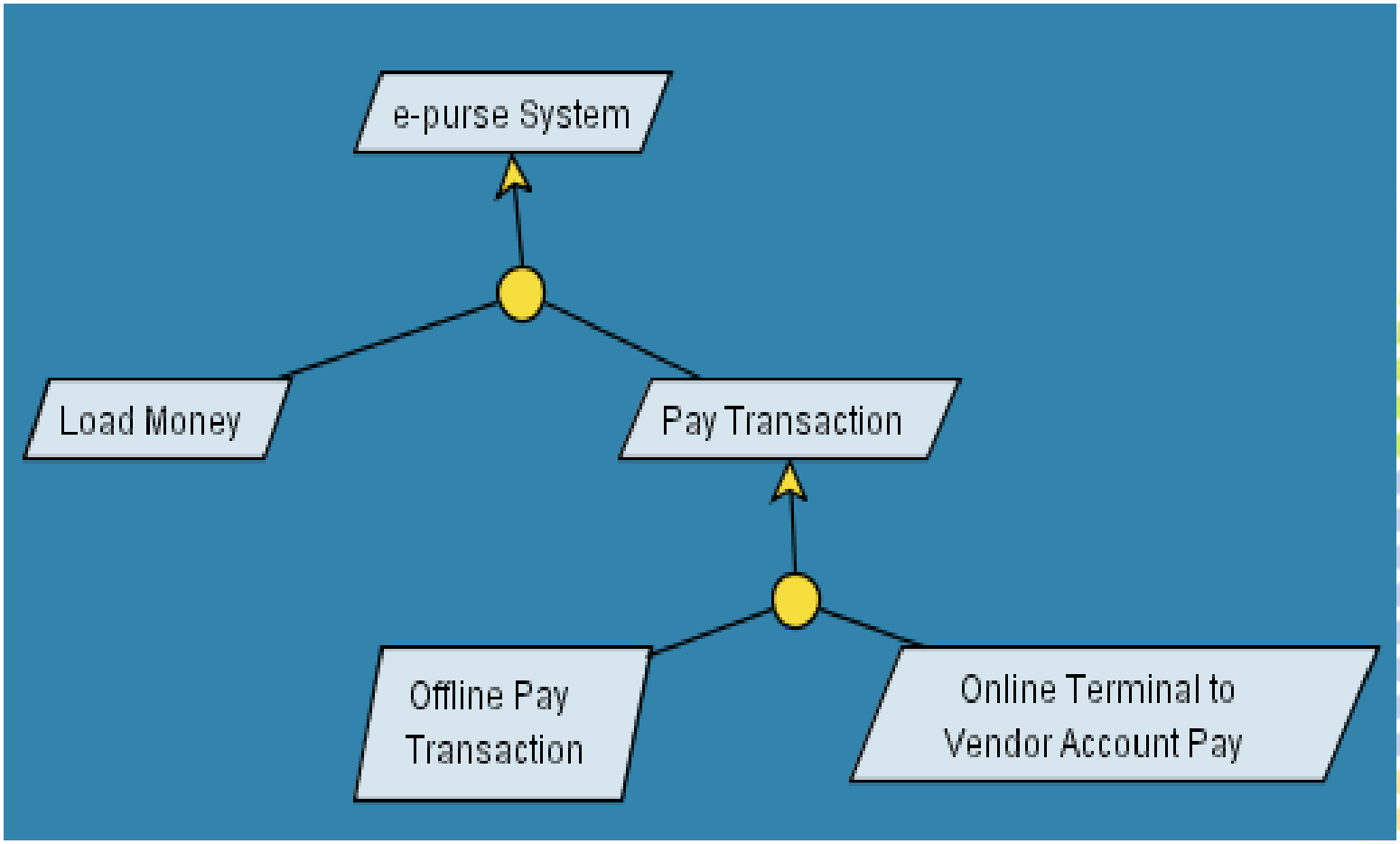
- High Level Functional requirements:
  1. The system shall allow the user to pay for goods using a card previously credited of an amount of money.
  2. On a pay transaction, the amount is deduced from the payer card and transferred to the payee, provided the credit is sufficient. Parties are informed of the outcome (success or failure) of the transaction

- Security requirements:
  1. No value may be created: e-money should only be generated in exchange for real one
  2. No value is lost: all value is accounted in the system
  3. Money transfer should only occur between payer and payee and for the agreed amount.

- For sake of simplicity:
  1. the only transactions considered are to load the card and to unload for paiement
  2. the system does not support: multiple currencies, transfert of electronic money between cards, to accounts or for real money

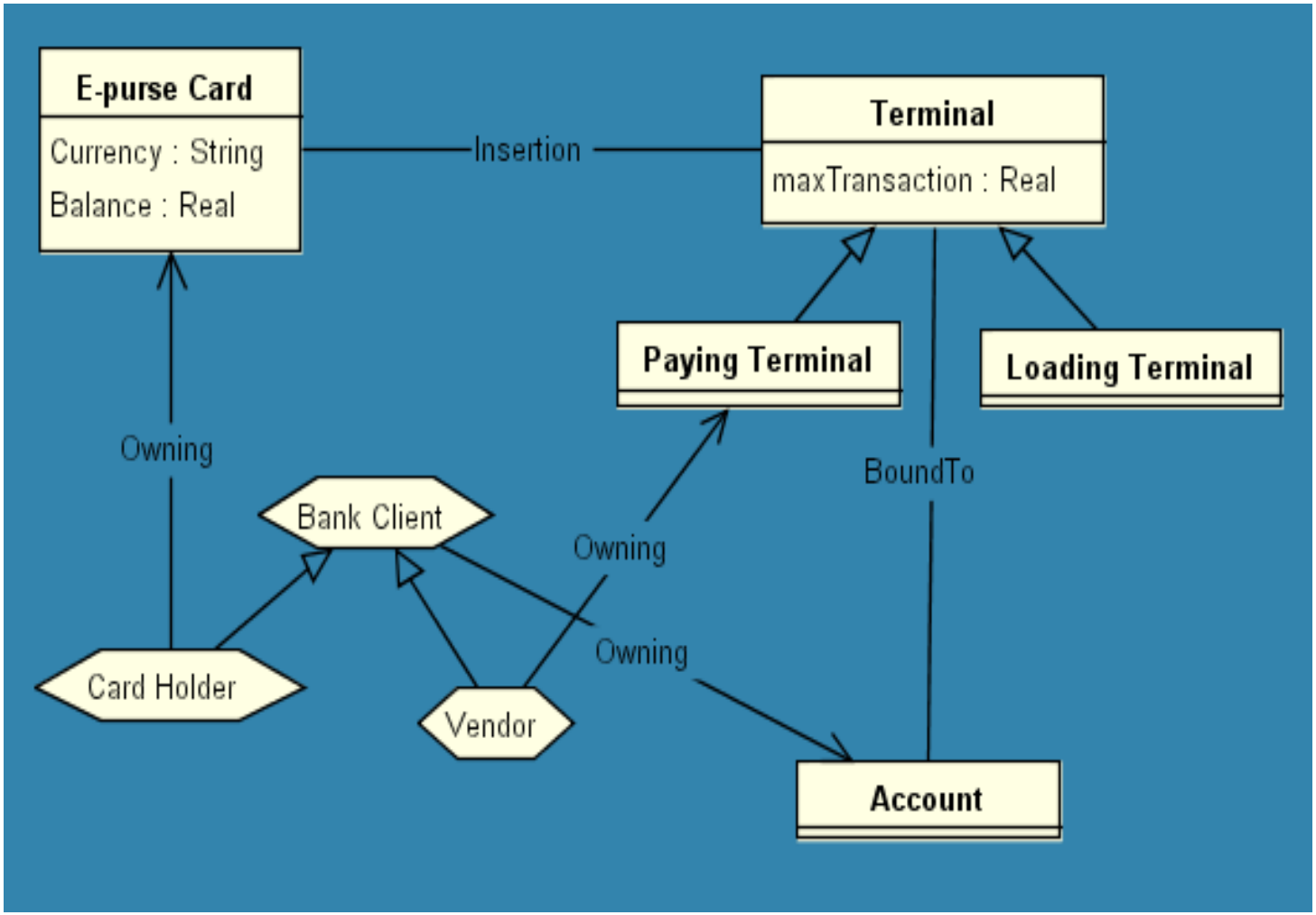
43

Functional Goals



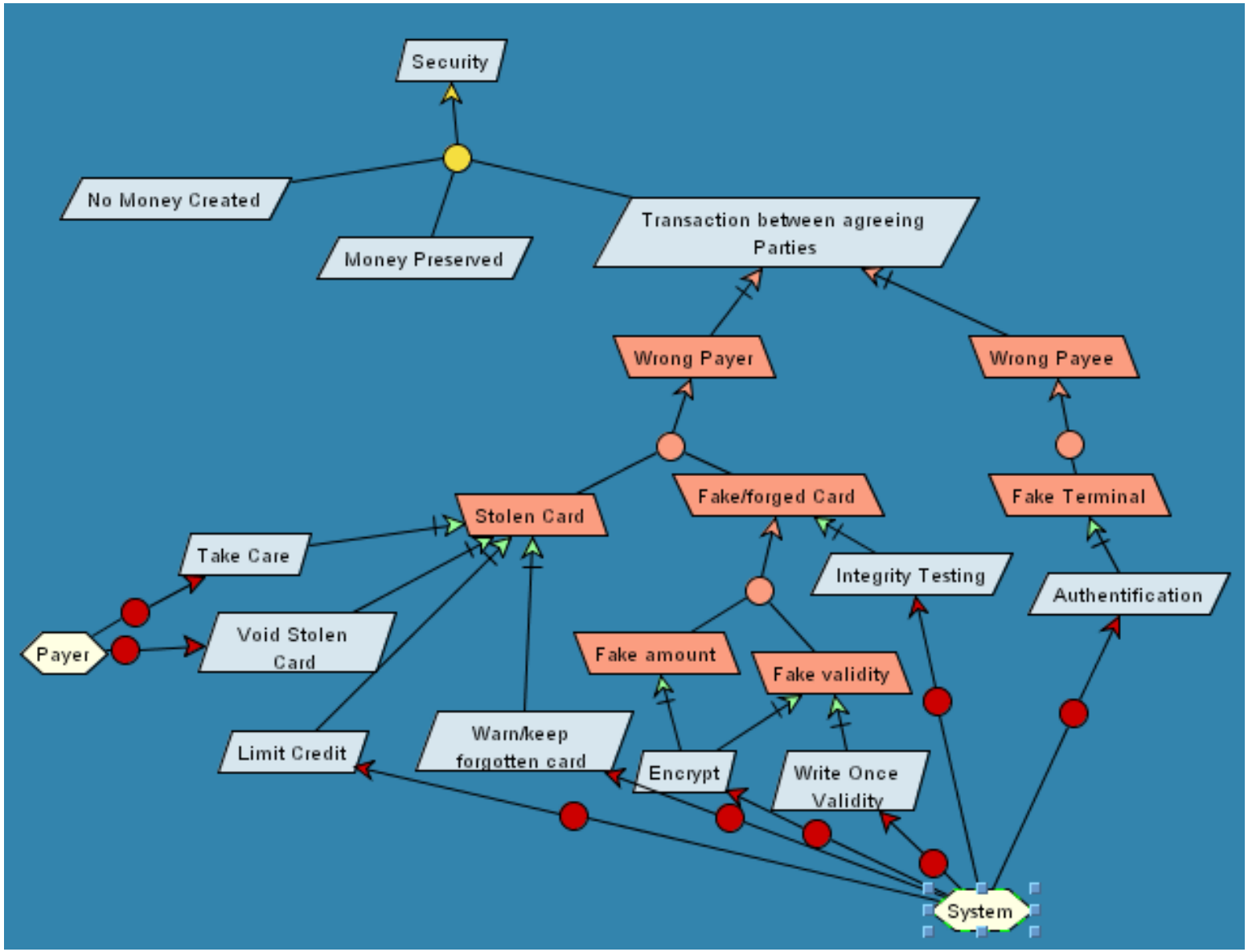
44

Modelling Environment and Assets



45

Threats: from Goals and Anti-goals



46

Document Generation

- All the information is in the model:
  - Assets, treaths, objectives, requirements
  - Also rationales !
    - Completeness tables from traceability links
    - Textual justification attached to the model
- Model-based approach:
  - Manage and evolve the model, not the document
  - Generate the document
- Short tool demo

47

General Conclusions

- Common Criteria provides strong guidelines for IT security
- Support reuse:
  - common criteria catalogue
  - protection profile library
  - instantiation primitives
- Model engineering helps support/improve the process
  - More systematic identification of threats
  - Better document management
  - Improved quality assurance
- Formal level required to achieve high evaluation assurance levels: see next presentation
- Extensible and also still evolving
- Links with other norms:
  - ISO 17799: good practices
  - EBIOS: CC compatible but includes other norms such as ISO17799

48

Benefits for the auditor

- Standard framework:
  - clear evaluation criteria
  - based on a serious approach of IT security
- Can be applied:
  - for actual certification purposes
  - in a wider scope
- Auditor present in the CC process
- Library of “domain specific” protection profiles (check list)
- Evaluation assurance levels : maturity scale
  - current situation, target, what to improve first

49

References

- Common Criteria Familiarization (slides), NIST
- Common Criteria for IT Security Evaluation, Part 1 (2 & 3), http://csrc.nist.gov/c
- D.S. Herrman, Using the Common Criteria for IT Security Evaluation, CRC Press, 2003.
- W Rankl, W. Effing, Smart Card Handbook – 3rd Edition, Wiley 2003
- Smart Card Security User Group – Smart Card Protection Profile (SCSUG-SCPP), version 3.0, sept 2001
- A. Van Lamsweerd & al, From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirement Engineering, in Proc RHAS'03, 2003
- A. Van Lamsweerd & al, Elaborating Security Requirements by Construction of Intentional Anti-Models, in Proc ICSE'04, 2004
- M. Vetterling, G. Wimmel, Secure Systems Development based on the Common Criteria – The PalME Project, FSE 10, 2002.