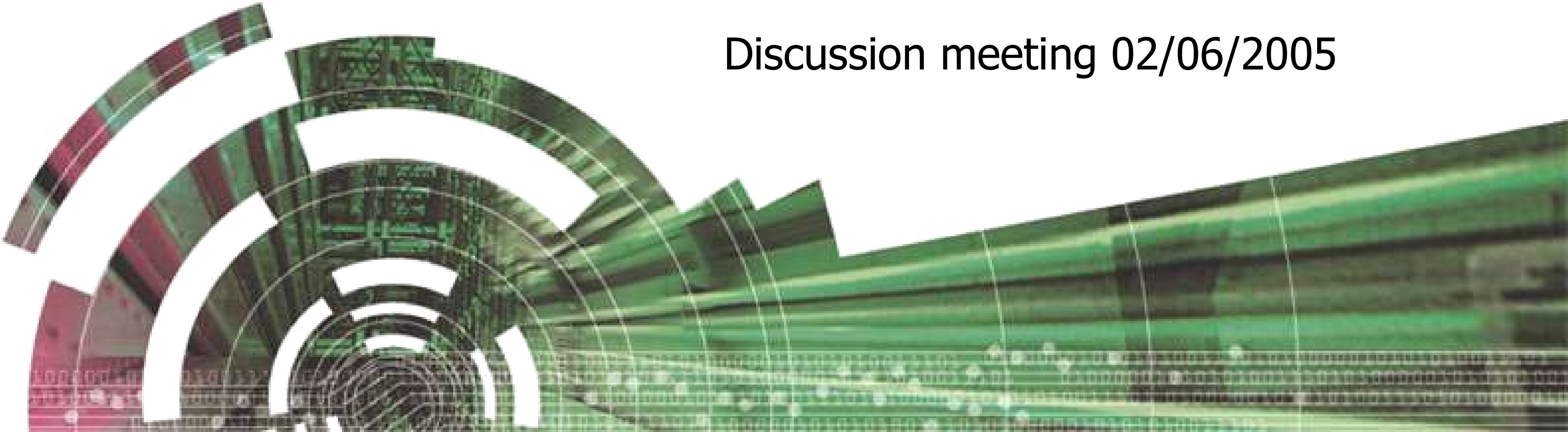
Common Criteria : an effective deployment

CETIC
J.F. Molderez

Discussion meeting 02/06/2005



Presentation Objectives

- IT Security & Common Criteria
- Common Criteria application examples
- Towards an effective Common Criteria utilization

Presentation Roadmap

- Introduction
  - IT Security
  - Common Criteria overview
- CC in practise :
  - Market
  - Application examples
- Process Support
- Conclusion :
  - Advantages and drawbacks

IT Security

- A system may be said to be secure if the properties of confidentiality, integrity, availability, authenticity of the various system entities are maintained.

- “Security is an issue
  - not only for security products (firewalls, VPNs, ...) but for all IT products
  - not because all IT products can provide security
  - but all IT products can undermine security “ [10]

Research on formal methods related to security

- Research in security has focused on formal methods for proving systems correct : utmost care required because of the disastrous consequences of security-related errors [8]

- In today's practise, the formalization threshold is still significant !

- **Program security** : no program learns information that it is not authorized to know

- **Security policy** : no unauthorized access to information,   restricting the behaviour of the system to achieve security

- **Database security** : every piece of information in a database is learnt only by users authorized to know it

- **Security protocols** : specifications of communication patterns intended to let agents share secrets over a public network

Common Criteria (CC) : Definition and Goals

- The CC combines the best aspects of existing European (ITSEC), US (TCSEC) and Canadian (CTCPEC) criteria for the security Evaluation of Information Technology (IT) systems and products. [1]

=> align separate criteria

- The Common Criteria Certification is an internationally recognized evaluation of security features as well as the development and testing processes associated with information technology products [6]

=> achieve mutual recognition, address fragmented market

- CC = internationally agreed and standardized methodology
  + catalog of IT security requirements

CC : origin and evolution

- 1985 : Trusted Computer System Evaluation Criteria , “the orange book “(US)
- 1991 : Information Technology Security Evaluation Criteria, (EU members)
- 1993 : Canadian Trusted Computer Product, CTCPEC version 3.0, published as a combination of the TCSEC and ITSEC approaches
- 1993 : Draft Federal Criteria For Information Technology Security Version 1.0 (US)
- 1998 : Mutual Recognition Agreement signed by the US, Canada, France, Germany, and the UK for Common Criteria-based evaluations
- 1999 : Common Criteria 2.1
- 2004: Common Criteria 2.2
- 2005: Common Criteria 3.0 draft

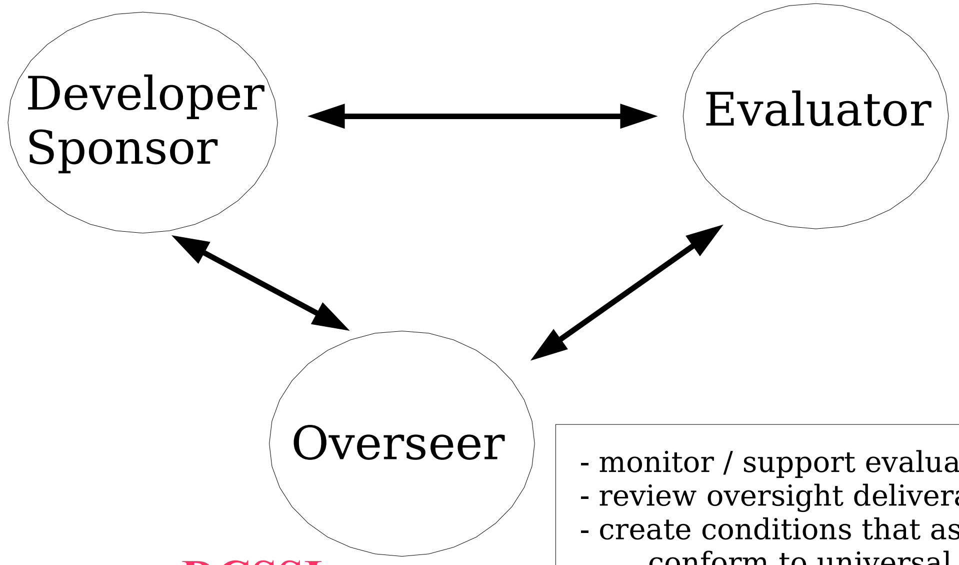
Common Criteria Reference Documents

- CC Standard v2.2
  - Part 1 : Introduction & General Model (61 p)
  - Part 2 : Security Functional Requirements (362 p)
  - Part 3 : Assurance Requirements (216 p)
- Common Evaluation Methodology v2.2
  - Part 2 : Evaluation Methodology (351 p)
- Functional Requirements = product level
  what a product is able to do
- Assurance Requirements = process level
  measures to inspire confidence that the objectives have been met

CC Stakeholders

- 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



Developer
Sponsor

Evaluator

Overseer

AQL, Oppida,
CEA, Serma

DCSSI

- 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

Stakeholders

- **Consumers** : to support the procurement of products / systems with IT security features
- **Developers & Integrators** : as a basis for the development of …
- **Certifiers & Auditors** : to support the certification process
- **Overseer** : to check certification labs

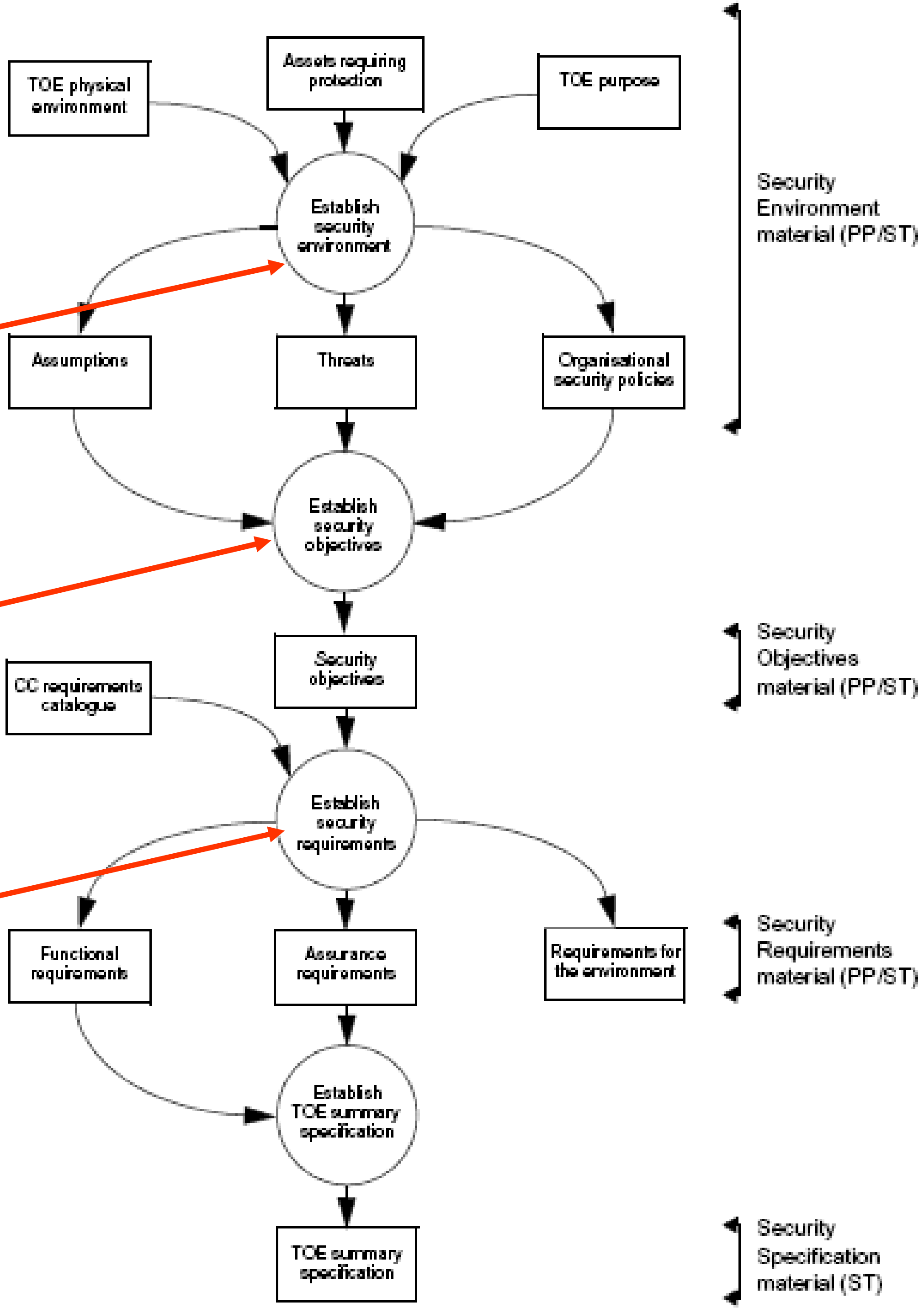
the Common Criteria Process

Your connection to
ICT research

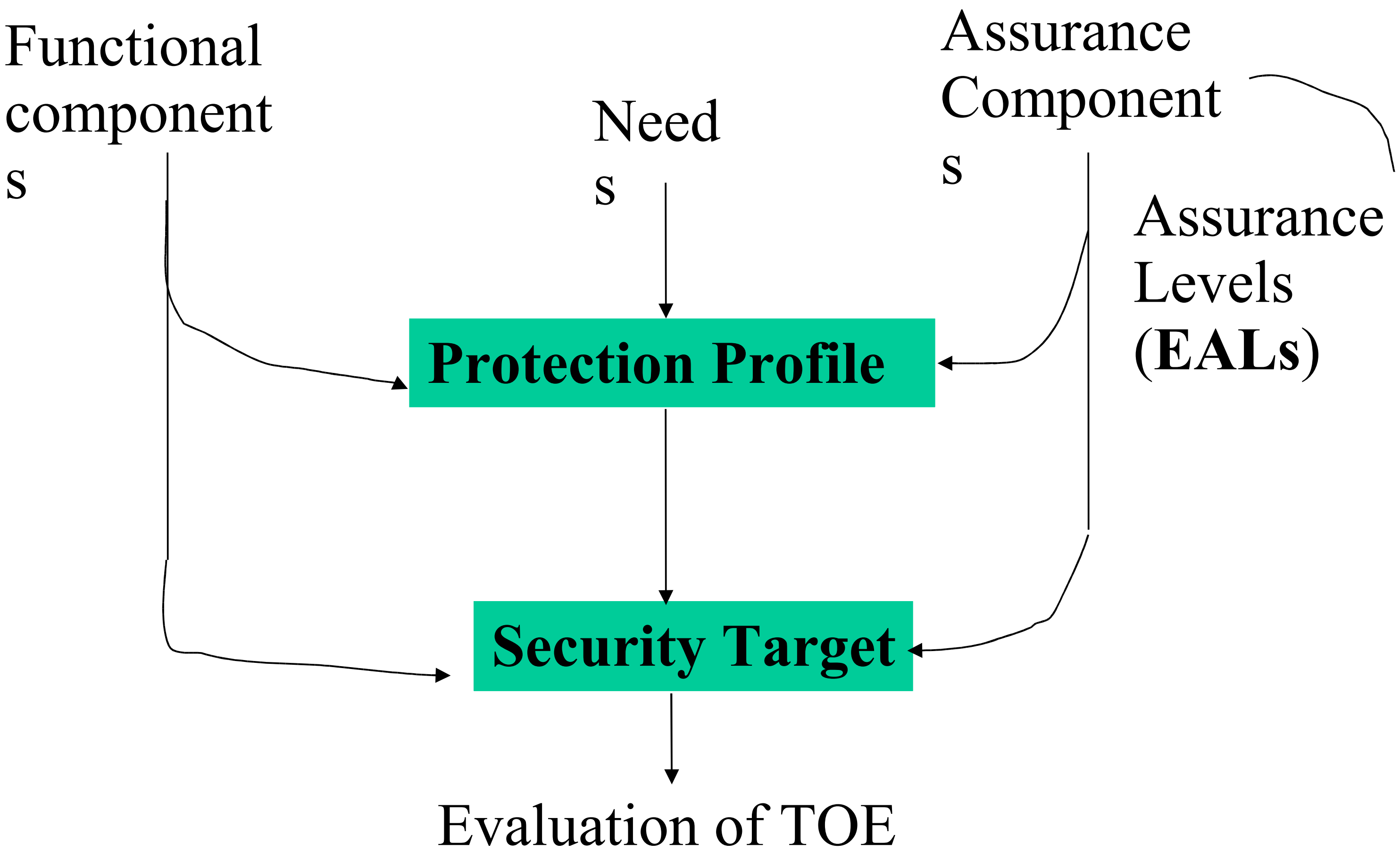
From assets to threats

Countering the threats

Addressing objectives by instantiating CC


TOE physical environment
Assets requiring protection
TOE purpose
Establish security environment
Assumptions
Threats
Organisational security policies
Security Environment material (PP/ST)
Establish security objectives
Security objectives
Security Objectives material (PP/ST)
CC requirements catalogue
Establish security requirements
Functional requirements
Assurance requirements
Requirements for the environment
Security Requirements material (PP/ST)
Establish TOE summary specification
TOE summary specification
Security Specification material (ST)

CC process



Functional components

Needs

Assurance Components

Assurance Levels **(EALs)**

Protection Profile

Security Target

Evaluation of TOE

CC process

- Protection Profile (PP) :
  - Requirements level – Implementation independent
  - **What do I need in a security solution ?**
- Security Target (ST) :
  - Specification level – Implementation dependent
  - **What do you provide in a security solution ?**
- Evaluation expected result : the Target of Evaluation (TOE) satisfies the ST

Structure of CC documents

Protection Profile	**Security Target**
Identification	Identification
Overview	Overview
TOE Description	TOE Description
Security Environment	Security Environment
Assumptions, Threats, Policies	Assumptions, Threats, Policies
Security Objectives	Security Objectives
Security Requirements	Security Requirements
Functional, Assurance (EAL)	Functional, Assurance (EAL)
Rationale	Rationale
	TOE Summary Specification
	CC Conformance Claim
	PP Claims

CC Evaluation Assurance Levels

- Evaluation Assurance Levels : sets of assurance components
  - EAL1 to EAL7 : uniformly increasing scale
  - balances the assurance level with cost and feasibility to acquire it
  - EAL<4 : informal & semi-formal model
  - EAL>=5 : formal model required

- Note :
  - Certification at EAL4 level mandatory in Germany and Hungary or systems that use private signature keys [5]
  - The level of certification is not a measure of the product's “security strength”
  - Rather, it is a measure of how well the product protects itself. [10]

CC in practise

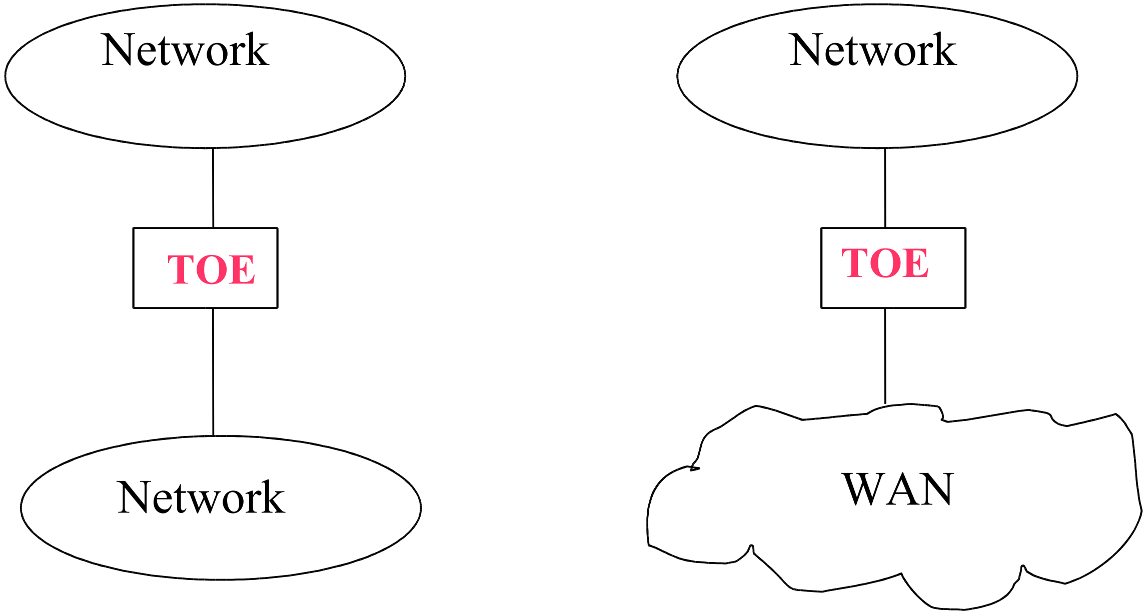
CC market (DCSSI France)

Application examples

Common Criteria Market

- From the DCSSI site (http://www.ssi.gouv.fr/en/confidence/certificats.html **) :**
- **Integrated circuits** : Microcontrollers
  - ST Micro, Samsung Electronics, Infineon Technologies, AMTEL smartcards, ...
  - 26 certificates 2000 - 2004 EAL4+ (most of them)
- **Smart Cards** : Operating Systems
  - ST Micro , Axalto, Schlumberger Système, Infineon Technologies, AMTEL, Oberthur Card, Philips, Gemplus, Mondex, Crédit mutuel, IBM, ...
  - 44 certificates 1996 – 2004 EAL1+, ITSEC E3, EAL4+
- **Network Products** : Firewalls
  - Bull, EADS Telecom, MATRAnet, Thomson CSF, ...
  - 7 certificates 1997 – 2004 max : EAL2+, ITSEC E4/medium

Firewall with strict requirements PP



- Filtering of communications (packets) based upon security policy rules
- Intrinsic security functions : audit, identification/authentication of users
- Interconnection of 2 networks without initial security degradation

MicroController : TOE

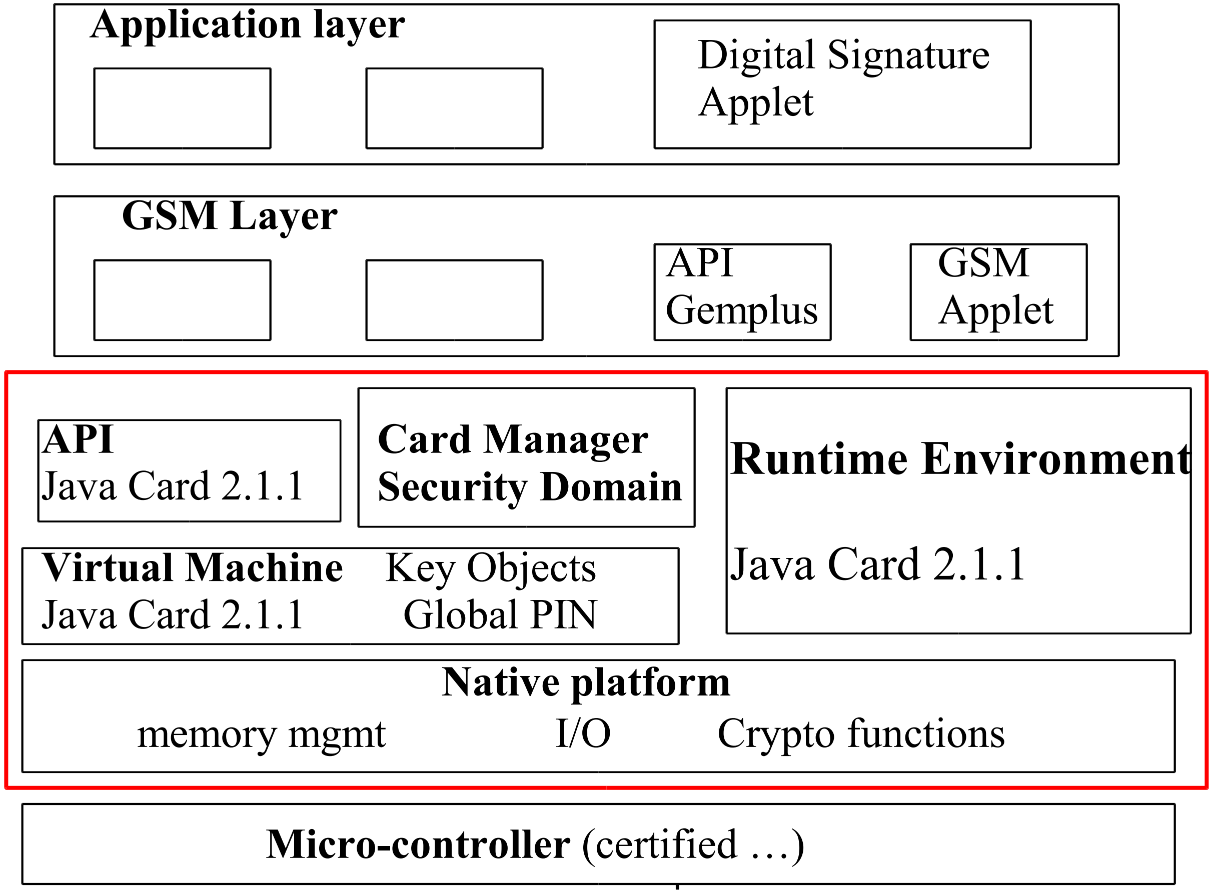
- P8WE5032 Secure 8-bit Smart Card Controller
- TOE: "the chip P8…that provides a hardware computing platform to run smart card applications executed by a smart card OS. The smart card OS and the application stored in the User-Mode ROM and in the EEPROM are not a part of the TOE …..
- Issue: composition of security functionalities:
  - only partly provided by the TOE
  - causes dependencies between the TOE security functions and the functions at OS or smart card application levels

MicroController: EAL and CC claims

- “The chosen level of assurance is EAL3
- This Security target claims the following conformances: Part 2 extended, conformant Part 3, no PP conformance claim ‟

Operating System : a JavaCard platform

- Java Card Platform Embedded Software V3 (Core) GemXplore'Xpresso V3



Application layer

Digital Signature Applet

GSM Layer

API Gemplus

GSM Applet

API Java Card 2.1.1

Card Manager Security Domain

Runtime Environment

Java Card 2.1.1

Virtual Machine Java Card 2.1.1

Key Objects Global PIN

Native platform

memory mgmt I/O Crypto functions

Micro-controller (certified …)

TOE
(OS for GSM applications written in Java)

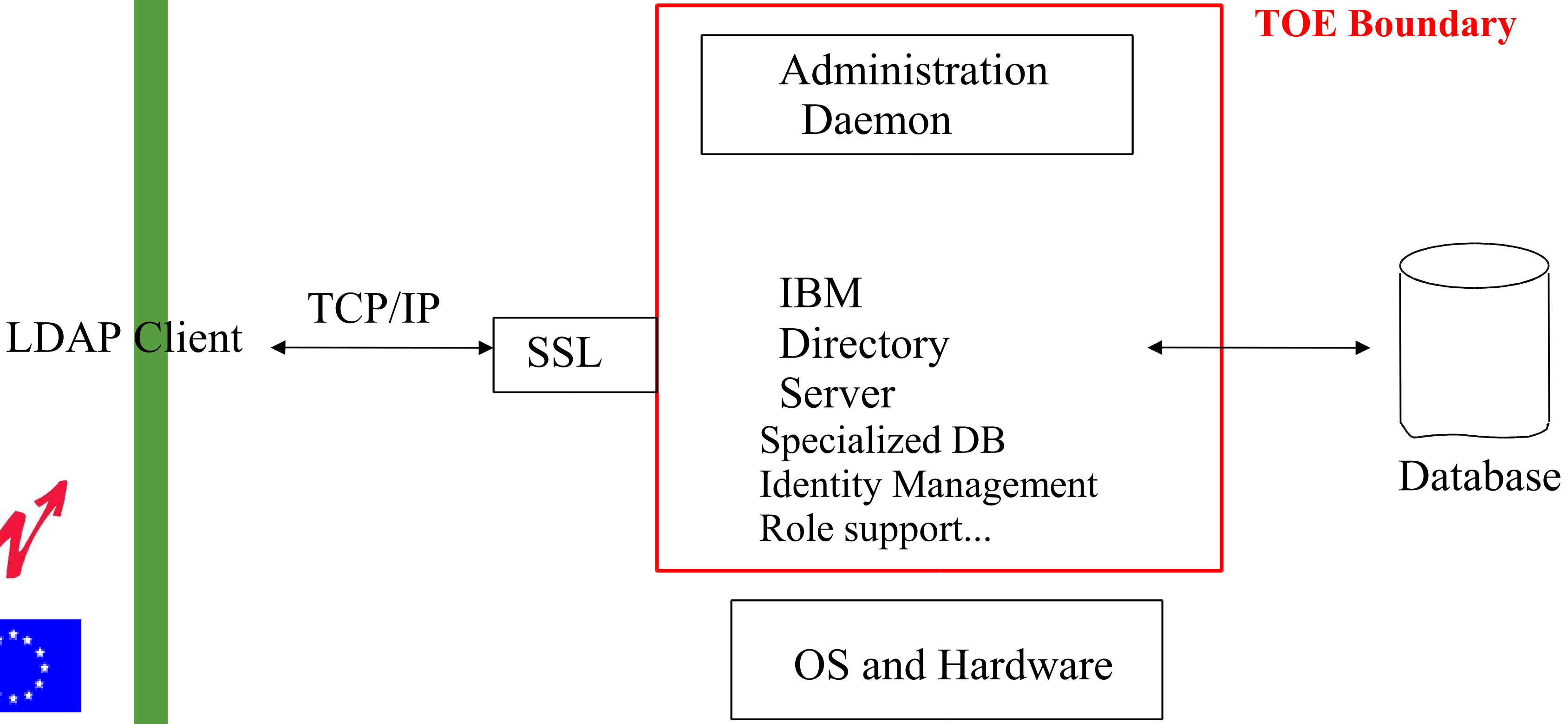
Operating System : a JavaCard platform

- Java Card Platform Embedded Software V3 (Core) GemXplore'Xpresso V3

- CC conformance claim
  - " This ST is in accordance with the Common Criteria Version 2.1 : Part 2 extended and Part 3 conformant
  - The minimum strength level for the TOE security functions is SOF-high.
  - The assurance level is EAL4.

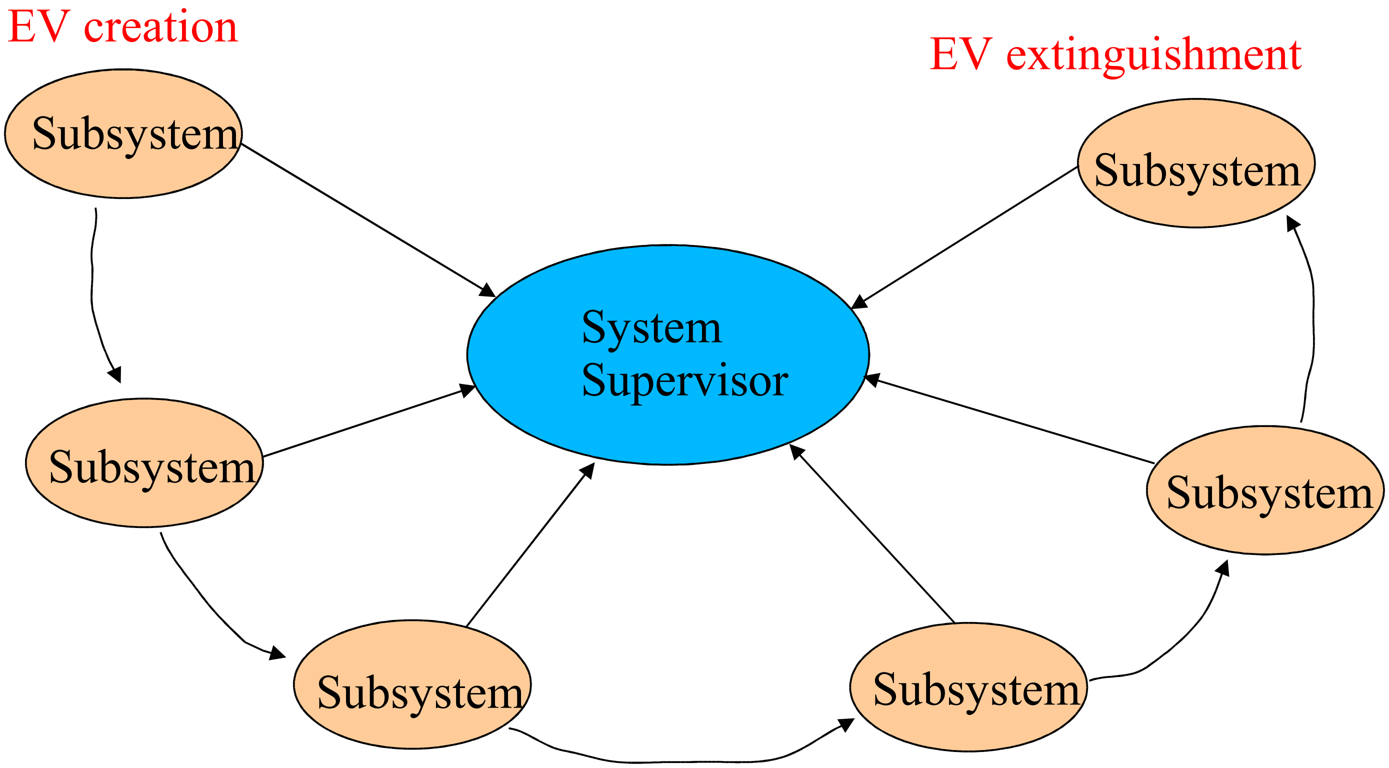
Software Component: Directory Server ST

- IBM Directory Server 5.1 FixPak510-01
- CC Conformance Claim
  - " This ST is Part 2 conformant and Part 3 conformant to the CC ... , and with the security assurance requirements for EAL2 ..."



Electronic Money System Security Objectives (ECB)

- Abstract model based on CC methodology
- Limited to threats and security objectives

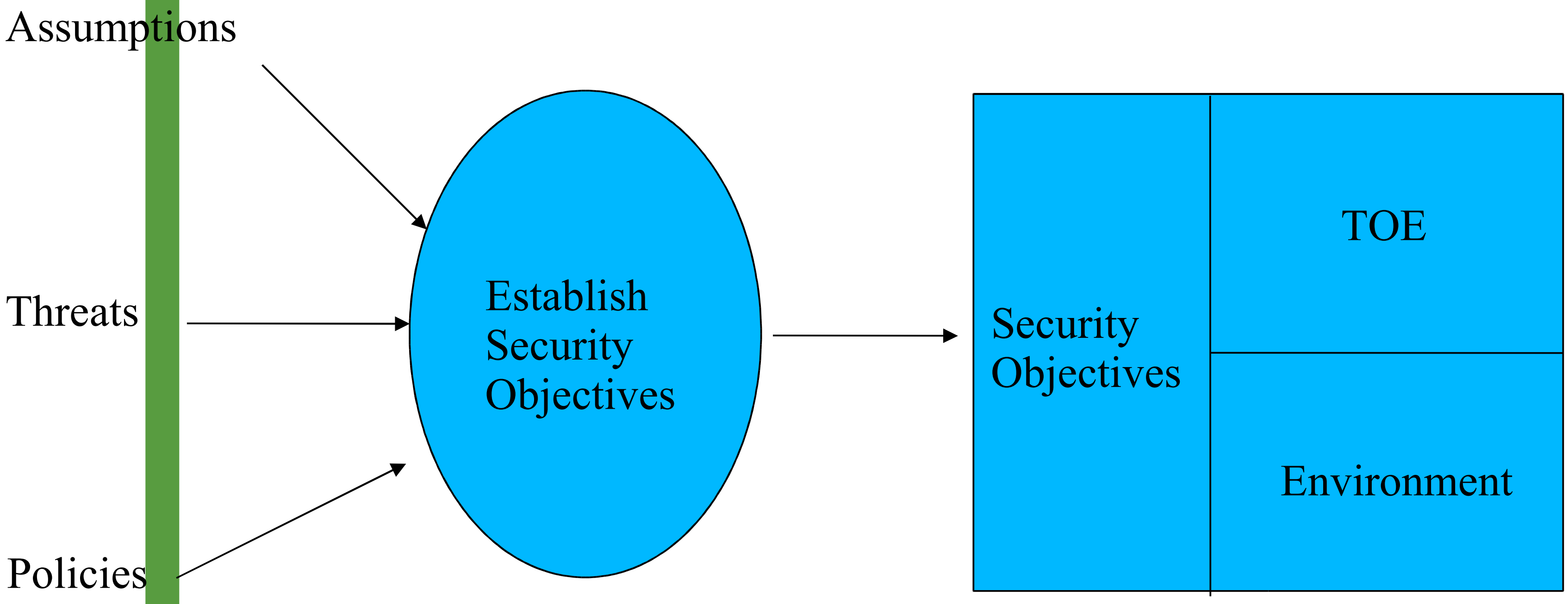


[9]

Process Support

Traceability links
Requirements & Models
Functionalities of an editor

Back to the Process



Assumptions

Threats

Policies

Establish Security Objectives

Security Objectives

TOE

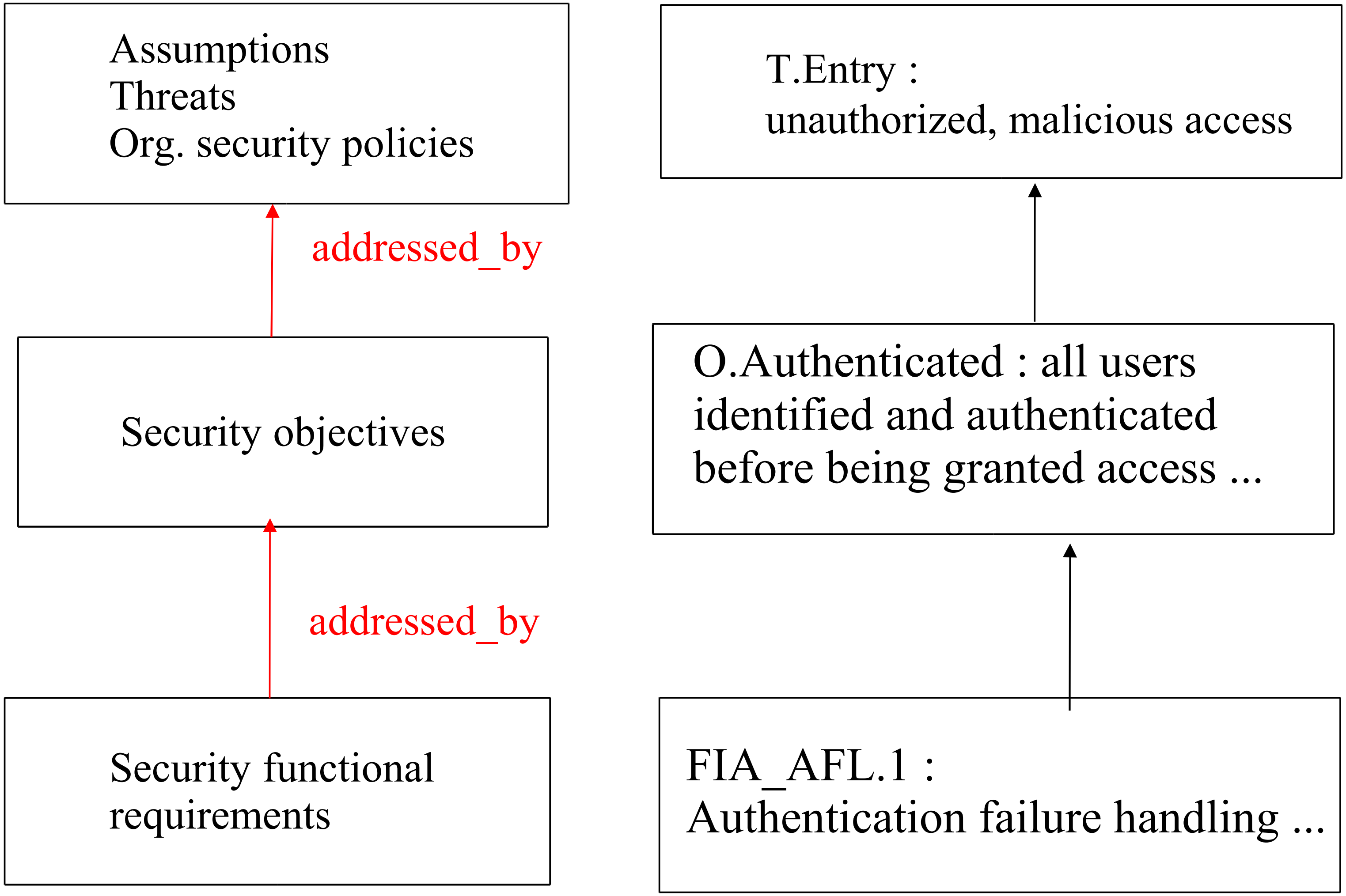
Environment

Back to the Process

- Asset :
  - “the attributes of a transaction, especially the EV exchanged between two subsystems and stored in a subsystem”
- Assumption :
  - “All actors ... have sufficient means, training and information to perform their functions.[A.Competence].”
- Threat :
  - “the modification of transaction attributes, Accounting Data, data related to EV creation and extinguishment, or secrets. [T.Usurpation_Extin].”
- Organizational Security Policy :
  - “The communication architecture of the TOE is based on standardized protocols and security procedures. [OSP.Protocol]”
- Security objective :
  - “ Every identified actor within the system has a clear set of access rights. [OE.SYS.ACC.PRIVILEGES]

[9]

The traceability links



Assumptions
Threats
Org. security policies

addressed_by

Security objectives

addressed_by

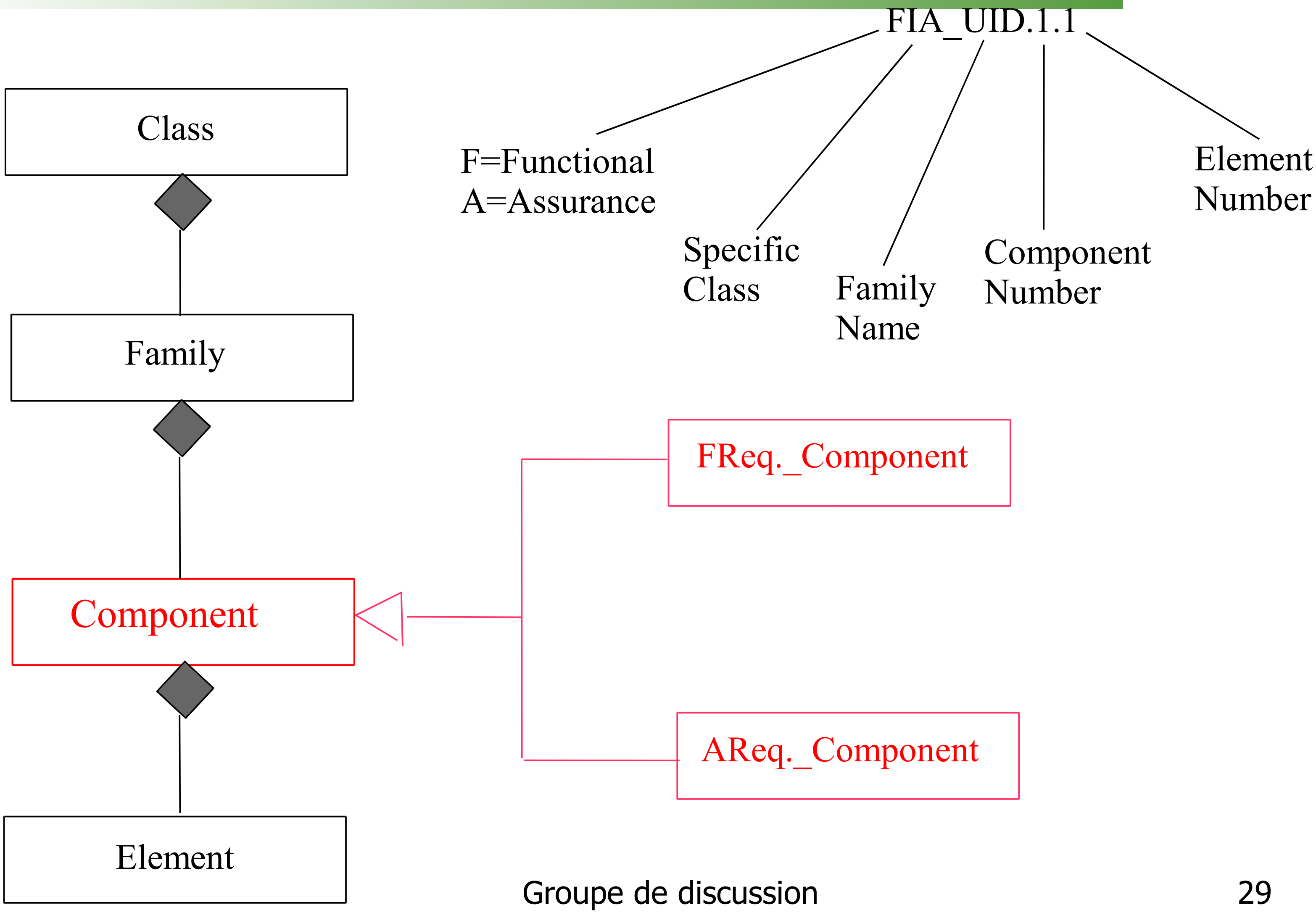
Security functional requirements

T.Entry :
unauthorized, malicious access

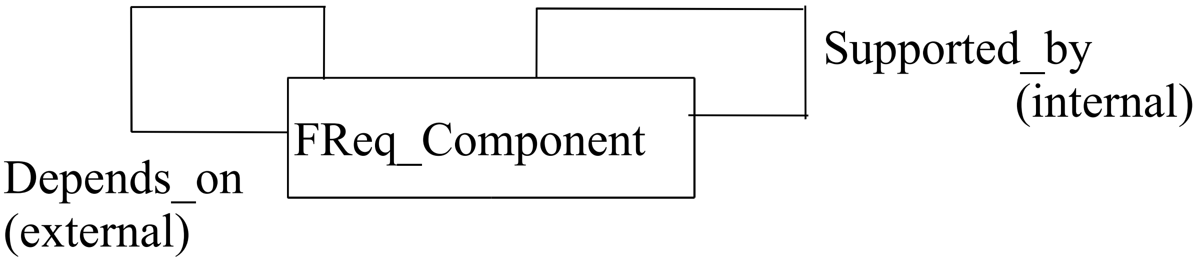
O.Authenticated : all users identified and authenticated before being granted access ...

FIA_AFL.1 :
Authentication failure handling ...

Requirements in CC

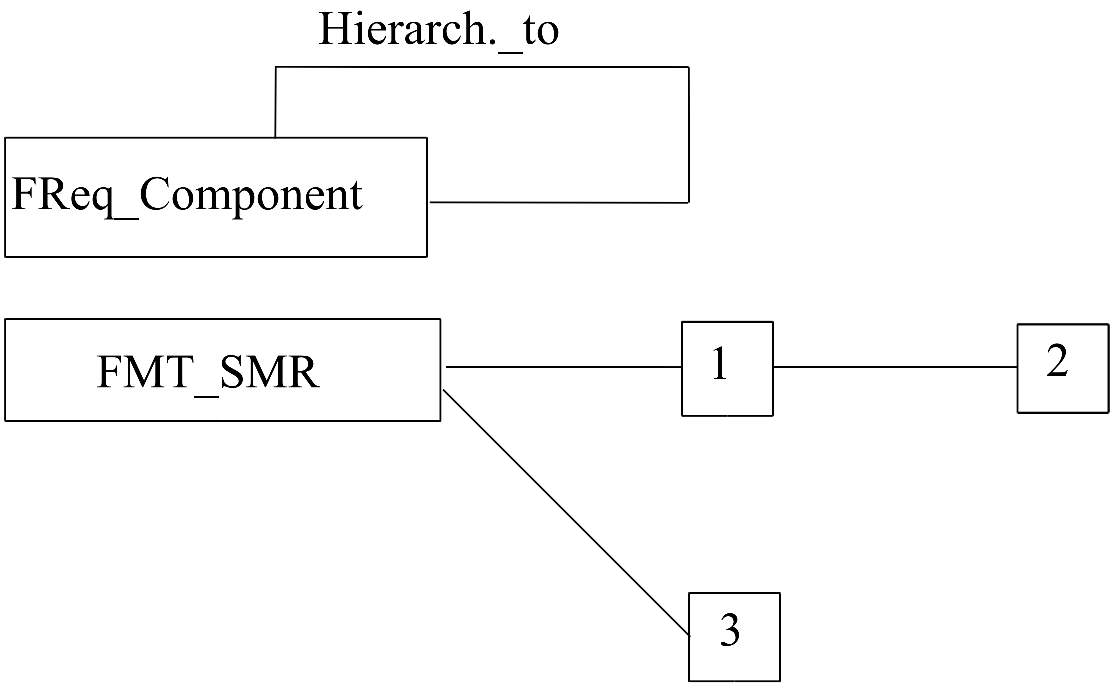


Requirements in CC



- Depends_On =
  - Assignment: fill-in the blank operation the PP writer defers completing assignments but ...
  - Selection: multiple choice the PP writer defers completing assignments but ...
  - Refinement: specify additional detail
  - Iteration: repetitive use of same component to address different aspects of the requirement being stated
- Supported_by = - No self sufficiency of a component .

Requirements in CC

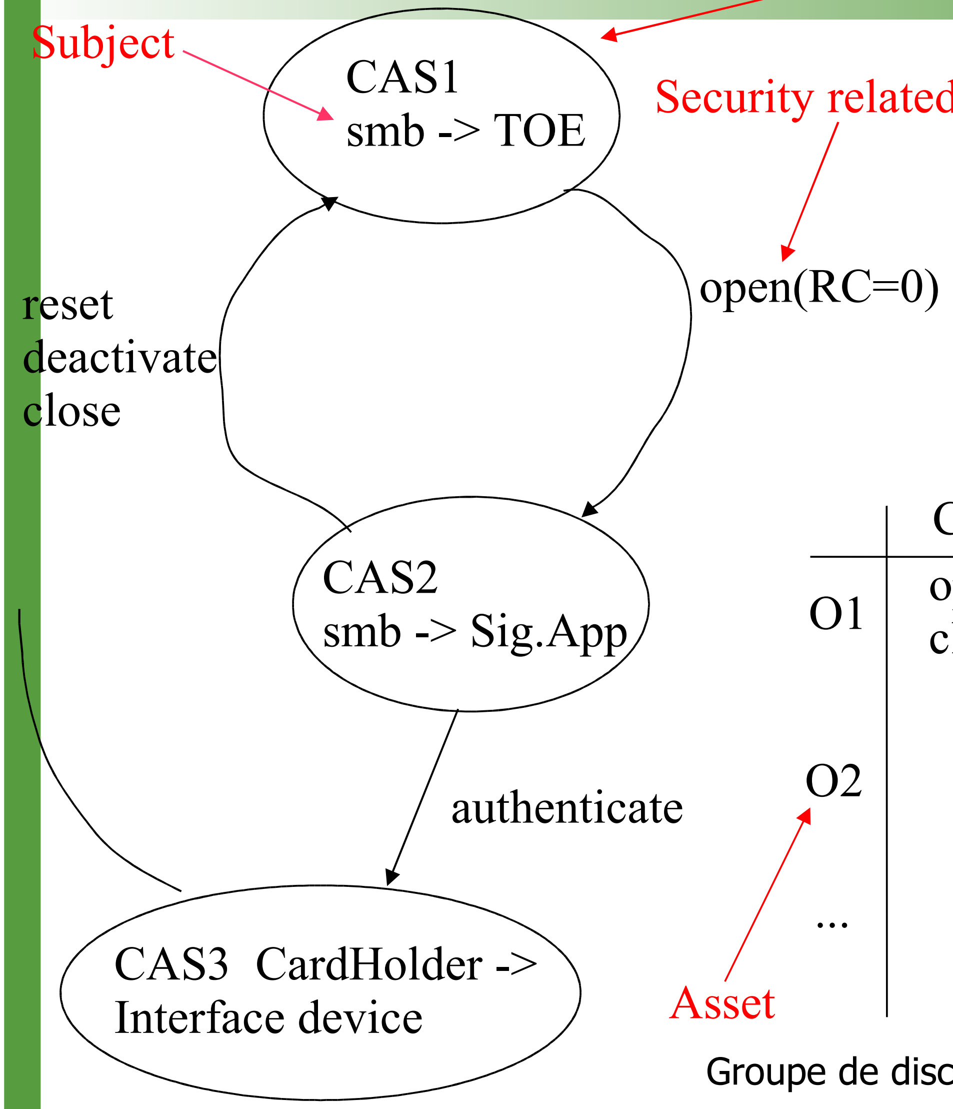


Component 2 Hierarch_to Component 1 =   2 may provide more security or more functionality than 1
==> Legal selections are {1}, {2}, {3}, {1, 3}, {2, 3}

Modelling

- EAL4 : semiformal model of security related functions
  - e.g. : structured natural language, UML diagrams, ...
- EAL5 : formal model of security related functions
  - e.g. : logical theories, finite state machines, state charts diagrams, ...
- => traceability of concepts between security requirements and (semi-)formal models

Traceability of concepts in models



Current Authentication State

Subject

Security related event

Asset

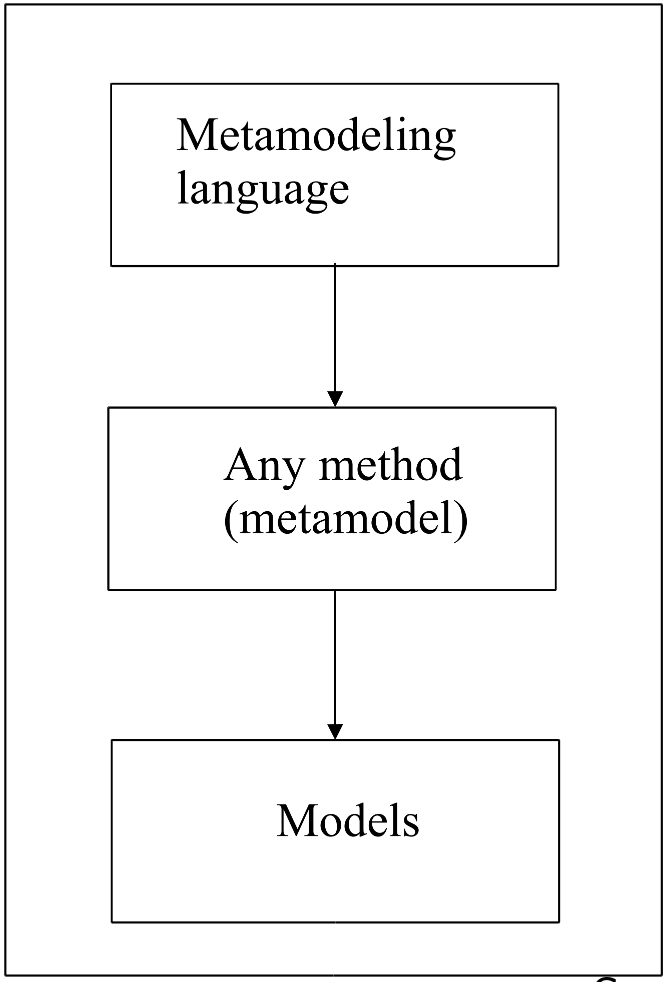
	CAS1	CAS2	CAS3 ...
O1	open close	open close	open close
O2			Use for Sig generation
...			

Functionalities of an editor

- Why an editor tool ?
  - link between requirements library, edition of CC reports and models
  - traceability of concepts
  - integration between stakeholders

Functionalities of an editor

Metacase tool



Metacase tool :

the tool may not dictate how you can design.

Functionalities of an editor

- Semi-automated production of documents :
  - Glossary generation
  - Rationale sections generation
- Support for operations on components
- Database support : requirements library

Tool support: internal consistency

- no unreferenced term
- coverage of every threat, assumption, policy
- coverage of every objective
- coverage of functional components by security functions
- dependencies between components
- legal selections of components
- coverage of assurance components by assurance measures

Tool support: external consistency

- no unassigned component
- no unselected component
- enhancements rationale
- no-inclusion rationale
- conformance claims (ST vs PP, ST vs CC part 2)
- conformance claims (PP/ST vs EAL-x as specified in CC part 3)
- strength of function claims (AVA_SOF : security functions realized by probabilistic/permutational mechanisms)

- Remark : a ST may conform to 0, 1 or more PP's

Conclusion

Positive side

- well-defined, stable and common methodology
- functional and assurance requirements
- encourage vendors to see to security issues they might otherwise neglect in the rush to the market : **correctness + robustness**
- sharing of attack information : “state-of-the-art” security testing
- flexible process : different use scenarios are possible
- Comparison of certified products : EAL **+** Security Functional requirements (! still other issues : implementation, performance, ...)
- Good **reuse** capability :
  - the evaluation results can be combined so that the evaluation costs may be shared over a product range.

Negative side

- Narrow scope : no “system of systems” approach [4]
  - does not address the needs of large-scale organizations and networks
  - how do security and non-security products work together accurately, consistently
- Threat modelling:
  - Static list in PP, come from “domain expert”
  - How to discover, structure and address them ?
- Failed incentive :
  - allows vendors to shop around for favourable evaluation [7]

Some Useful References

[1] : Using B Method to Formalize the Java Card Runtime Security Policy for a Common Criteria Evaluation   S. Motré C. Téri

[2] : Common Criteria Familiarization http://csrc.nist.gov/cc/documents/Guidance/CC_Overview.ppt

[3] : http://www.ssi.gouv.fr/en/documentation/

[4] : http://www.computerworld.com/securitytopics/security/story/0,10801,58497,00.html

[5] : J.L. Lanet , Are Smart Cards the Ideal Domain for Applying Formal Methods, Gemplus Research Laboratory

[6] : Arrival of Windows Server 2003 ....
http://www.microsoft.com/presspass/features/2002/apr03/04-14WS03Security.asp

[7] : R. Anderson, Why Information Security is Hard – an economic perspective http://www.cl.cam.ac.uk/users/rja14/

[8] : S.P. Suresh, Foundations of Security Protocols, Phd Thesis

[9] : Electronic Money System Security Objectives - European Central Bank – May 2003
http://www.ecb.int/ecb/pdf/cons/emoneysecurity/emoneysecurity200305.pdf

[10] : Manager's guide to the Common Criteria http://www.alexragen.com