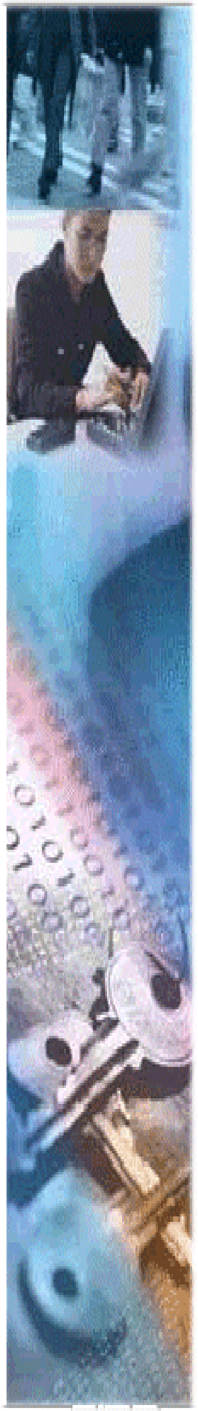
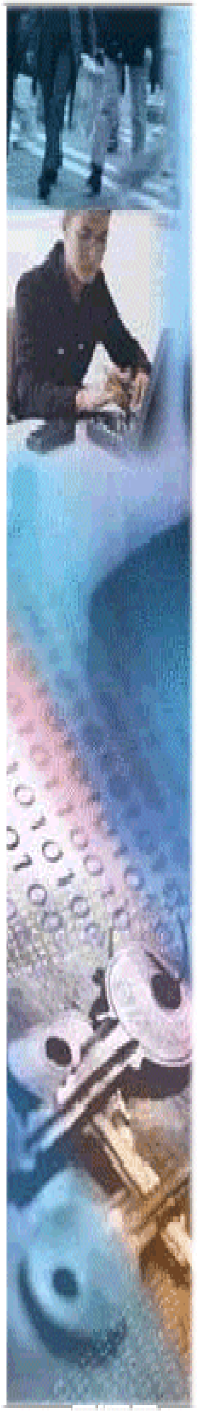
AfriNIC-9 MEETING
Mauritius
22-28 November 2008



IT Security Evaluation : Common Criteria

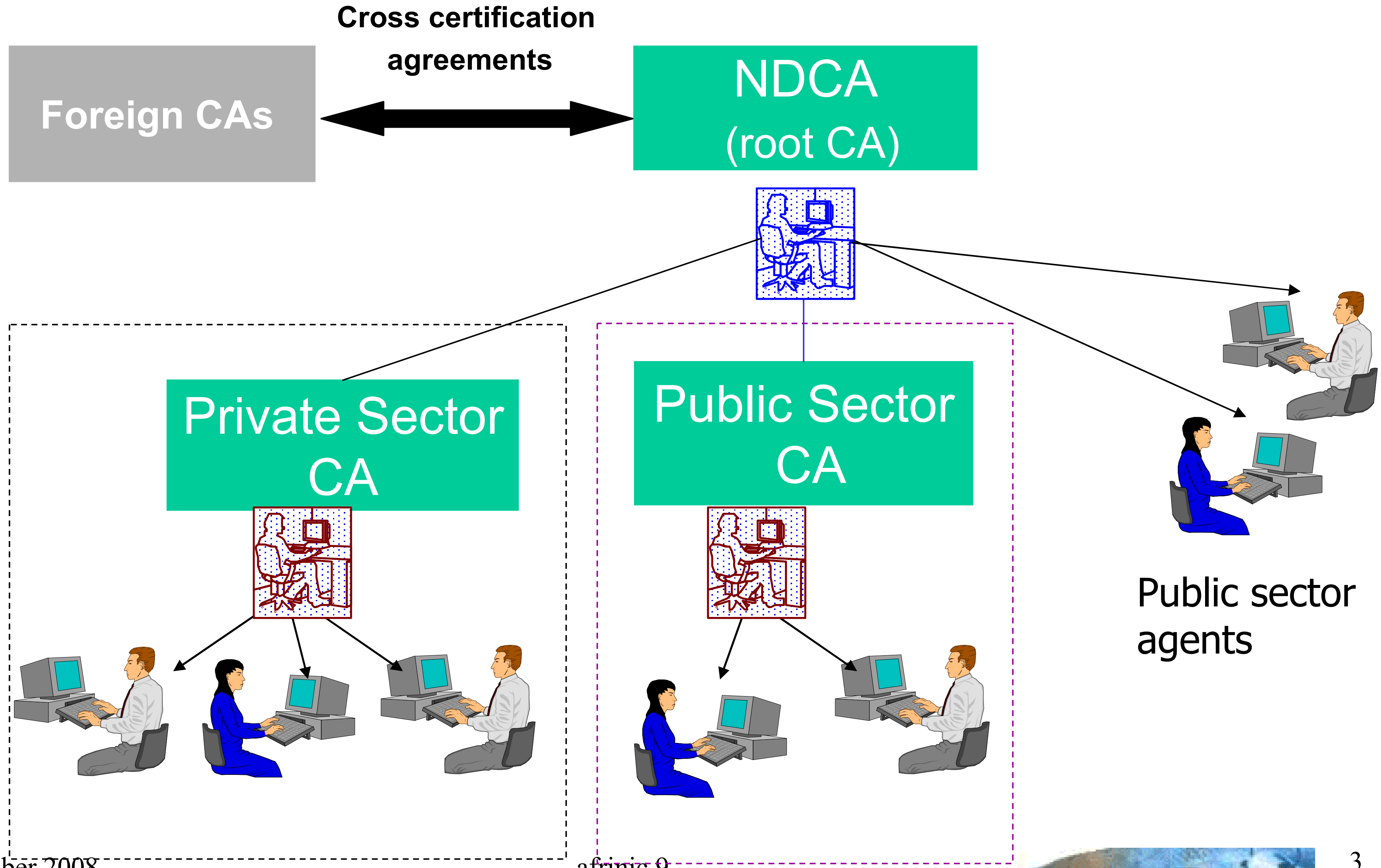
Ministry of Communication Technologies
National Digital Certification Agency
Mounir Ferjani



NDCA

1. **Legal framework** *(2000)*
2. **Technology** based on cryptography, digital certificates and digital signature ***(E-commerce, E-banking, E-gov,…)***
3. **Trusted Third Parties** *(Certification Authorities)*: security policy and procedures, standards, CP and CSP,…
4. **Crypto tools approval**

Tunisian PKI Architecture



Cross certification agreements

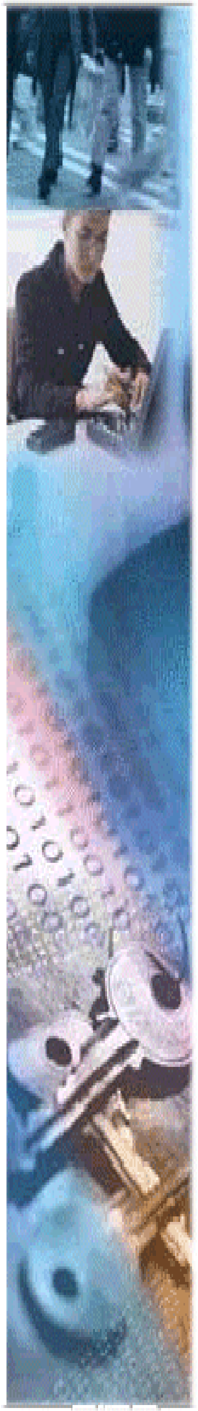
Foreign CAs

NDCA
(root CA)

Private Sector CA

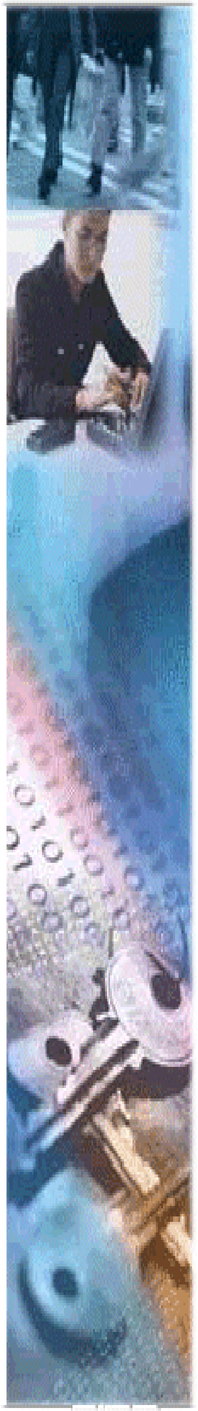
Public Sector CA

Public sector agents



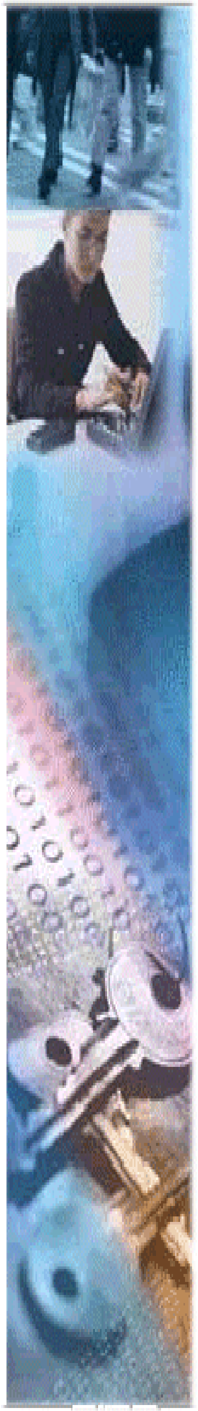
Contents

- IT Security evaluation
- CC evaluation
- Assurance
- Vulnerability



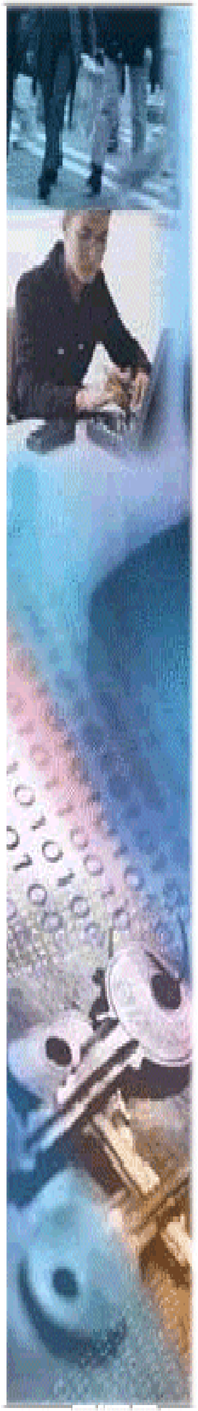
IT security evaluation

- An IT product : is it secure?
  - No ? We can only prove the insecurity.
- What could we do?
  - We can setup confidence degrees in the product security.
- How could we do?
  - A methodology for developing secure products (architecture, implementation, design, development (product + environment), security guidance, testing…)
  - A methodology for security evaluation (security specification documents, Evaluation technical reports, standards (e.g. crypto)).
  - Vulnerability assessment
  - Penetration testing

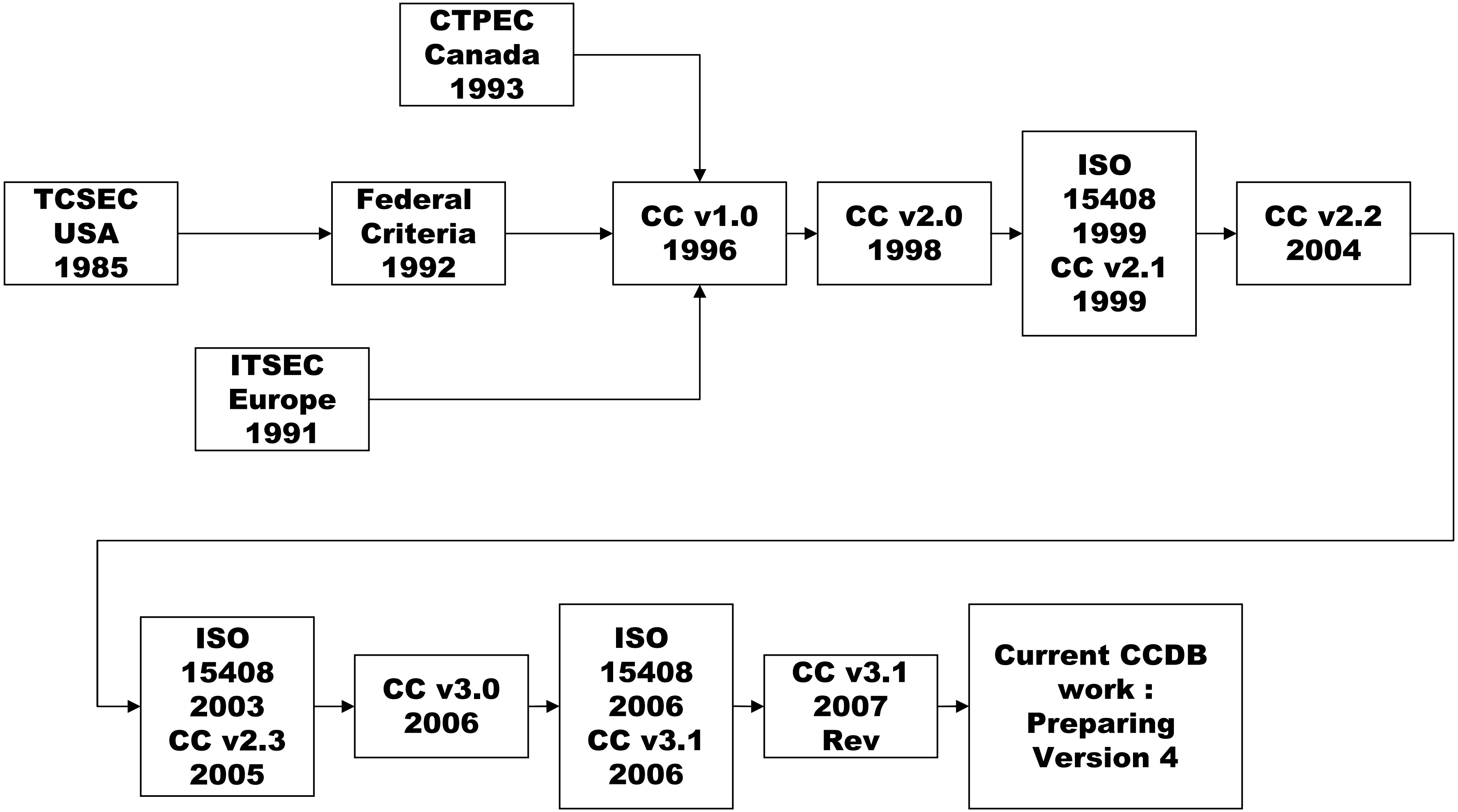


Contents

- IT Security evaluation
- CC evaluation
- Assurance
- Vulnerability



History



TCSEC USA 1985

Federal Criteria 1992

CTPEC Canada 1993

ITSEC Europe 1991

CC v1.0 1996

CC v2.0 1998

ISO 15408 1999 CC v2.1 1999

CC v2.2 2004

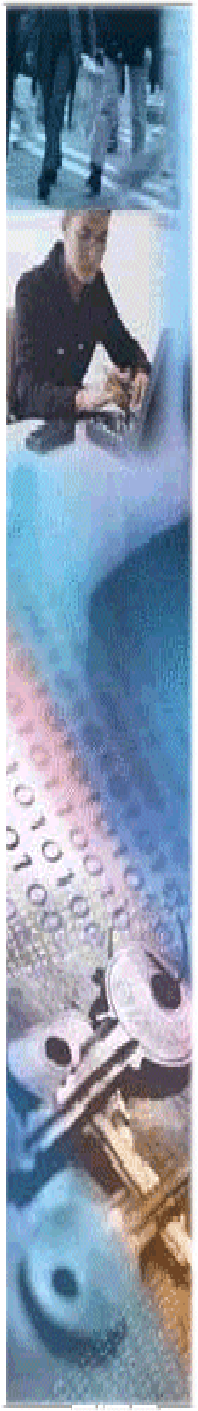
ISO 15408 2003 CC v2.3 2005

CC v3.0 2006

ISO 15408 2006 CC v3.1 2006

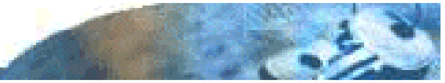
CC v3.1 2007 Rev

Current CCDB work : Preparing Version 4



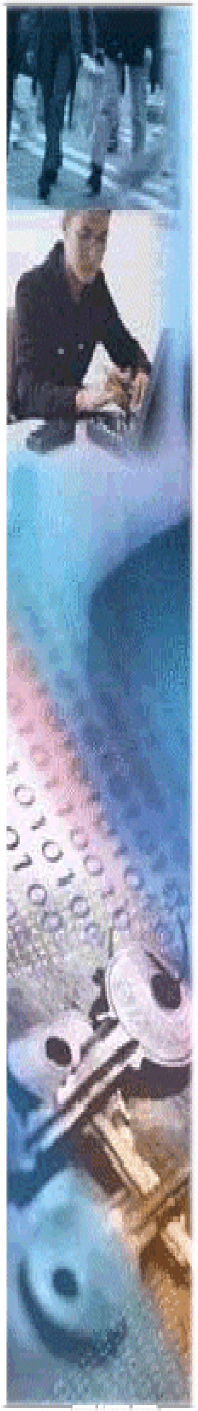
Target audience

- **Consumers**
  - They identify security needs from risk analysis, ...
  - They use evaluation results to help decide if the TOE fulfills their security needs.
- **Developers**
  - They use specifications in STs and PPs to develop conformant TOE
- **Evaluators**
  - CC provides means of evaluation and methodology.

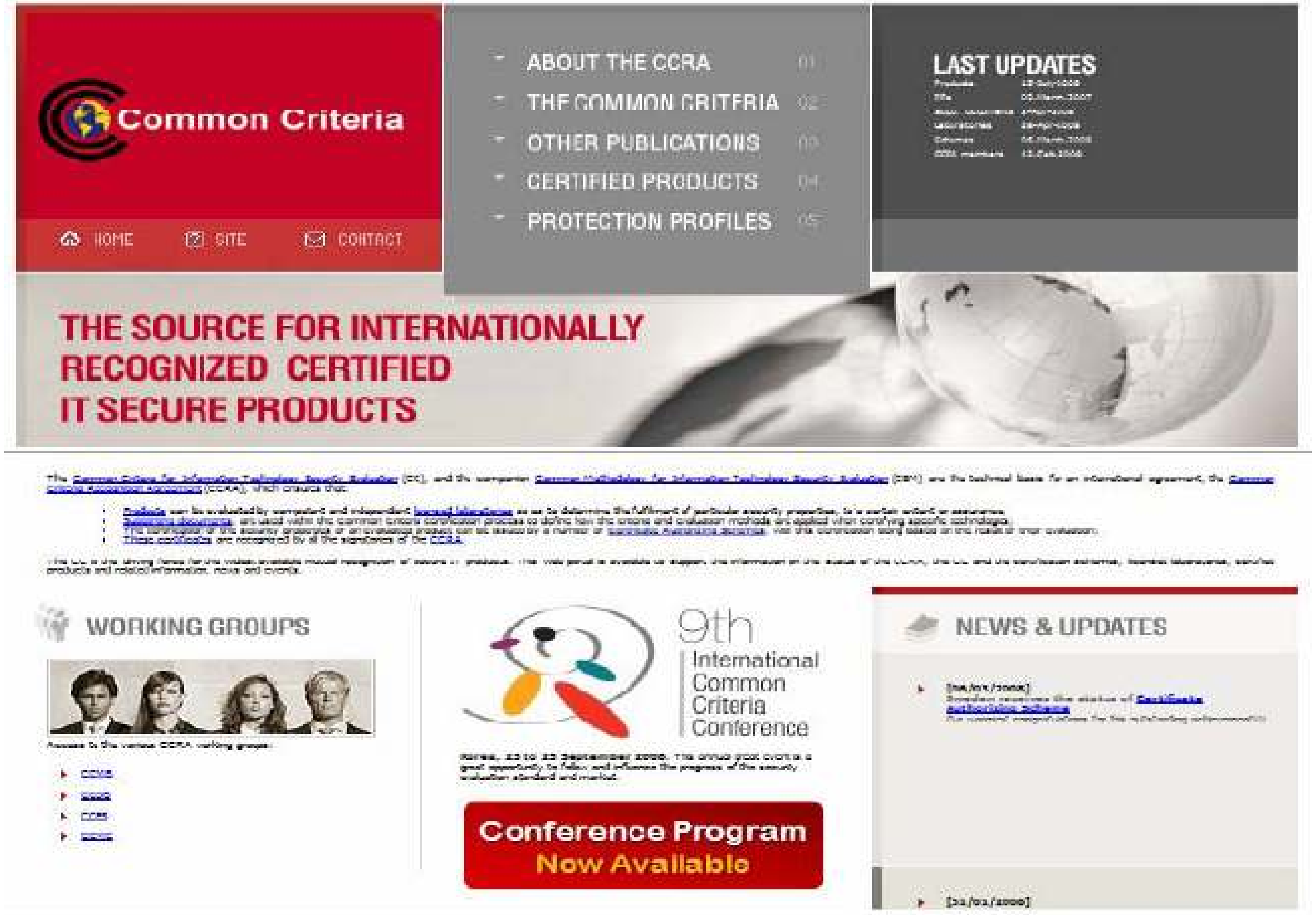


CC structure

- CC part I : Introduction and general model
- CC Part 2 : Security functional requirements
  - Catalogue of security requirements classes
- CC Part 3 : Security assurance requirements
  - Catalogue of security assurance classes
- CEM : Evaluation methodology
  - Methodology for technical reports, roles in and between schemes,…



CC portal



THE SOURCE FOR INTERNATIONALLY RECOGNIZED CERTIFIED IT SECURE PRODUCTS

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
- These certificates are recognized by all the signatories of the CCRA.

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

WORKING GROUPS

Access to the various CCRA working groups.

- CCMB
- [illegible]
- CCES
- [illegible]

9th International Common Criteria Conference

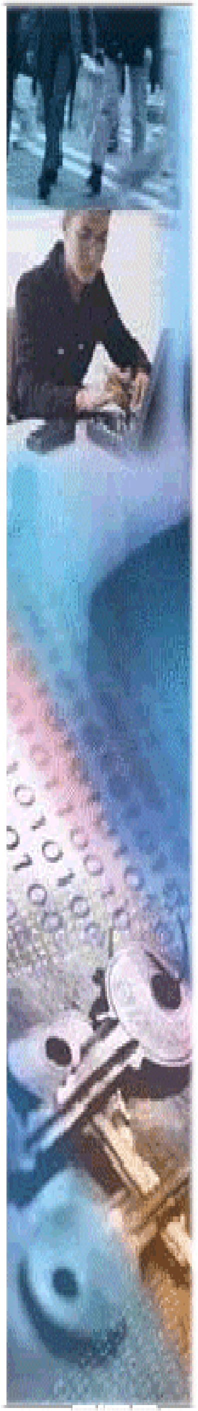
Korea, 23 to 25 September 2008. The annual ICCC event is a great opportunity to follow and influence the progress of the security evaluation standard and market.

Conference Program Now Available

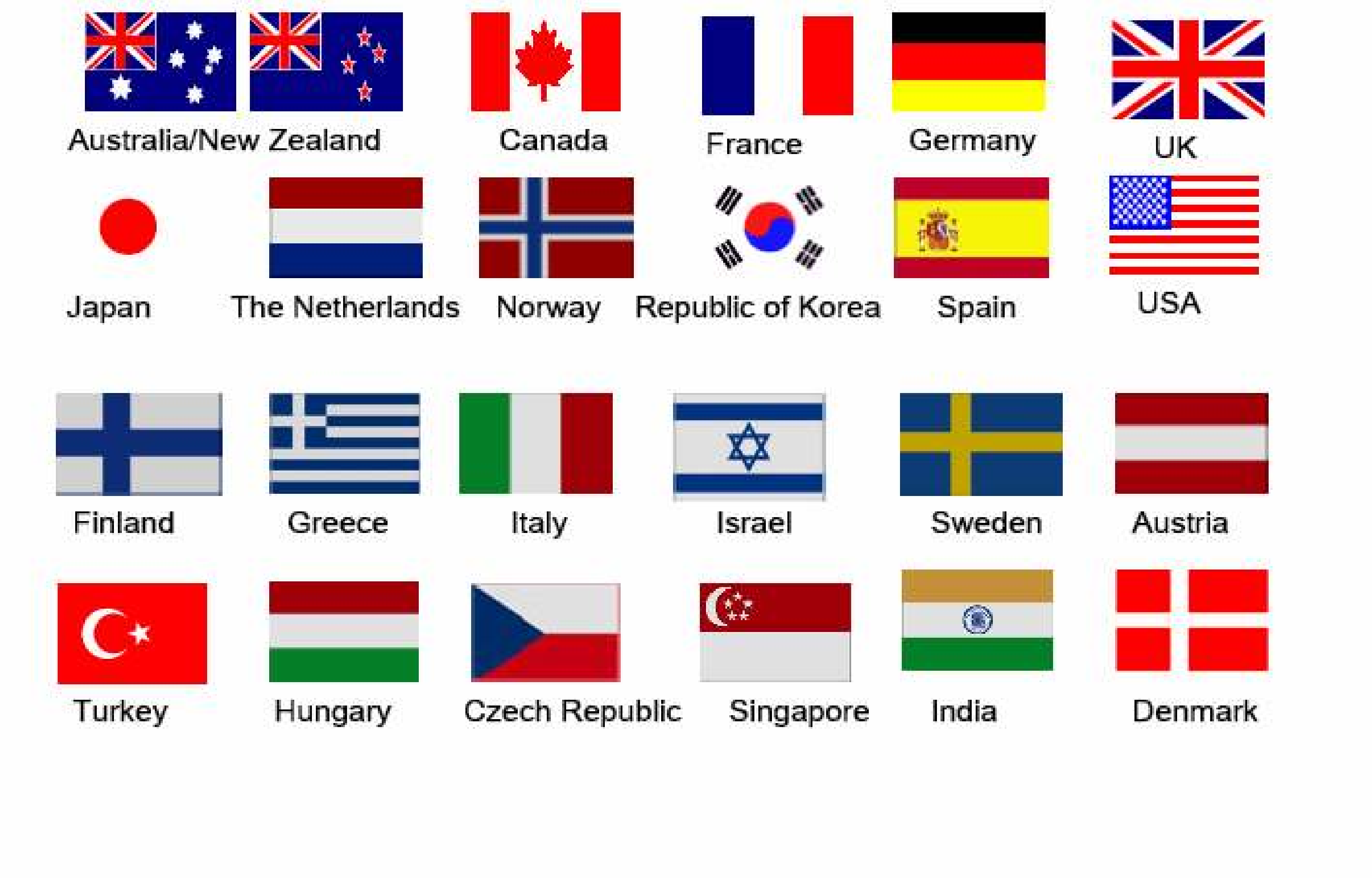
NEWS & UPDATES

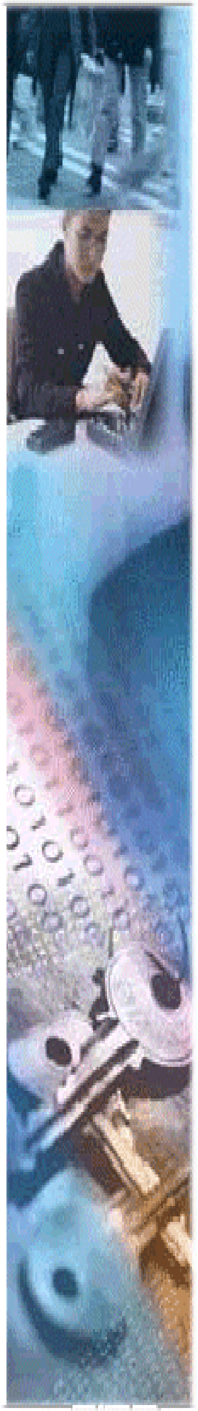
- [illegible]
- [illegible]

www.commoncriteriaportal.org



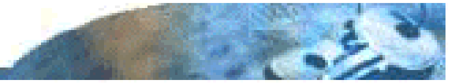
CCRA

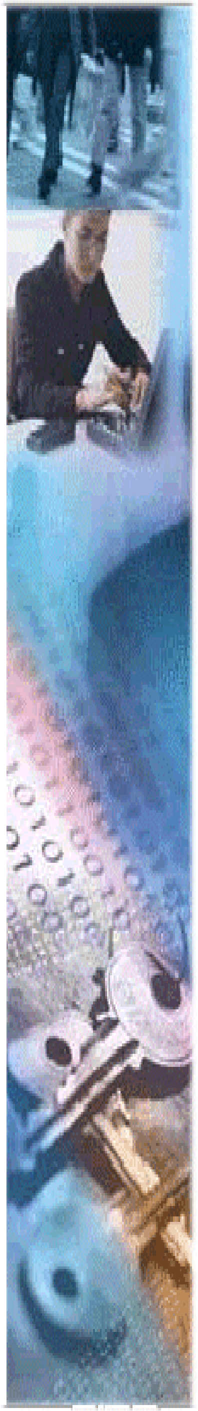

Australia/New Zealand
Canada
France
Germany
UK
Japan
The Netherlands
Norway
Republic of Korea
Spain
USA
Finland
Greece
Italy
Israel
Sweden
Austria
Turkey
Hungary
Czech Republic
Singapore
India
Denmark



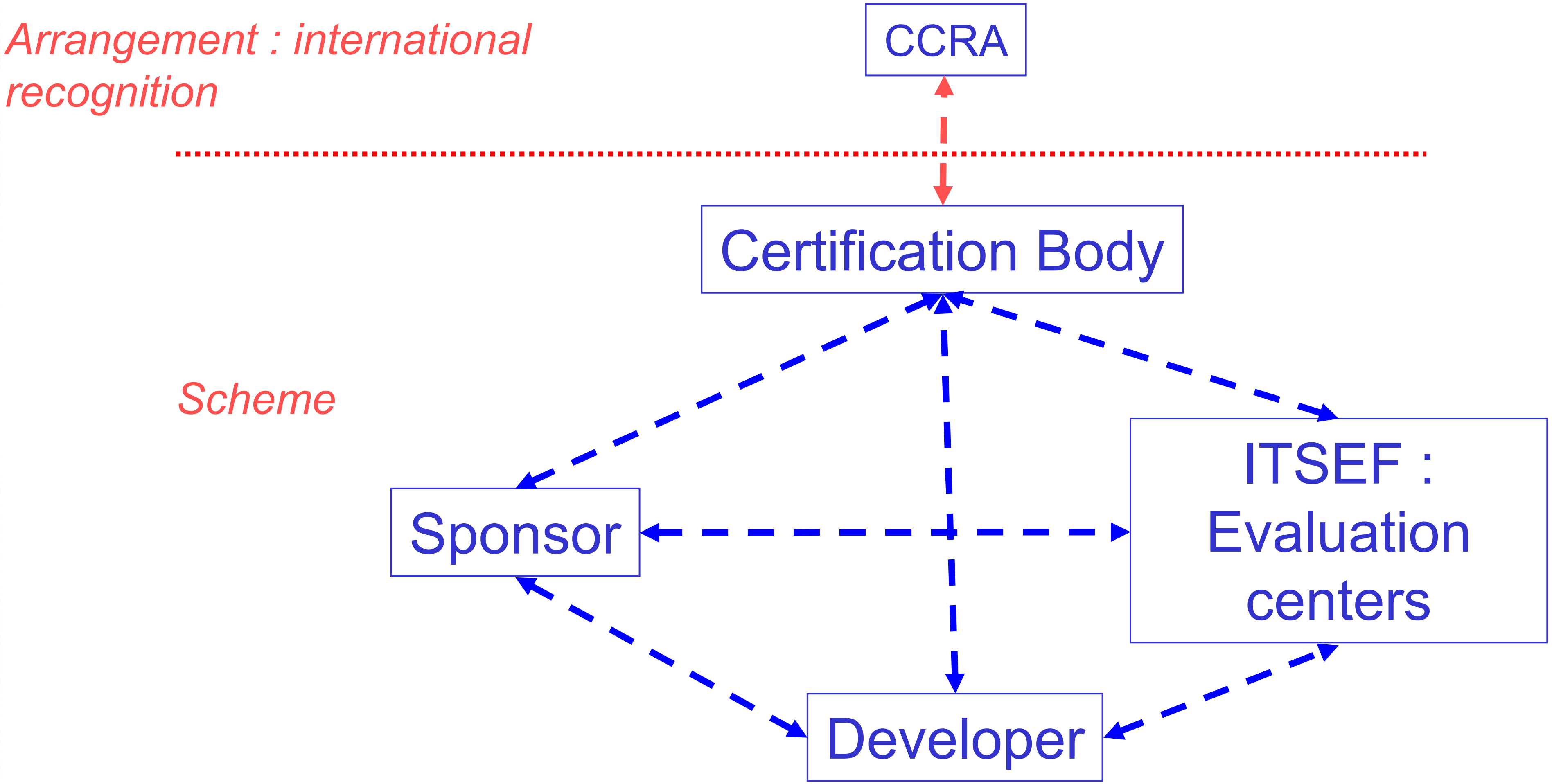
Evaluation context (1/2)

- Evaluation authority :
  - Sets the standards, administers the regulations, to which the evaluators and evaluation facilities must conform.
  - The CC does not state requirements for regulation.
  - CCRA is an example of regulatory framework.
  - The need for expertise is necessary.





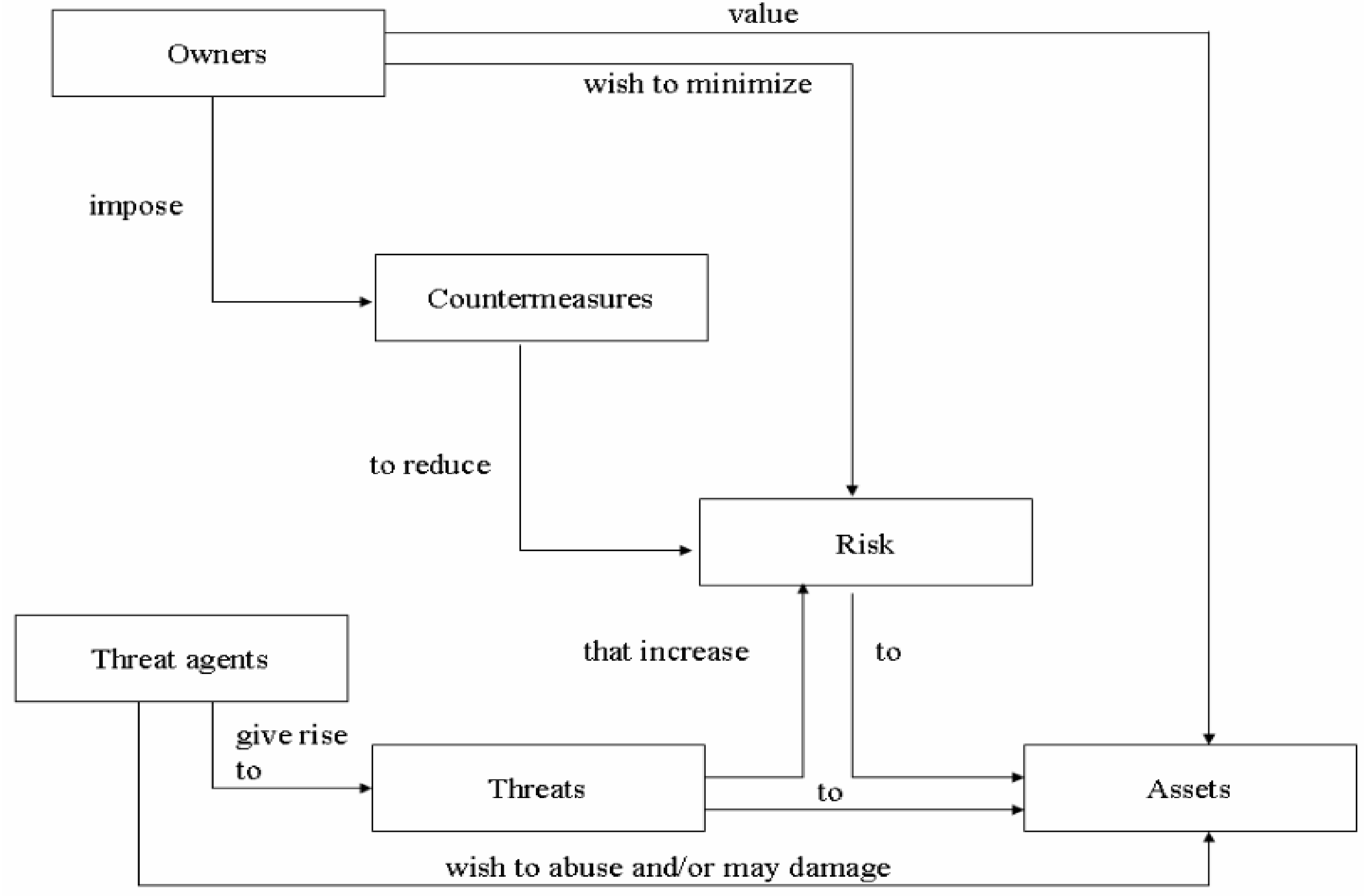
Evaluation context (2/2)



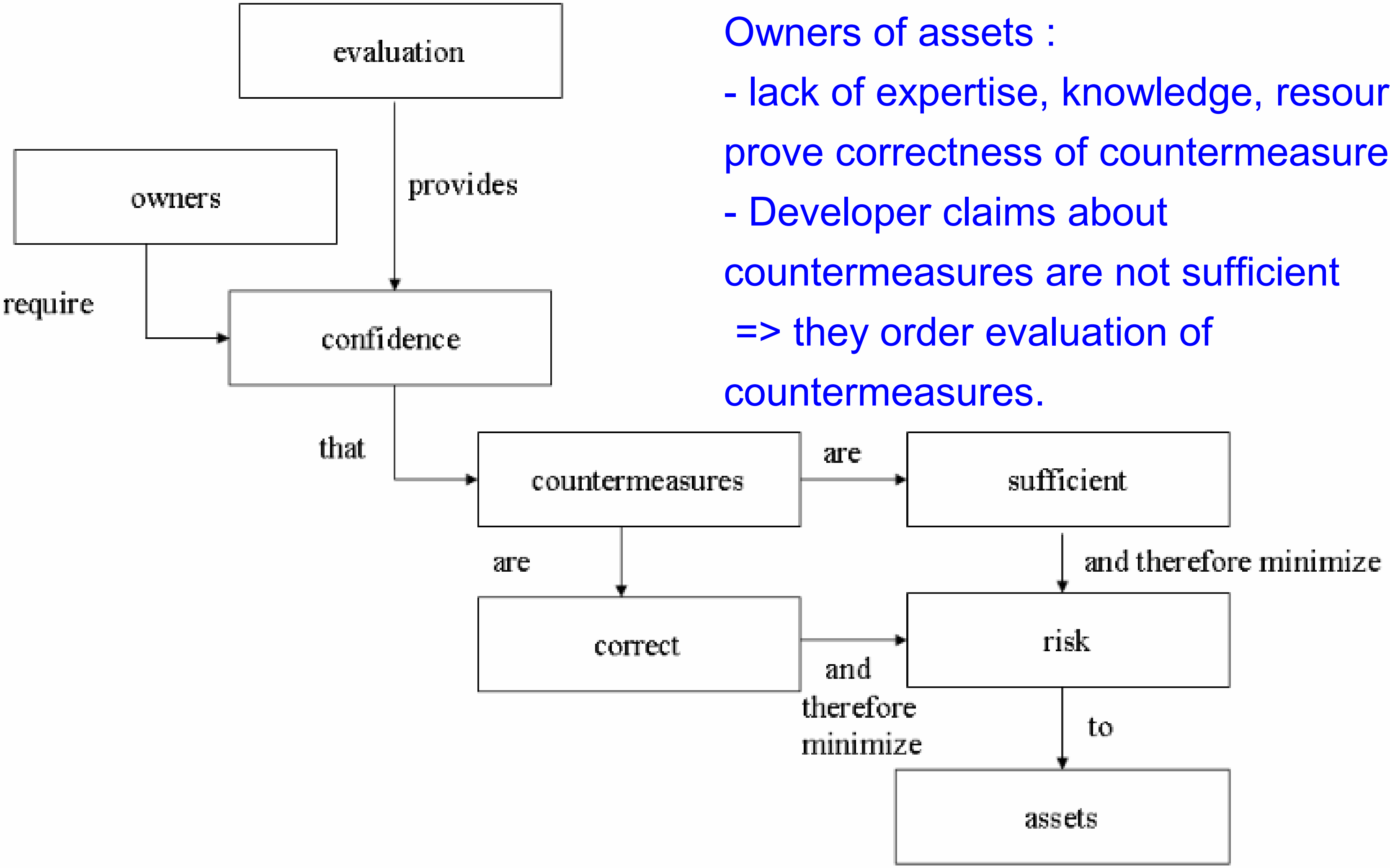
Arrangement : international recognition

Scheme

Security concepts and relationships



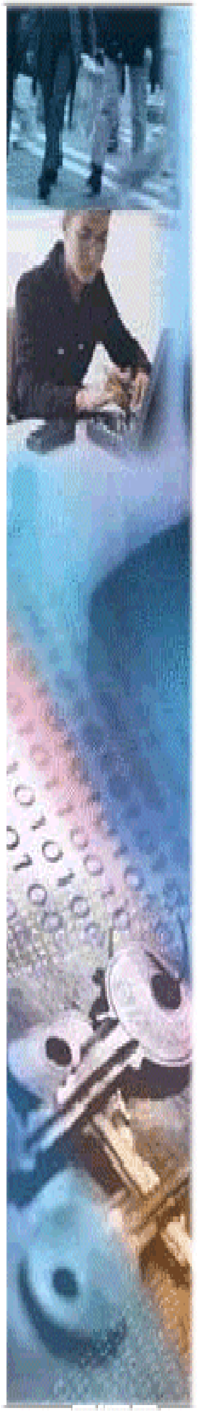
Evaluation Concepts and relationships



Owners of assets :

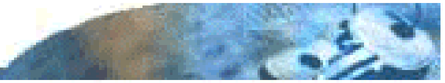
- lack of expertise, knowledge, resource to prove correctness of countermeasures
- Developer claims about countermeasures are not sufficient

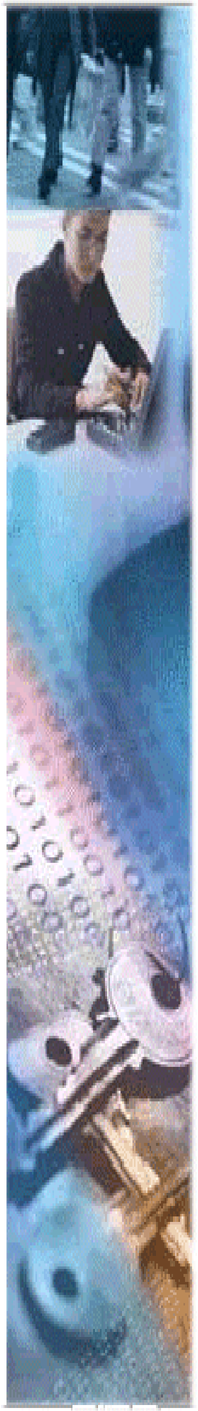
=> they order evaluation of countermeasures.



Definitions (1/2)

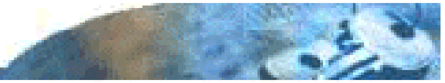
- **TOE =** IT product, a part of an IT product, a set of IT products.
- **Representations of a TOE :**
  - A single master copy that just have been compiled
  - An installed and operational version
- **Configurations :**
  - A TOE must verify security requirements so it must allow only configuration or configurations that do not differ in security relevant ways
  - E.g. The administrator does not need to be authenticated # (contradiction)
  - That's why we say CC is constraint by a configuration.
  - TOE guide is different from IT product guide (TOE guide treats only certain configurations that verify security requirements).

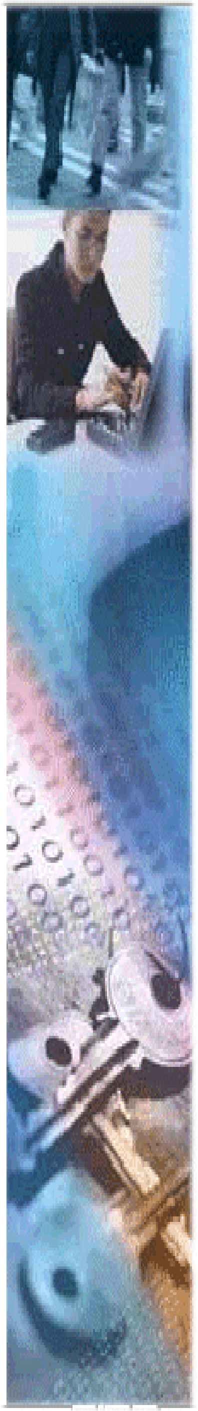




Definitions (2/2)

- Functionality (SFR) :
  - Defines the TOE security needs for the TOE.
- Assurance (SAR) :
  - Assurance needs.
  - Confidence degree in the enforcement of the security objectives of a TOE ⇔ **Correctness** & **Effectiveness.**
- Documents to write needs :
  - ST : Security Target
  - PP : Protection Profile



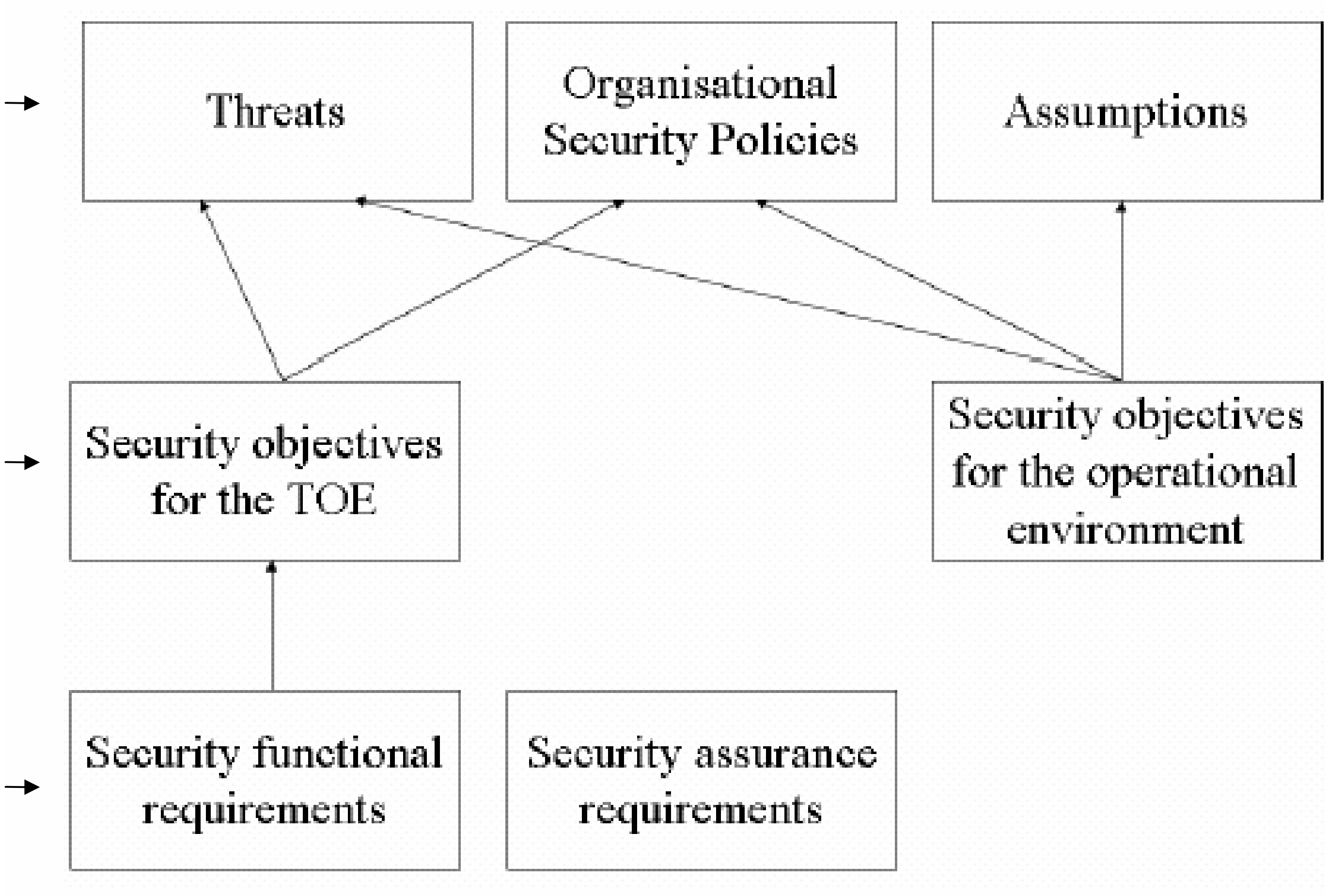


General View

SPD →

OBJ →

CC SPEC →



Threats

Organisational Security Policies

Assumptions

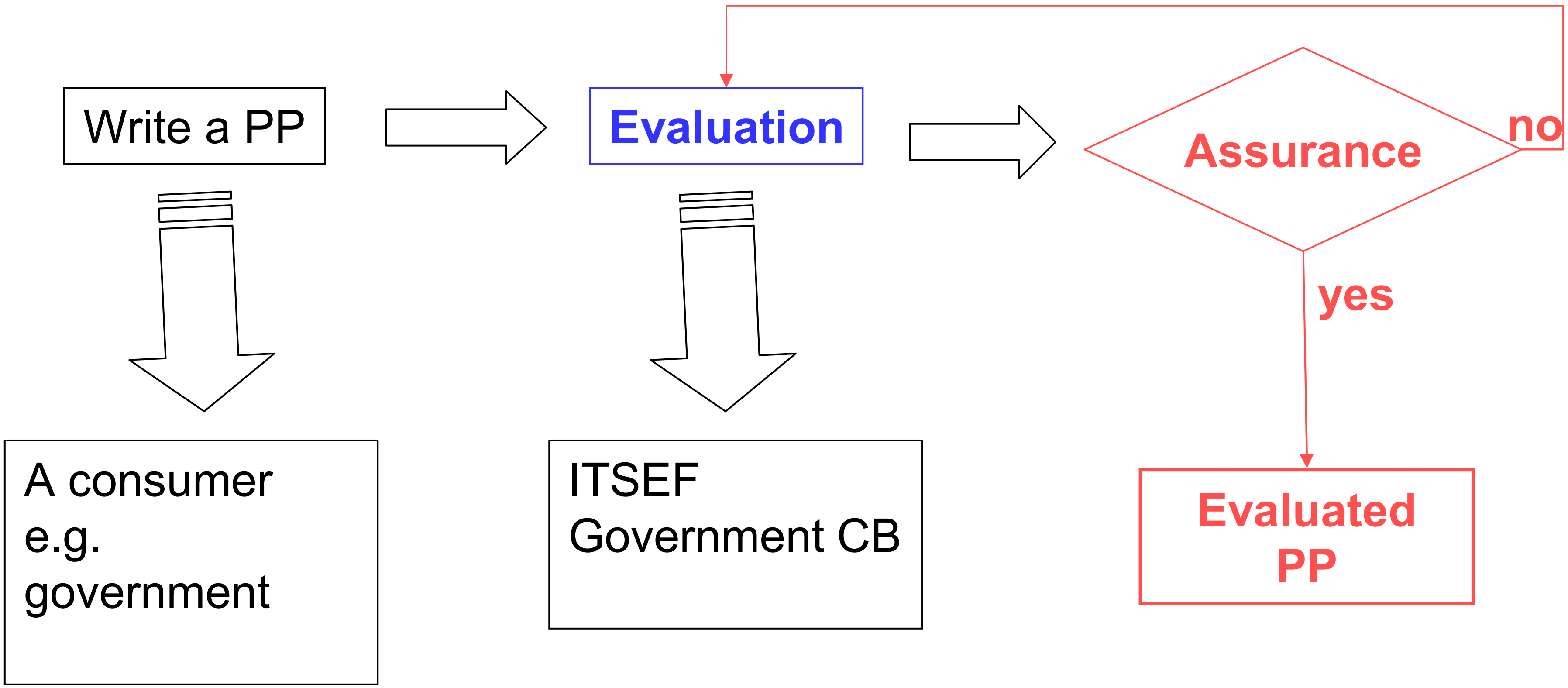
Security objectives for the TOE

Security objectives for the operational environment

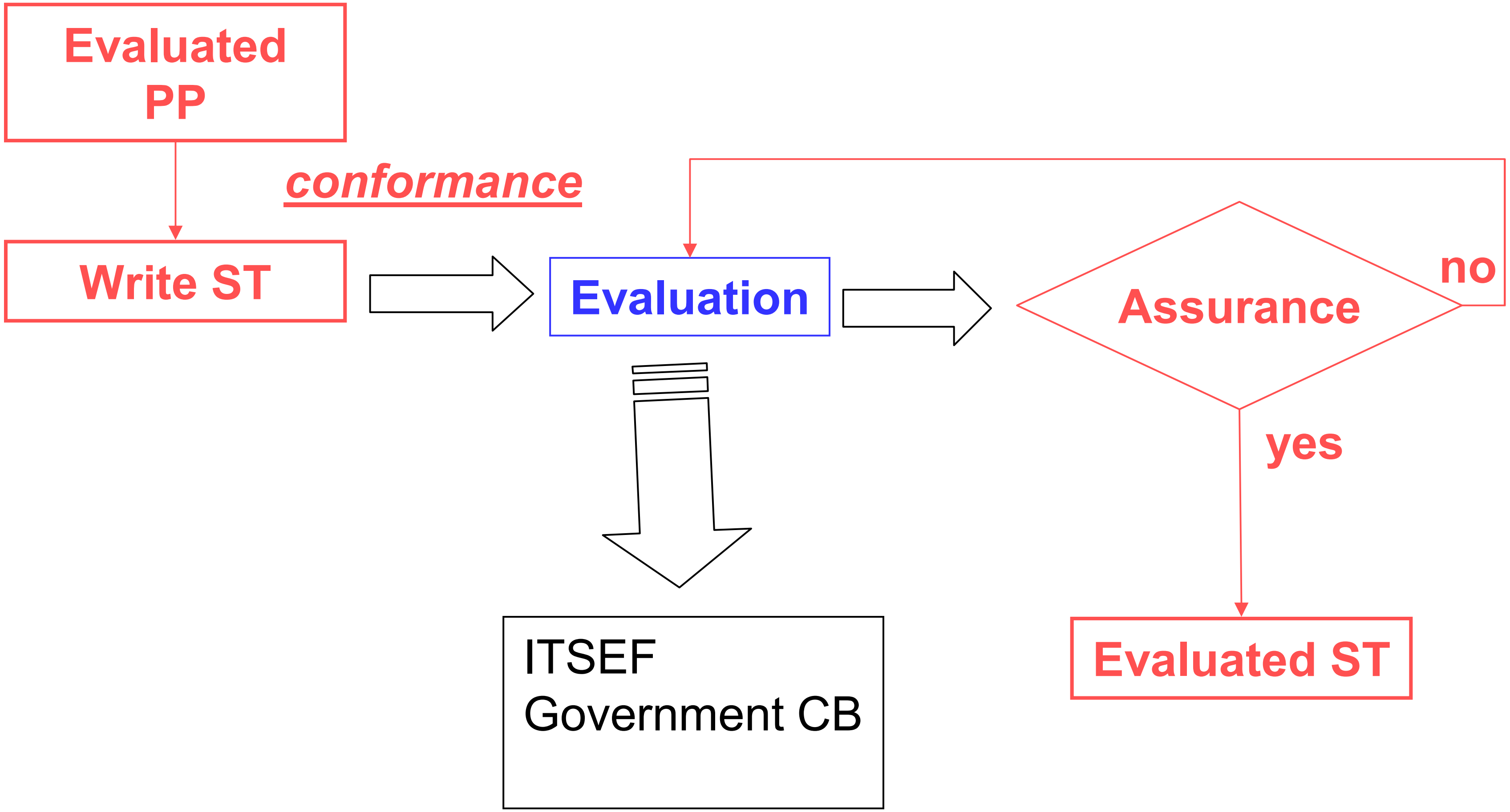
Security functional requirements

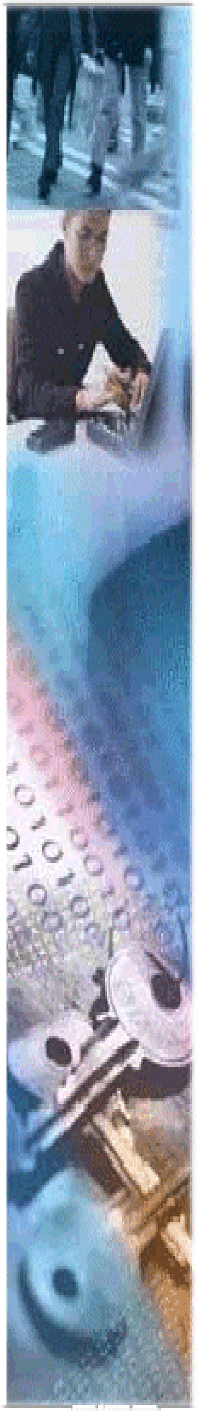
Security assurance requirements

Process (1/3)

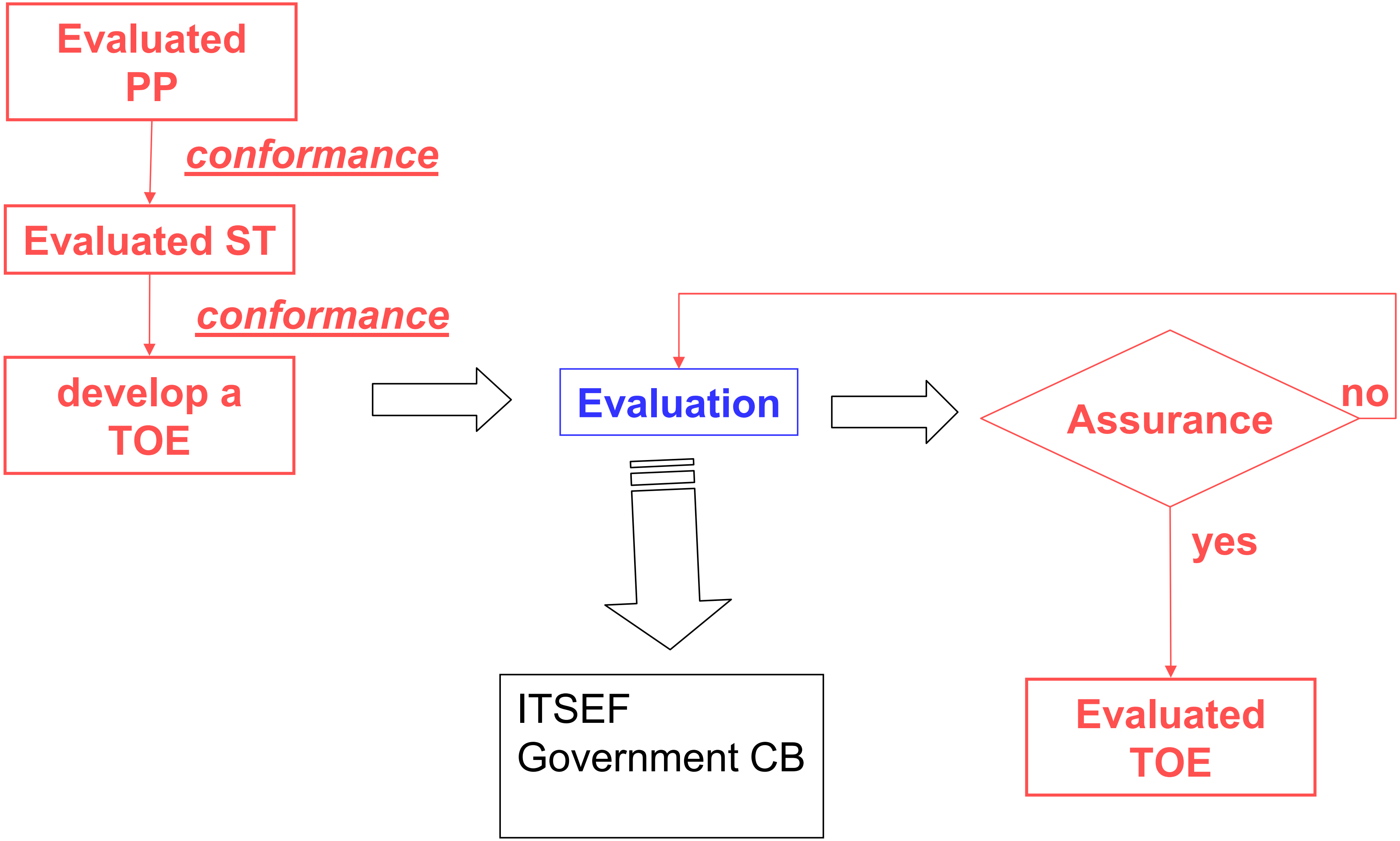

Write a PP
Evaluation
Assurance
no
yes
A consumer e.g. government
ITSEF Government CB
Evaluated PP

Process (2/3)


Evaluated PP
conformance
Write ST
Evaluation
Assurance
no
yes
ITSEF
Government CB
Evaluated ST



Process (3/3)



Evaluated PP

conformance

Evaluated ST

conformance

develop a TOE

Evaluation

Assurance

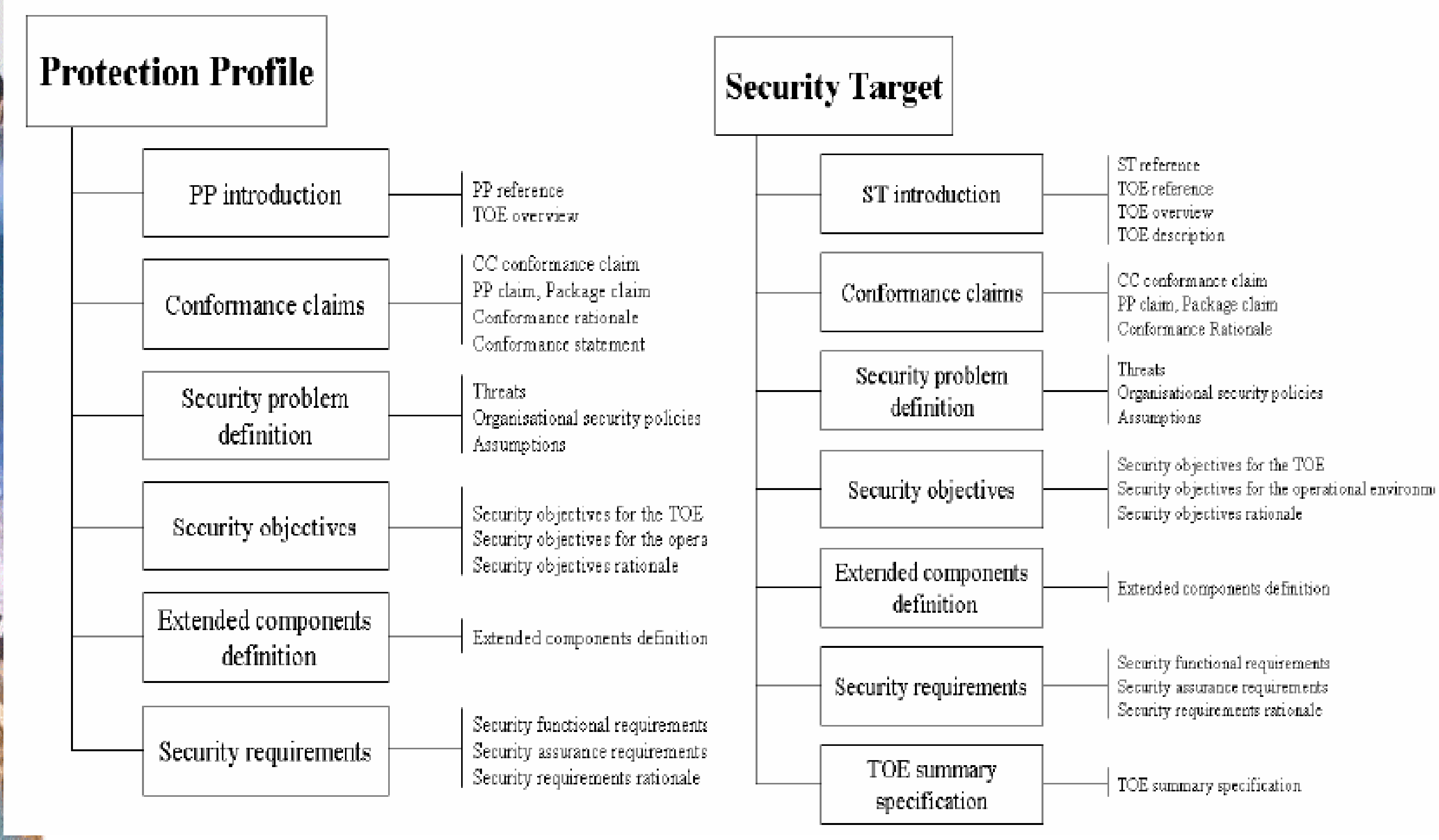
no

yes

ITSEF
Government CB

Evaluated TOE

PP & ST content

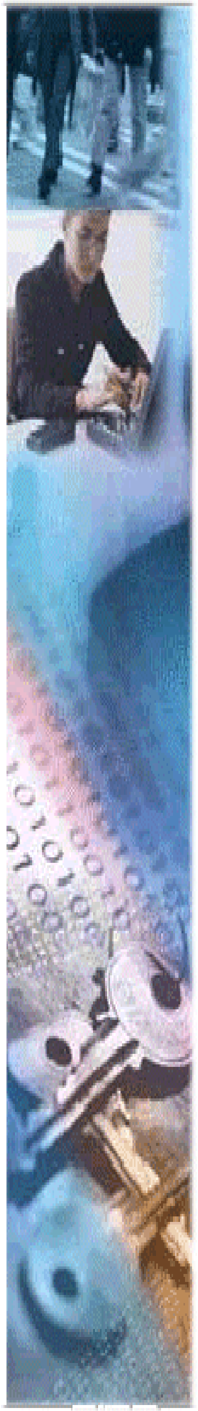


Protection Profile

- PP introduction
  - PP reference
  - TOE overview
- Conformance claims
  - CC conformance claim
  - PP claim, Package claim
  - Conformance rationale
  - Conformance statement
- Security problem definition
  - Threats
  - Organisational security policies
  - Assumptions
- Security objectives
  - Security objectives for the TOE
  - Security objectives for the opera
  - Security objectives rationale
- Extended components definition
  - Extended components definition
- Security requirements
  - Security functional requirements
  - Security assurance requirements
  - Security requirements rationale

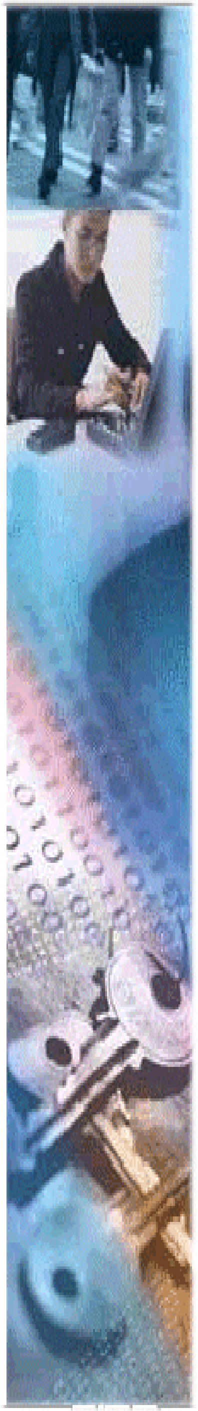
Security Target

- ST introduction
  - ST reference
  - TOE reference
  - TOE overview
  - TOE description
- Conformance claims
  - CC conformance claim
  - PP claim, Package claim
  - Conformance Rationale
- Security problem definition
  - Threats
  - Organisational security policies
  - Assumptions
- Security objectives
  - Security objectives for the TOE
  - Security objectives for the operational environm
  - Security objectives rationale
- Extended components definition
  - Extended components definition
- Security requirements
  - Security functional requirements
  - Security assurance requirements
  - Security requirements rationale
- TOE summary specification
  - TOE summary specification



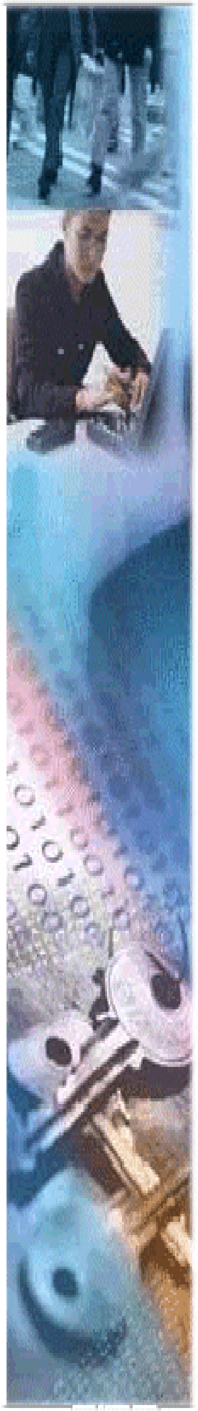
Contents

- IT Security evaluation
- CC evaluation
- Assurance
- Vulnerability

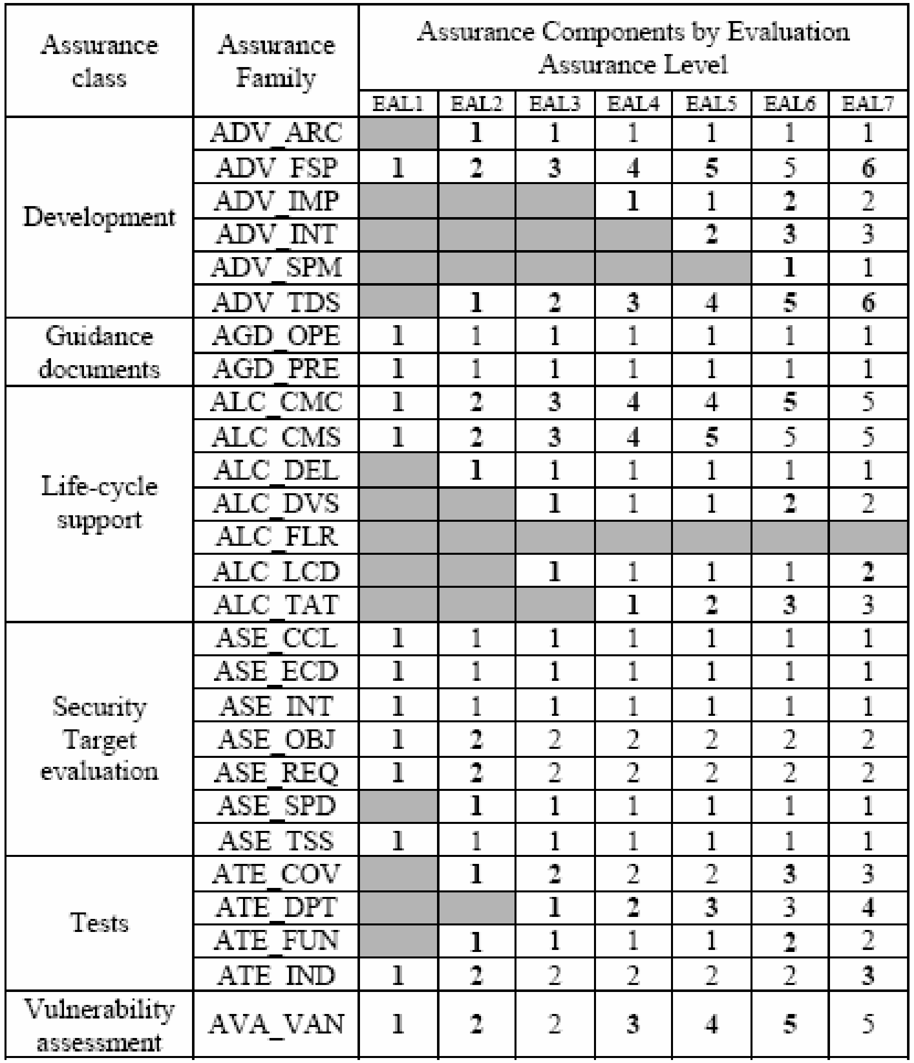


Assurance

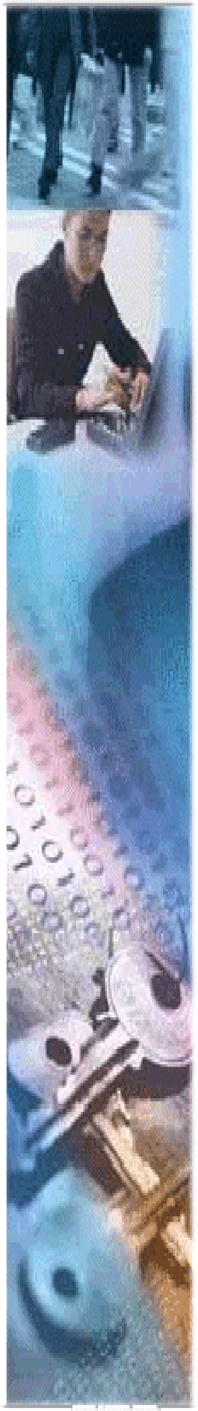
- Assurance is based on evaluation
- CEM defines 4 levels of assurance in the EAL packages.
    - But we can go up to EAL 7.
- It depends on how conducted the vulnerability analysis.
- EAL1 : functionality tested
    - TSF testing using TSFI and vulnerability analysis from public domain.
- EAL2 : structurally tested
    - design infos : basic architectural infos
- EAL3 : methodically tested and checked
    - vulnerability analysis based on architecture of the TOE
- EAL 4 : methodically designed, tested, and reviewed
    - Implementation
- EAL5-7 : Semi formal and formal testing and verification



EAL summary

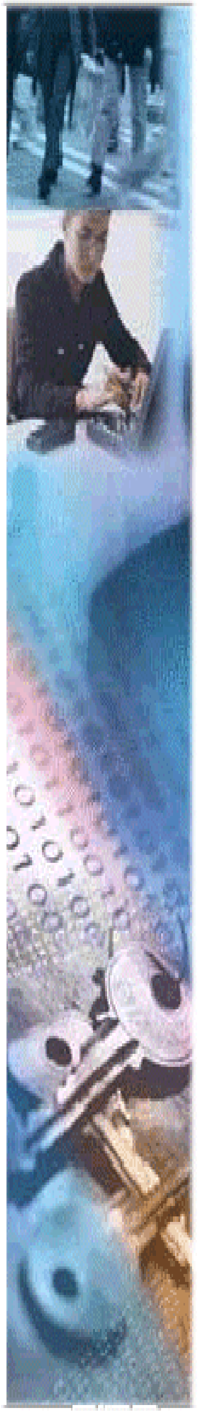


Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	4	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	**2**	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	4	**5**	5



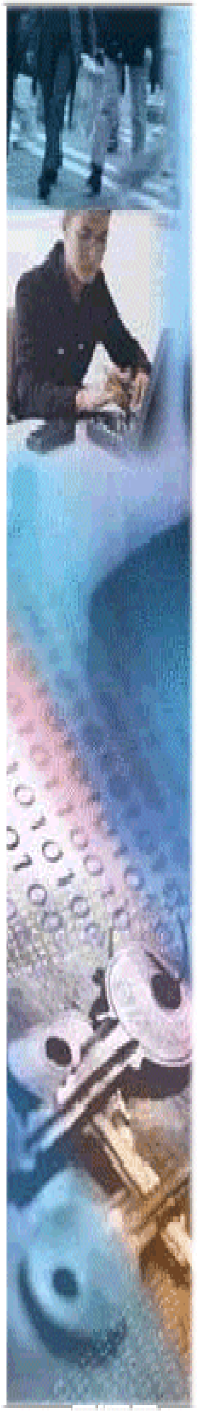
Contents

- IT Security evaluation
- CC evaluation
- Assurance
- Vulnerability



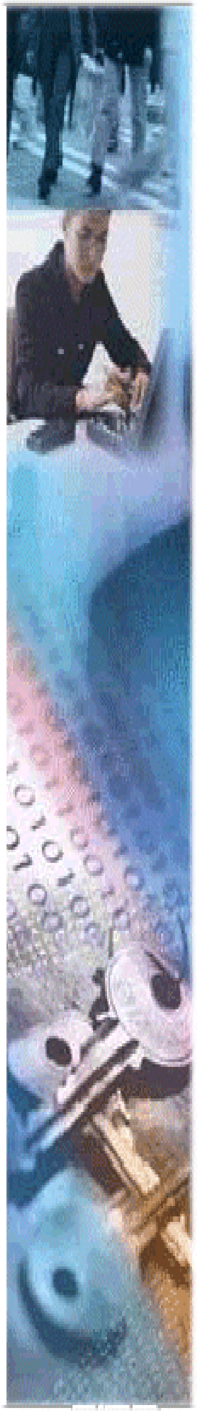
Vulnerability analysis (1/2)

- Vulnerability : a weakness in the TOE that can be used to violate the SFRs in some environment.
- Vulnerability analysis : a systematic search for vulnerabilities in the TOE and an assessment of those found to determine their relevance for the intended environment for the TOE.
- Penetration testing : A testing carried out to determine the exploitability of TOE potential vulnerabilities

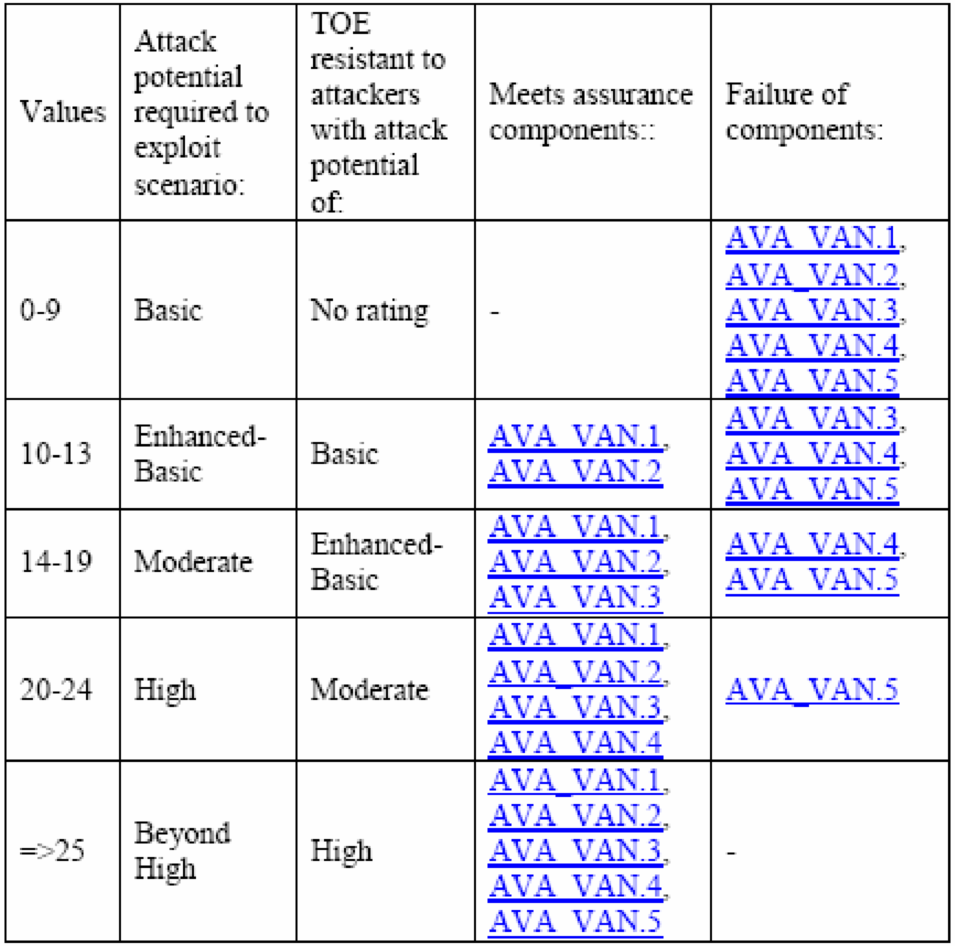


Vulnerability analysis (2/2)

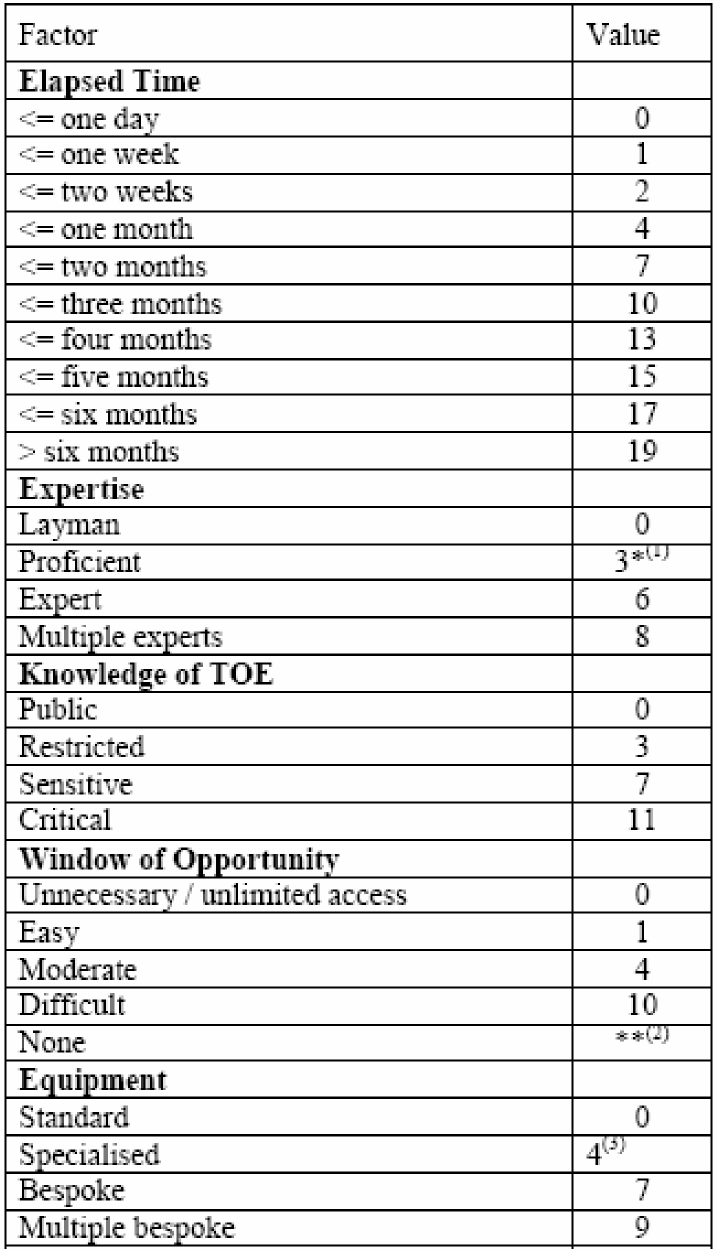
- Attack potential factors :
  - Time elapsed to identify an exploit.
  - Specialist technical expertise required.
  - Knowledge of the TOE design and implementation.
  - Hardware/software required to perform exploitation.
  - Window of opportunity



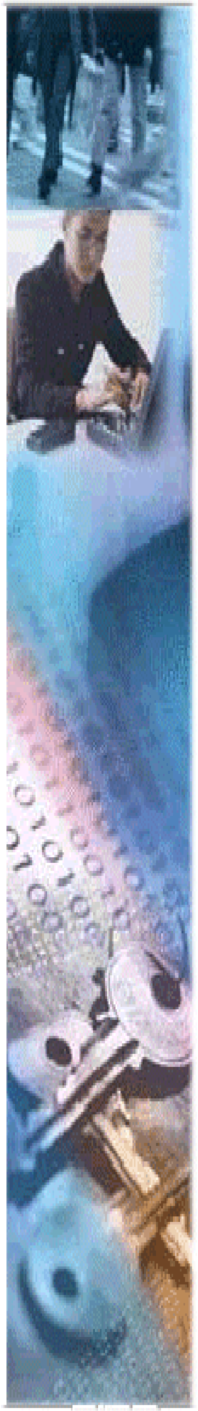
Attack potential calculation



Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

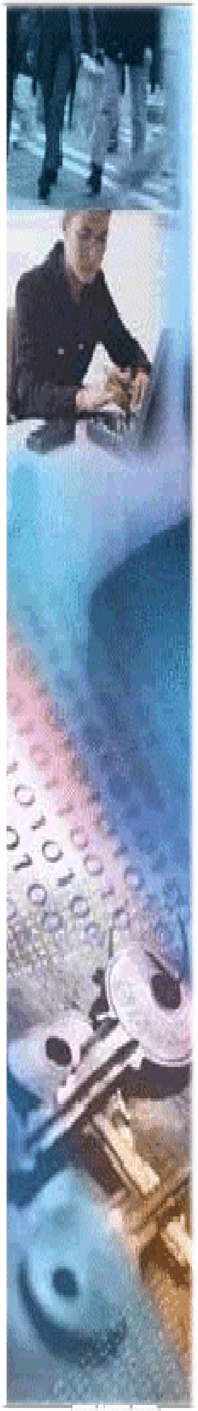


Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9



Conclusion

- A complete IT security standard.
- Complex.
- Legal framework : requires a national scheme setup.
- International recognition framework : CCRA : between countries, !!!
  - Consumer participant application.
  - Authorizing participant application.



Thank you

Questions?