Introduction to ISO/IEC 15408

Evaluation and Application

TUV Asia Pacific Ltd.
IT Business Dept.
Manager
Philip

Office: +886-2-2378-0578
Mobile: +886-930-807-346
e-Mail: philipku@tuev-nord.de

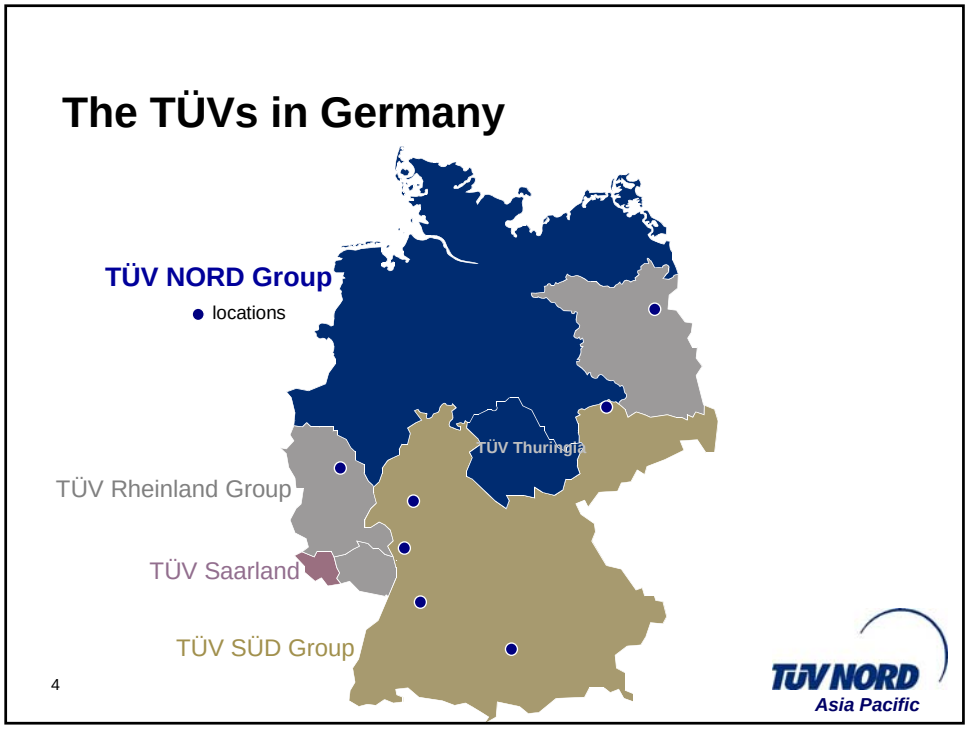
TÜV NORD
Asia Pacific

Contents

- Common Criteria overview
- Common Criteria evaluation
- Banking criteria evaluation

TÜV NORD
Asia Pacific


in Germany, we say...
„Sicherheit“
that means „Secutity“ and „Safety“


The TÜVs in Germany
TÜV NORD Group
locations
TÜV Thuringia
TÜV Rheinland Group
TÜV Saarland
TÜV SÜD Group
4
TÜV NORD
Asia Pacific

TÜV NORD Asia Pacific – IT services

ISMS (ISO 27001)
ITBPM
ITIL / ITSM (ISO 20000)
SQ, Security Qualification
Common Criteria (ISO 15408)
Functional Safety (IEC 61508)
ISO 9000, QS 9000
ISO/TS 16949
ISO 14001
OHSAS 18001
EN 46000
HACCP
VDA6.1
GS
CE Mark
EMC Test
…

astern Europe

…
t
mirates…

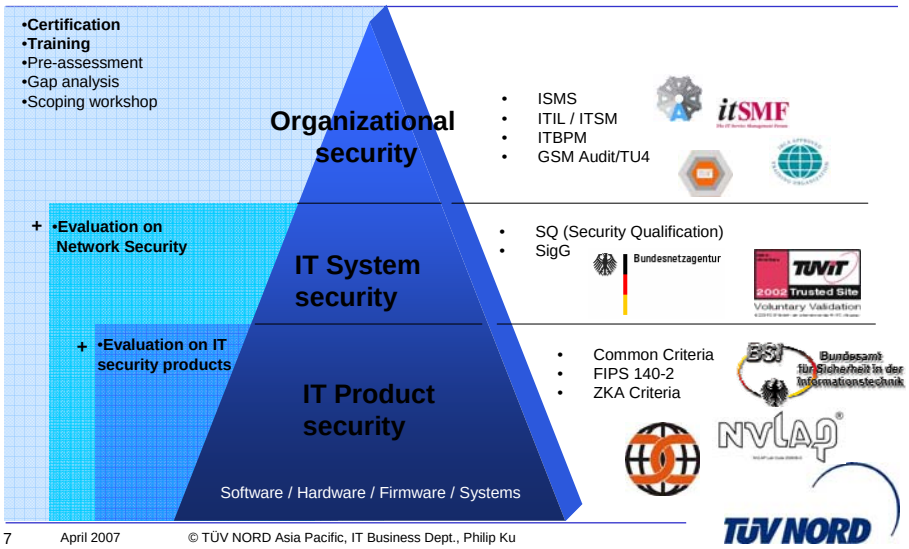
Asia Pacific
China
Hong Kong
India
Indonesia
Iran
Japan
Korea
Malaysia
Philippines
Taiwan
Thailand
Vietnam …

"We provide IT professional services in the field of Security and Safety related testing / evaluation / certification and supporting services in Asia Pacific."

TÜV NORD

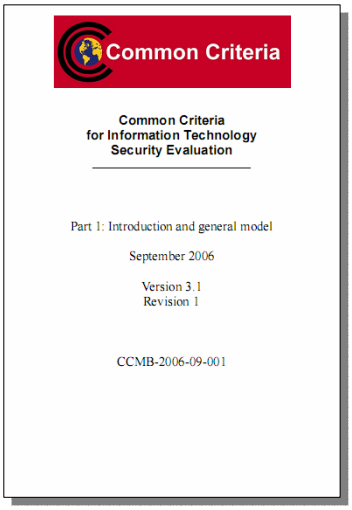
Asia Pacific – IT business dept.

TÜV NORD IT security services



TÜV NORD Asia Pacific

ISO/IEC 15408



ISO/IEC 15408:1999-12-01
Information technology – Security techniques – Evaluation criteria for IT security –

Common Criteria for IT Security Evaluation
- Part 1 – Introduction and general model
- Part 2 – Security functional requirements
- Part 3 – Security assurance requirements
- Common Evaluation Methodology, **CEM** (up to EAL 4)
- **Protection Profiles, PPs**

TÜV NORD Asia Pacific

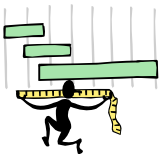
CC Document overview

- Common Criteria (CC)
  - Part 1
    - Context and general model of a CC evaluation
    - Structure, scope and evaluation of Protection Profiles and Security Targets
  - Part 2
    - Partly hierarchical functional classification system
    - Catalogue of security functional requirements
  - Part 3
    - Hierarchical classification system for security assurance requirements
    - Catalogue of security assurance requirements
    - Definition of Evaluation Assurance Levels (EAL)

TÜV NORD Asia Pacific

Types of evaluation

Concurrent



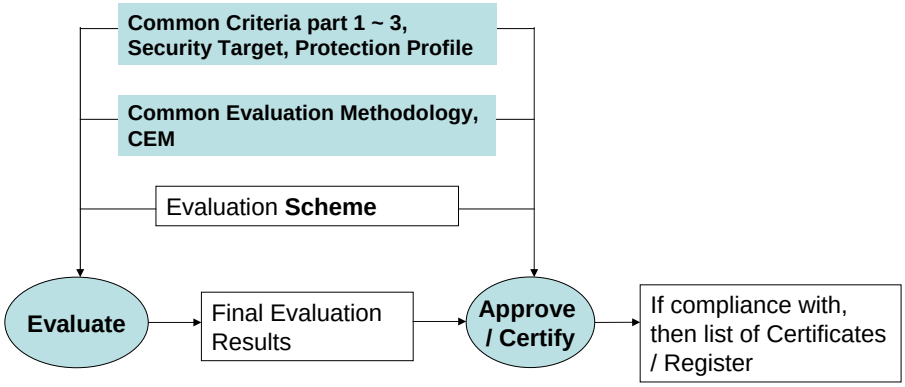
Consecutive

Re-Evaluation

TÜV NORD Asia Pacific

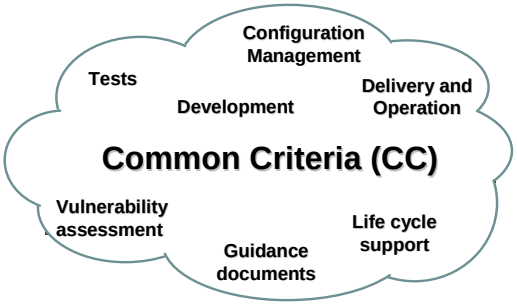
Evaluation context

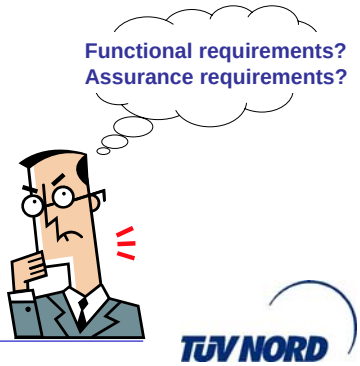
Ref: CC part 1, figure 3.1



TÜV NORD Asia Pacific

What is Common Criteria





TÜV NORD Asia Pacific

CC part 2 – Functional classes

Class	Name
FAU	security audit
FCO	communication
FCS	cryptographic support
FDP	user data protection
FIA	identification & authentication
FMT	security management
FPR	privacy
FPT	protection of the TOE security functions
FRU	resources utilization
FTA	TOE access
FTP	trusted path/channels

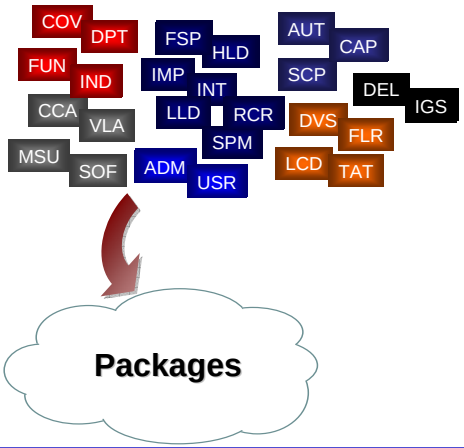
TÜV NORD Asia Pacific

CC part 3 – Assurance classes

Class	Name
ACM	Configuration management
ADO	Delivery and operation
ADV	Development
AGD	Guidance documents
ALC	Life cycle support
ATE	Test
AVA	Vulnerability assessment
APE	PP evaluation
ASE	ST evaluation
AMA	Assurance maintenance

TÜV NORD Asia Pacific

“Pre-defined” security requirements



- The **“package”** concept make CC…
  - Easier to understand
  - Easier to be use and customize
  - Flexible to adapt
  - Flexible to implement

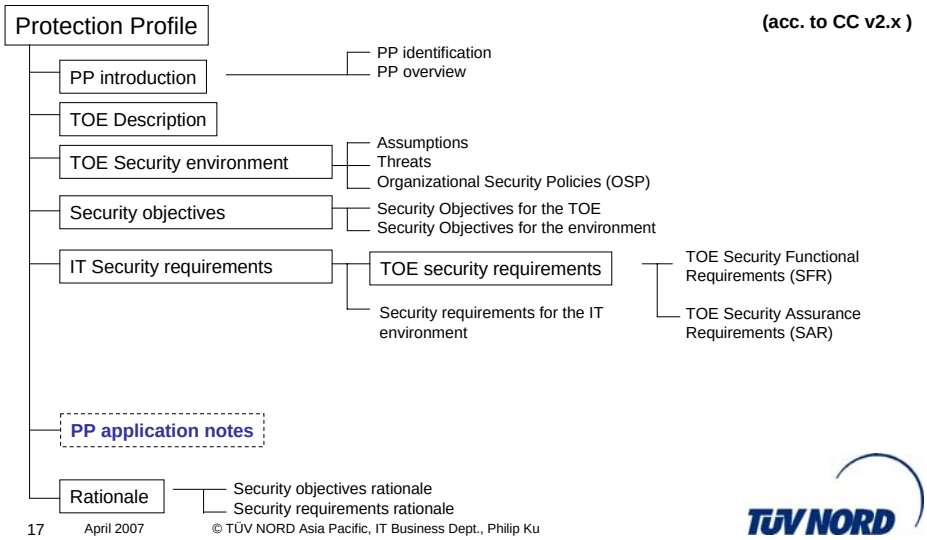
TÜV NORD Asia Pacific

Evaluation packages and EAL levels

Ref: Common Criteria v 2.x

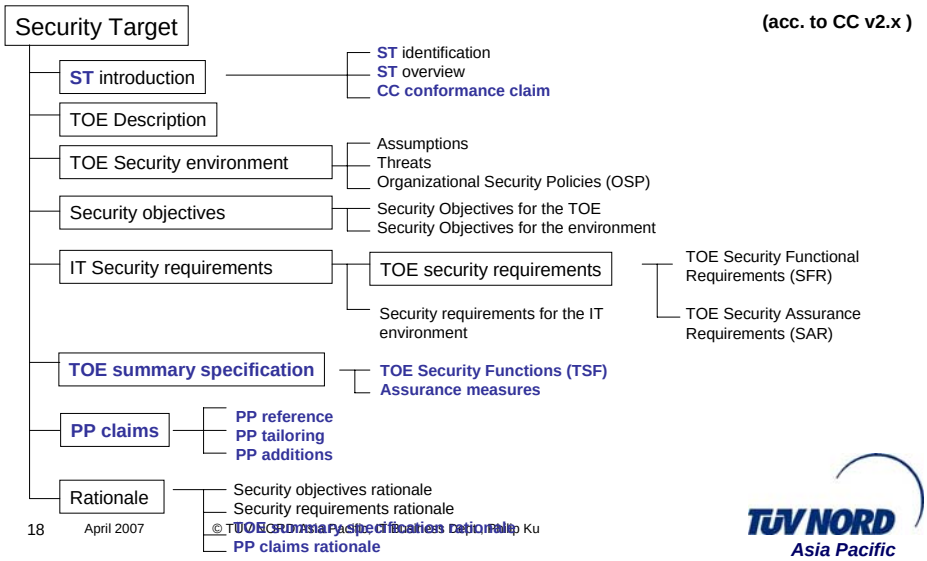
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	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

Protection Profile



TÜV NORD Asia Pacific

Security Target



TÜV NORD Asia Pacific

Protection Profiles (PP) (I)

Sequence number	Title
PP-0015	**Low Assurance Protection Profile for an Office Based Photocopier Device, Version 1.3**
PP-0014	**Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use, Version 1.2**
PP-0013	Low Assurance Protection Profile for a VPN Gateway, Version 1.4
PP-0012	Low Assurance Protection Profile for a Voice over IP Infrastructure, Version 1.1
PP-0010	Protection Profile Waste Bin Identification System WBIS-PP
PP-0008	Schutzprofil - Benutzerbestimmbare Informationsflusskontrolle (MU) Protection Profile - Discretionary Information Flow Control (MU)
PP-0007	Schutzprofil - Benutzerbestimmbare Informationsflusskontrolle (SU) Protection Profile - Discretionary Information Flow Control (SU)
PP-0006	Protection Profile - Secure Signature-Creation Device Type 3, Version 1.05
PP-0005	Protection Profile - Secure Signature-Creation Device Type 2, Version 1.04
PP-0004	Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05
PP-0003	**Schutzprofil Smart Card Security User Group - Smart Card Protection Profile Version 3.0**
PP-0002	**Schutzprofil Smartcard IC Platform Protection Profile, 1.0**
PP-0001	Schutzprofil SIZ-PP 2.0

TÜV NORD Asia Pacific

Protection Profiles (PP) (II)

Sequence number	Title
PP-0034	**Mobile Synchronisation Services (MSS PP) Version 1.1**
PP-0031	Schutzprofil Digitales Wahlstift-System, Version 1.0.1
PP-0026	Machine Readable Travel Document with "ICAO Application" Extended Access Control, Version 1.1
PP-0025	Schutzprofil für USB-Datenträger, Version 1.4
PP-0024	Protection Profile Version 1.17 for a Identity Manager
PP-0023	**Schutzprofil Software zur Verarbeitung von personenbezogenen Bilddaten, Version 2.0**
PP-0021	**BAROC Smart Card Protection Profile Version 1.2**
PP-0020 PP-0020-V2	Protection Profile — electronic Health Card (eHC)– elektronische Gesundheitskarte (eGK)
PP-0019	Secure Module Card (SMC) – Sicherheitsmodul-Karte
PP-0018	Protection Profile — Professional Health Card (PP-HPC)
PP-0017	Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control Version 1.0
PP-0016	**Protection Profile - Biometric Verification Mechanisms Version 1.04**

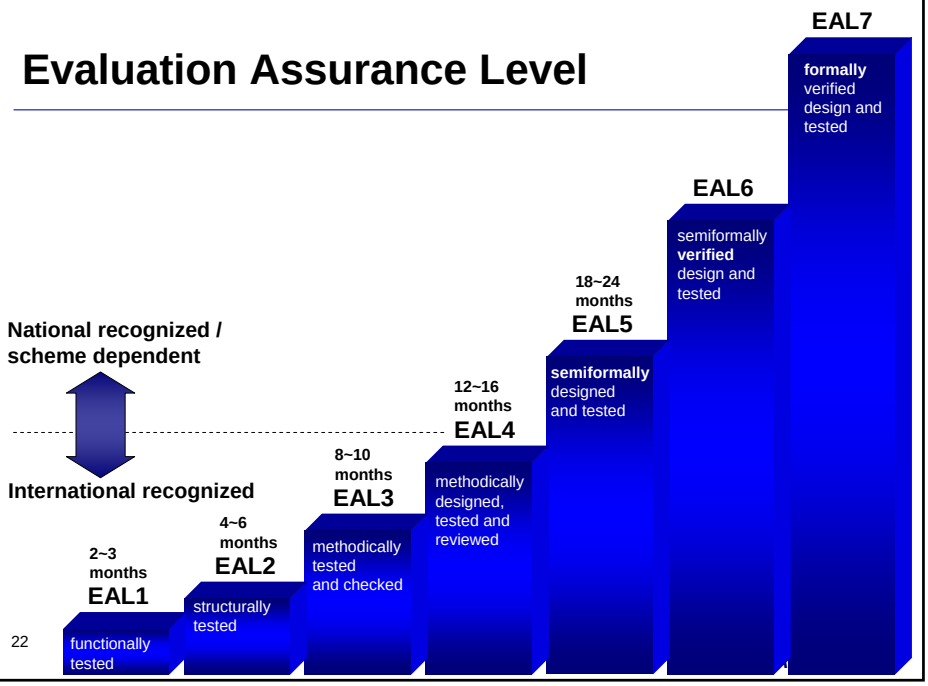
TÜV NORD Asia Pacific

Protection Profiles (PP) (III)

- U.S. Government **Firewall** Protection Profile For Medium Robustness Environments, 2003, EAL4+
- U.S. Government **Traffic-Filter Firewall** Protection Profile For Medium Robustness Environments, 2006, EAL4+
- Low assurance Protection Profile for a **Software based Personal Firewall** for home Internet use Version 1.2, 2005, EAL1
- U.S. Government Virtual Private Network (**VPN**) Boundary Gateway for Medium Robustness Environments, 2006, EAL4+
- U.S. Government Wireless Local Area Network (**WLAN**) Access **System** Protection Profile for Basic Robustness Environments, 2006, EAL2+
- U.S. Government Wireless Local Area Network (**WLAN**) **Client** Protection Profile For Basic Robustness Environments, 2006, EAL2+
- …

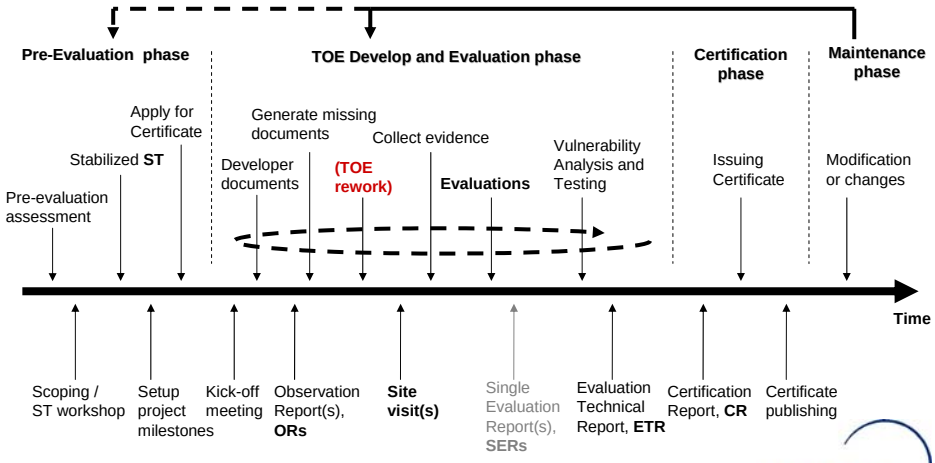
TÜV NORD Asia Pacific

Evaluation Assurance Level



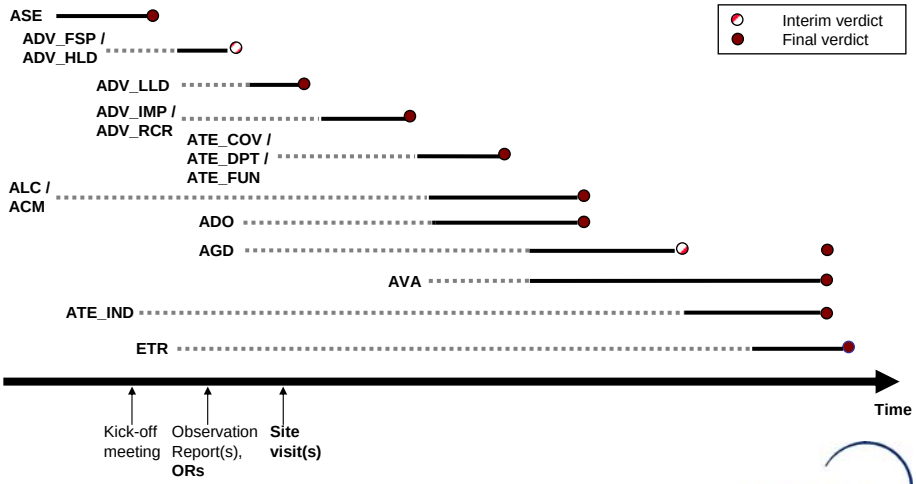
Common Criteria for IT security evaluation –

Project phases and milestones (up to EAL4)



TÜV NORD Asia Pacific

Generic evaluation work program



TÜV NORD Asia Pacific

Generic developer's work program

Pre-Evaluation phase

- Apply for Evaluation
- Confidentiality concerns
- Resources allocation
- Competent to CC
- Request for consultancy
- EAL allocation
- Drafting ST
- Stabilizing ST
- Secure TOE environment
- Secure communication
- Apply for Certification

TOE Develop and Evaluation phase

- Kick-off meeting
- Approved project and delivery schedule
- Preparation on developer's documentations
- Response to the Evaluation and Certification process
- Response to Evaluator and Certifier's comments
- TOE develop life cycle performance
- Vulnerability analysis
- Developer's test
- Evidence references
- TOE-rework (if necessary)
- Preparation for site visit(s)

Certification phase

- Response to CR
- Finances to CB
- Certificate
- Maintain certificate

Maintenance phase

Time

In general aspects

- Organizational supports
- Management system support
- Competent to project management
- Product life cycle management

TÜV NORD Asia Pacific

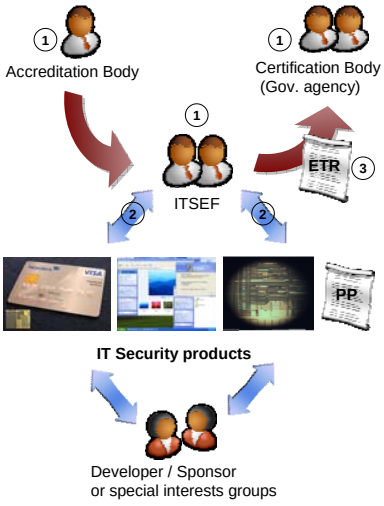
Categories of evaluated products

Ref: www.commoncriteriaportal.org

1. Access Control Devices and Systems
   - Citrix, Safeguard…
2. Boundary Protection Devices/Systems
   - Netscreen, Microsoft –ISA 2000, Lucent, 3Com, Symantec, CheckPoint, Cisco…
3. Databases
   - IBM, Sybase, Oracle,
4. Data Protection
   - Atmel, Utimaco…
5. Detection Devices and Systems
   - Symantec…
6. ICs, Smart Cards and Smart Card related Devices and Systems
   - Samsung, Philips, Infineon, Mondex, Gemplus, Sony, Hitachi, Atmel, IBM…
7. Key Management Systems
   - Entrust, RSA…
8. Network and Network related Devices and Systems
   - Juniper, Foundry, Cisco, Symantec, HP, Richo…
9. Operating systems
   - HP, Oracle, Cray, SuSE, Silicon Graphic, RedHat, Nokia, Microsoft, Sun, IBM…
10. Other Devices and Systems
    - NEC, Sharp, Xerox, Toshiba, Canon,Konica, Trend Micro…
11. Products for Digital Signatures
    - Dictao, Cybertrust…

TÜV NORD Asia Pacific

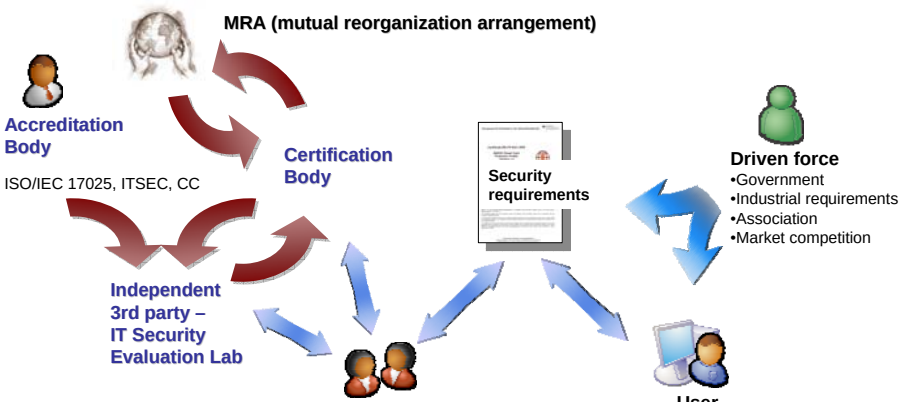
CC evaluation scheme – International



1. Accreditation Body (**AB**), Certification Body (**CB**) and Labs (**ITSEF**, IT Security Evaluation Facility).
2. Labs evaluate IT Security Products (SW/HW/FW) or Requirements (**PP**, Protection Profile)
3. CB perform the certification process (**ETR**, Evaluation Technical Report prepared by ITSEF) and (**CR**, Certification Report prepared by CB)
4. CB issues **CC Certificate** to evaluated product
5. MRA Nations recognize product certificates up to EAL4

TÜV NORD Asia Pacific

Common Criteria International scheme



TÜV NORD Asia Pacific

Common Criteria Recognition Arrangement (CCRA)

Ref: www.commoncriteriaportal.org

2006.09 update

- Participants are only governmental bodies
- Actually 10 CAPs + 14 CCPs
- Bilateral acceptance of certificates up to the level EAL4

CCRA participants
10 CAPs, Certificate-Authorizing participants
14 CCPs, Certificate-Consuming participants

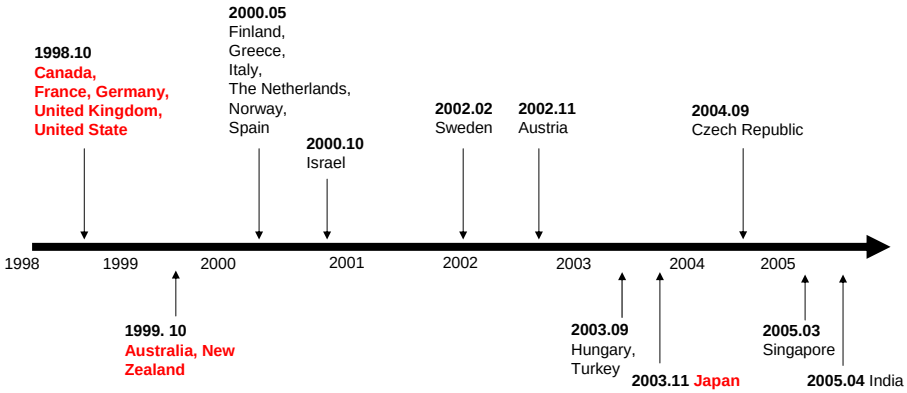
TÜV NORD Asia Pacific

Common Criteria:

Arrangement of mutual recognition participants (up to EAL4)

Ref: www.commoncriteriaportal.org

2006.09 update



Notes: **CAP** perform re-shadow certificate process for each 5 years.

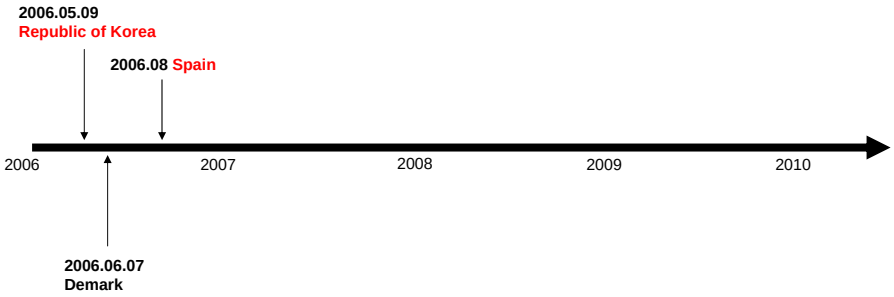
TÜV NORD Asia Pacific

Common Criteria:

Arrangement of mutual recognition participants (up to EAL4)

Ref: www.commoncriteriaportal.org

2006.09 update



Notes: **CAP** perform re-shadow certificate process for each 5 years.

TÜV NORD Asia Pacific

Common Criteria for IT security Evaluation / Certification scheme – Germany

Common Criteria Recognition Arrangement, CCRA
– CCP / **CAP** participants

Accreditation Body
ISO/IEC 17025, ITSEC, CC

Certification Body

ITSEF

Security requirements

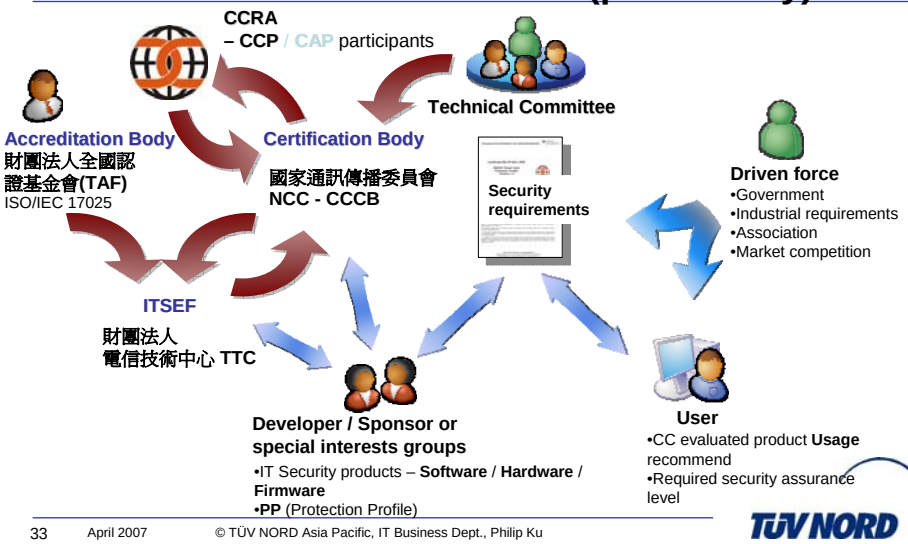
Driven force
- Government
- Industrial requirements
- Association
- Market competition

Developer / Sponsor or special interests groups
- IT Security products – **Software** / **Hardware** / **Firmware**
- **PP** (Protection Profile)

User
- CC evaluated product **Usage** recommend
- Required security assurance level

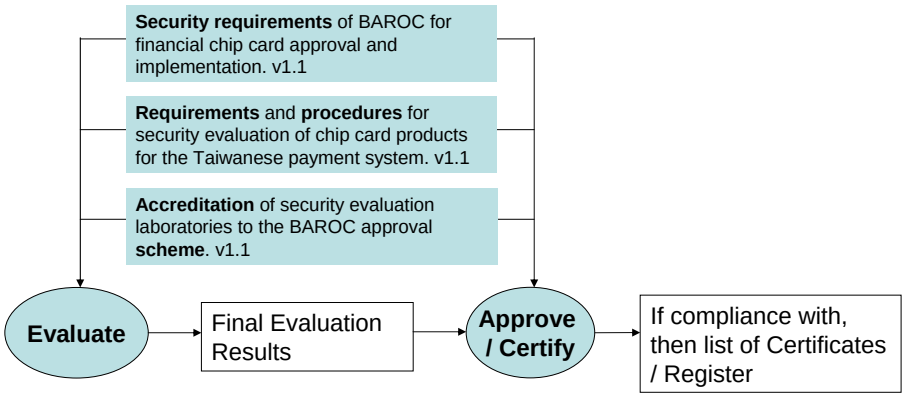
TÜV NORD Asia Pacific

Common Criteria for IT security Evaluation / Certification scheme – Taiwan (preliminary)



TÜV NORD Asia Pacific

Banking criteria evaluation context



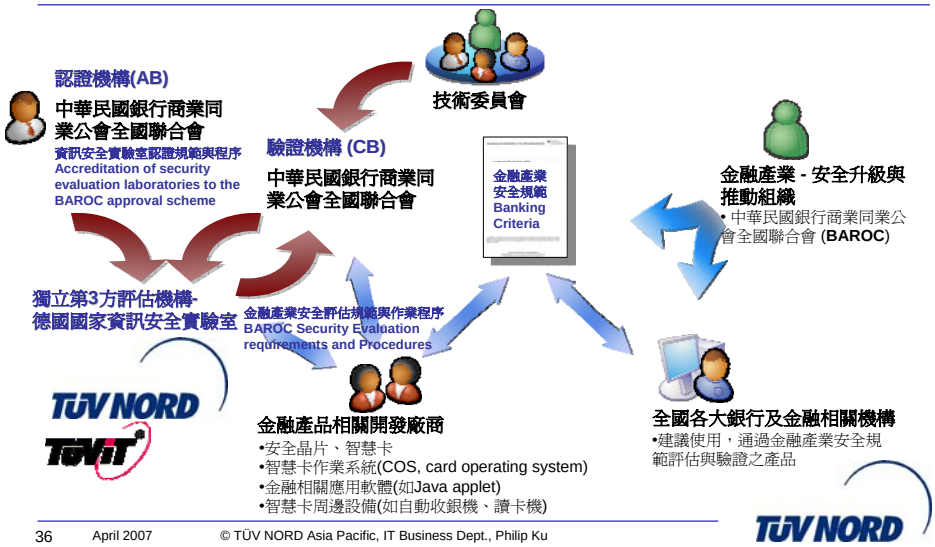
TÜV NORD Asia Pacific

Evaluation packages and EAL levels

Ref: Common Criteria v 2.x

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

Banking criteria evaluation scheme – Taiwan



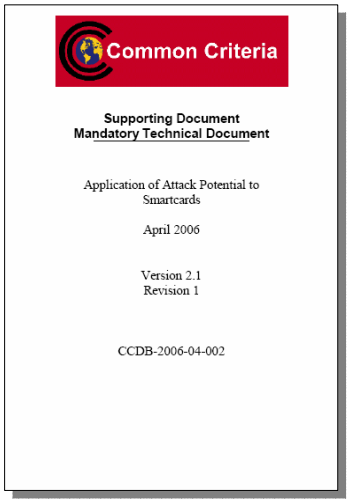
TÜV NORD Asia Pacific

Banking criteria evaluation activities

- Evaluate on evidences – documentations
- Code review – evaluation on security code
- Penetration test
  - SPA/DPA testing
  - DFA testing
  - Attacks
    - Depends on the countermeasure
- Reporting

TÜV NORD Asia Pacific

Application of Attack Potential to Smartcards


Common Criteria

Supporting Document
Mandatory Technical Document

Application of Attack Potential to Smartcards

April 2006

Version 2.1
Revision 1

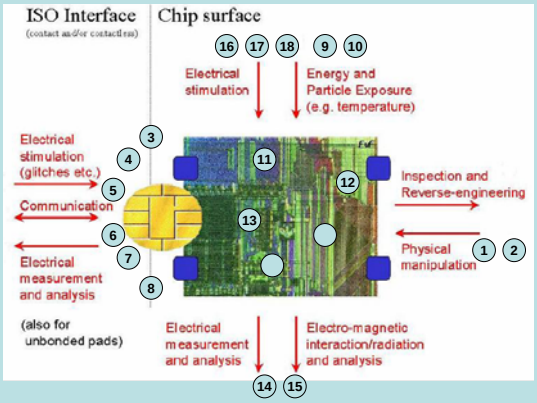
CCDB-2006-04-002

- Physical Attacks
- Overcoming sensors and filters
- Perturbation Attacks
- Retrieving keys with DFA
- SPA/DPA – Non-invasive retrieving of secret data
- Higher Order DPA
- EMA Attacks
- Exploitation of Test features
- Attacks on RNG
- ill-formed Java Card applications
- Software Attacks
- Information gathering
- Editing commands
- Direct protocol attacks
- Man-in-the-middle attacks
- Replay attacks
- Bypass authentication or access control
- Buffer overflow or stack overflow

TÜV NORD Asia Pacific

Example of smartcard attack concepts

Smartcard



Physical attacks
1. Physical probing of the IC
2. Physical alteration of the IC

Logical attacks
3. Insertion of Faults
4. Forced Reset
5. Invalid Input
6. Replay Attack
7. Brute Force Data Space Search
8. Unauthorized Program Loading

Control of access
9. Invalid access
10. Fraud on first use

Unanticipated Interactions
11. Use of Un-allowed application functions
12. Use of Un-allowed Life Cycle Functions

Cryptographic function
13. Cryptographic attacks

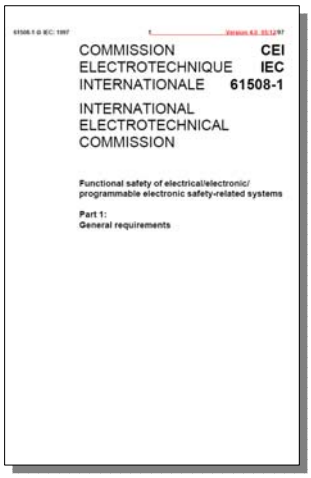
Monitoring information
14. Information leakage
15. Linkage of Multiple Observations

Others
16. Environmental Stress
17. Linked Attacks
18. Cloning

Operational environment
19. Chip Modification and Reuse
20. Abuse by Privileged Users

Safety in software !?

IEC 61508


COMMISSION ELECTROTECHNIQUE INTERNATIONALE
CEI IEC 61508-1
INTERNATIONAL ELECTROTECHNICAL COMMISSION
Functional safety of electrical/electronic/ programmable electronic safety-related systems
Part 1: General requirements

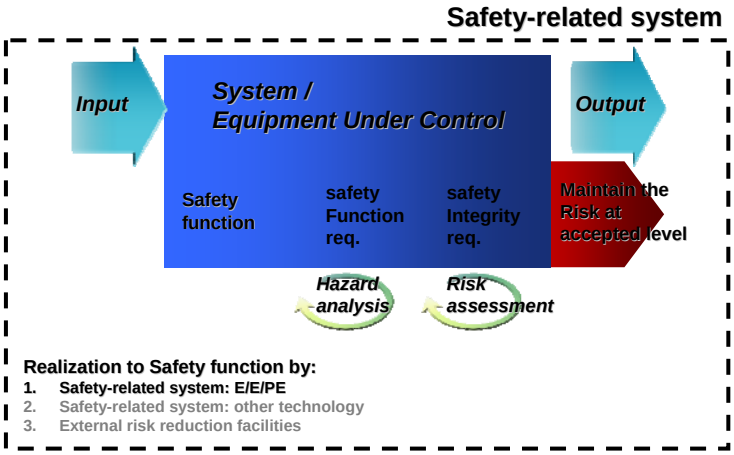
IEC: International Electrotechnical Commission

Functional safety of **E**lectrical / **E**lectronic/ **P**rogrammable **E**lectronic safety-related systems

Part 1: General requirements;
Part 2: Requirements of electrical / electronic / programmable electric safety-related system;
Part 3: Software requirements;
Part 4: Definitions and abbreviations;
Part 5: Examples of methods for the determination of safety integrity levels;
Part 6: Guidelines on the application of part 2 and 3;
Part 7: overview of techniques and measures.

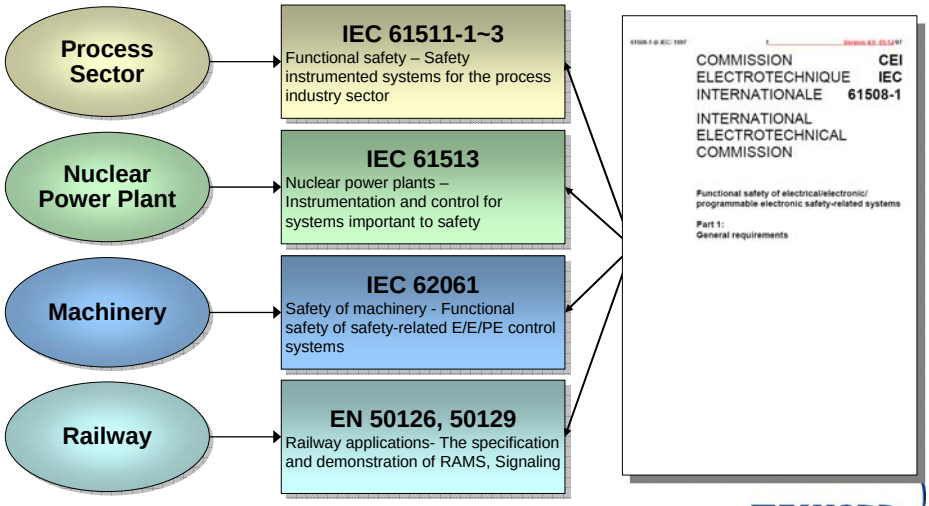
TÜV NORD Asia Pacific

Safety-related system – IEC 61508



TÜV NORD Asia Pacific

Standards based on IEC 61508



TÜV NORD Asia Pacific

Thanks for your participation.

We are delighted to discuss any question with you.

TÜV NORD Asia Pacific


TÜV NORD
Asia Pacific – IT business dept.