



**ISO 15408**

**The international  
IT security standard**

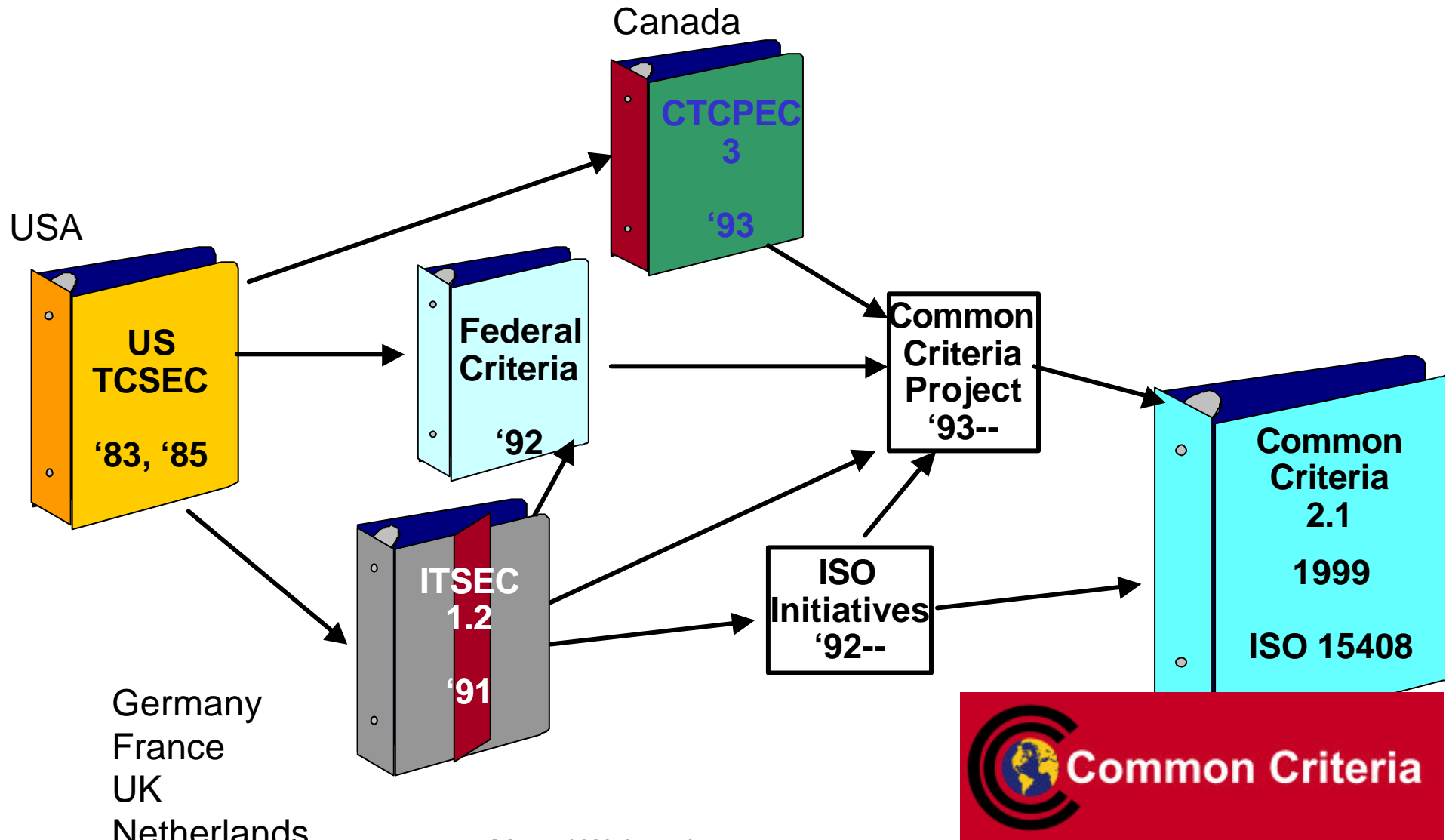


Marcel Weinand  
049-228/9582-152

[MarcelWeinand@bsi.bund.de](mailto:MarcelWeinand@bsi.bund.de)

Marcel Weinand  
Hannover Messe 2005 Interkama

# History of IT-Security Criteria

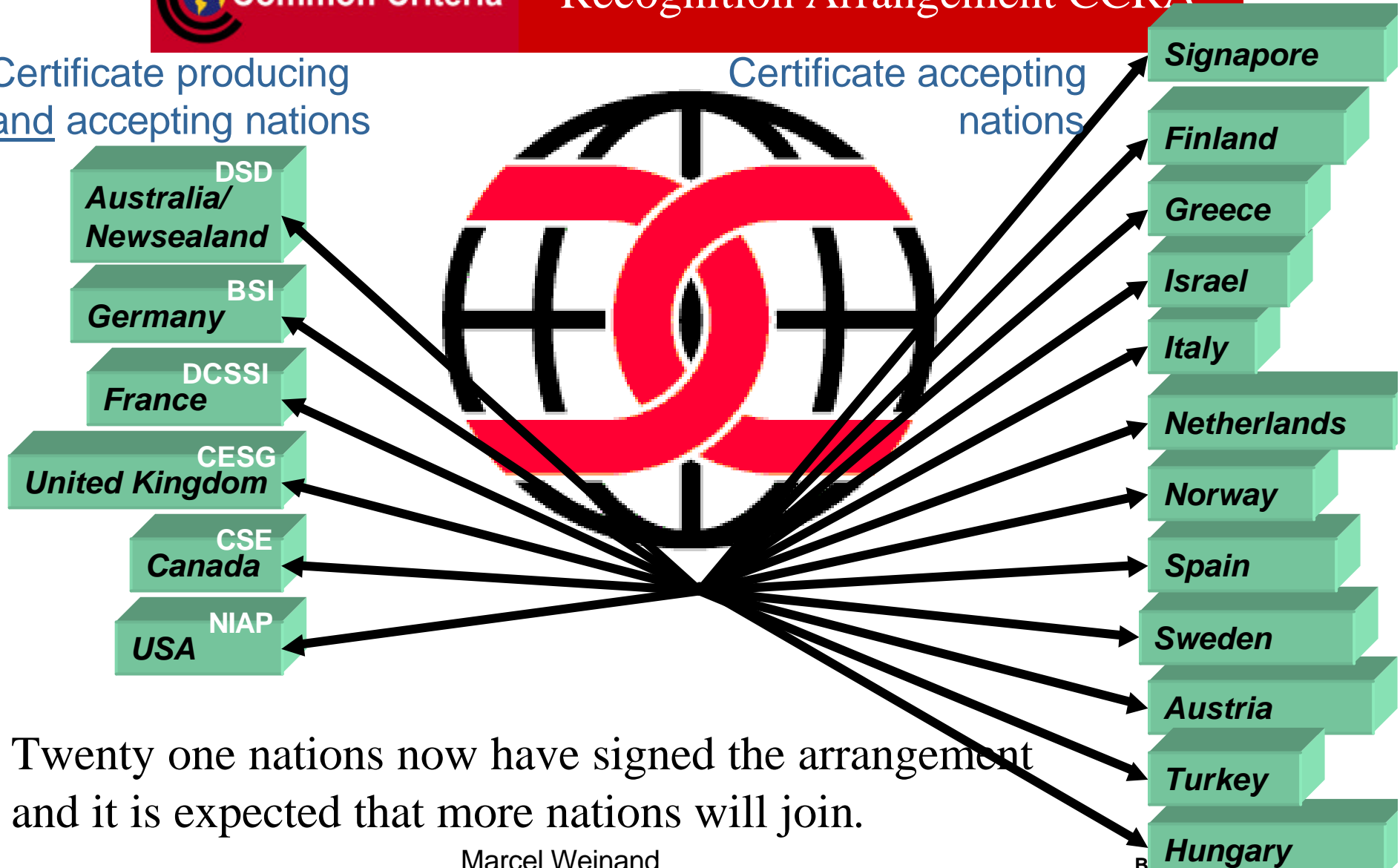


# The CC Community

## Common Criteria - Recognition Arrangement CCRA

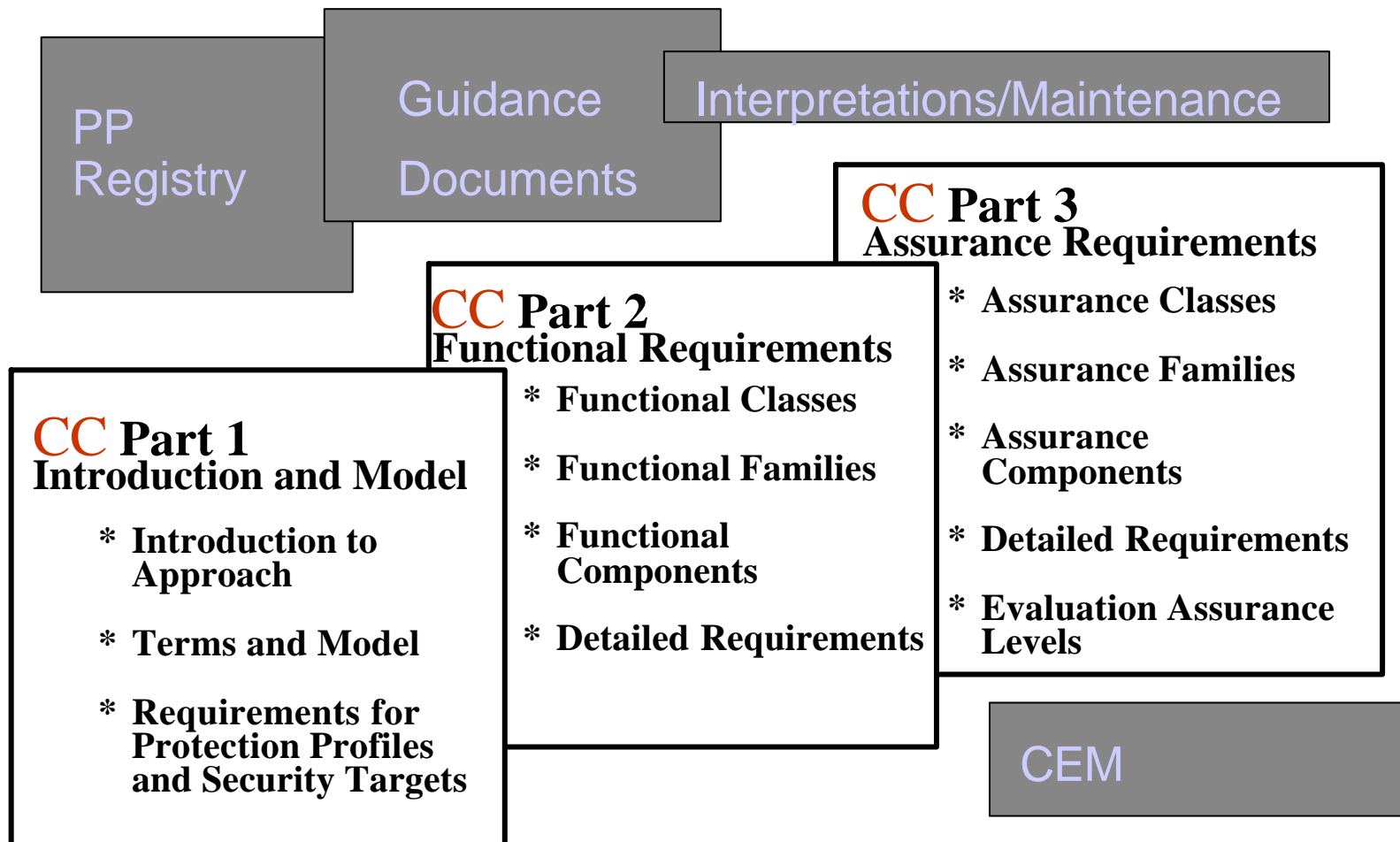
Certificate producing and accepting nations

Certificate accepting nations



Twenty one nations now have signed the arrangement and it is expected that more nations will join.

# CC Documentation



## Example: Evaluation of Open Source Operating Systems

- Successive Evaluation of Linux Distributions like SUSE Linux Enterprise Server (SLES) and RedHat Enterprise Linux AS/WS (RHEL).  
E.g. SLES has been evaluated/re-evaluated at EAL2/3 and EAL4 on different hardware platforms.
- Product is meant to be used in a server environment.
- Evaluated Security Functions were:
  - Identification and Authentication
  - Discretionary Access Control
  - Audit
  - Object Reuse
  - Communication Security
  - Self-Protection

## Example: Benefits/Drawbacks of Certification

- Development process and product itself has been improved.  
E.g. Audit subsystem added to be compliant to internationally recognised Protection Profiles. Test Suite augmented with Common Criteria related testing.
- New markets could be opened (e.g. U.S. government market requires usage of certified products in certain areas).
- Product became more compatible with other already certified operating systems like MS Windows and other Unix derivatives.

# Building „Normative Documents“ by **CC** Constructs

Package

**Protection Profile PP**



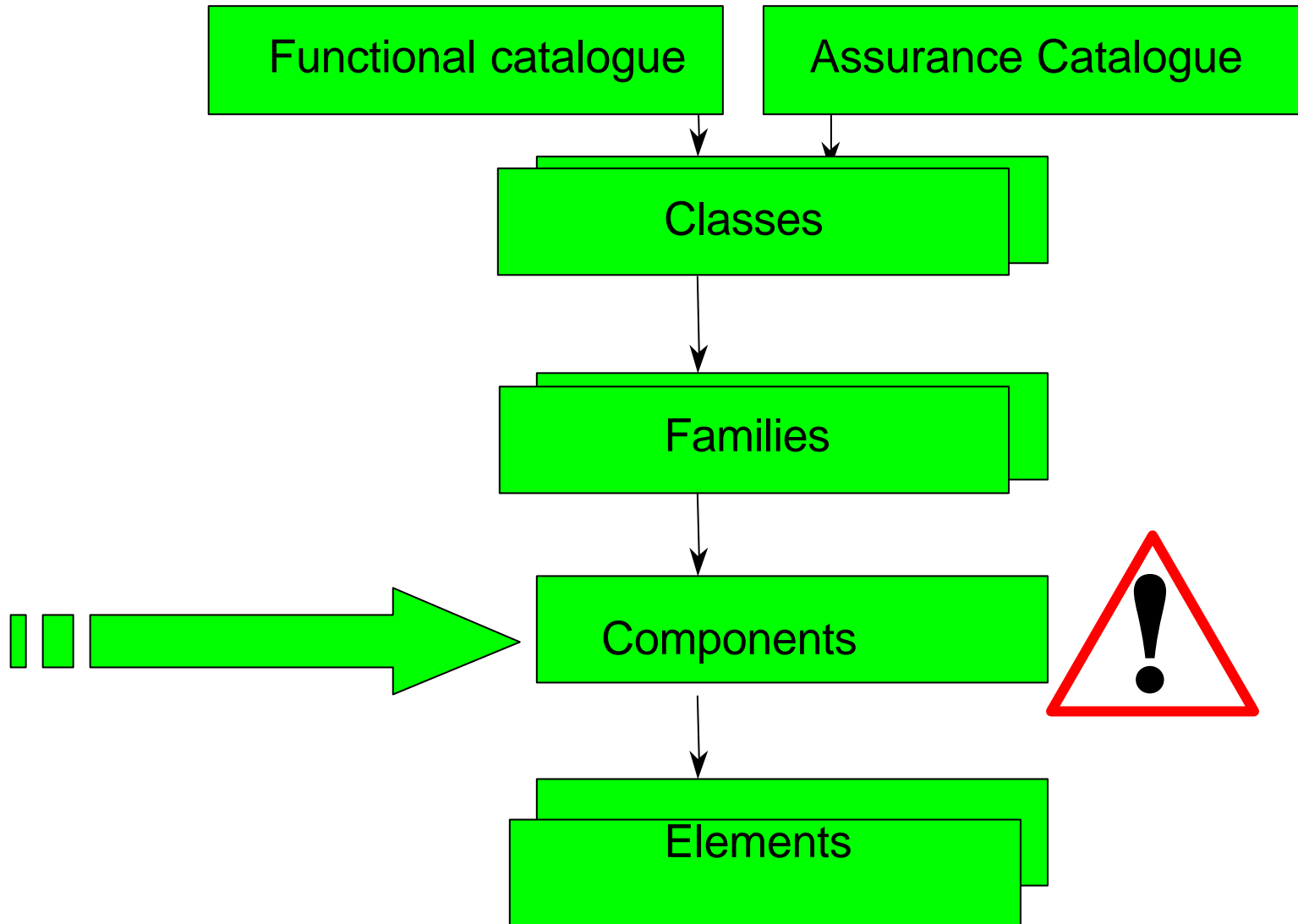
Security Target ST

# Some Characteristics of Protection Profiles

presentation of an **IT security problem** and a general  
solution in conformity with the CC (security concept)  
**independent** of an implementation  
represents a special **category** of TOEs  
consists of functional **and** assurance requirements  
basis for the development of Security Target (optional)

# Some Advantages of Protection Profiles

- Products, developed/chosen based on one common PP guarantee a comparable or common security concept.
- registration being national and by ISO
- International acceptance
- PP is a customer requirement specifications document
- PP is the normative document from customer view

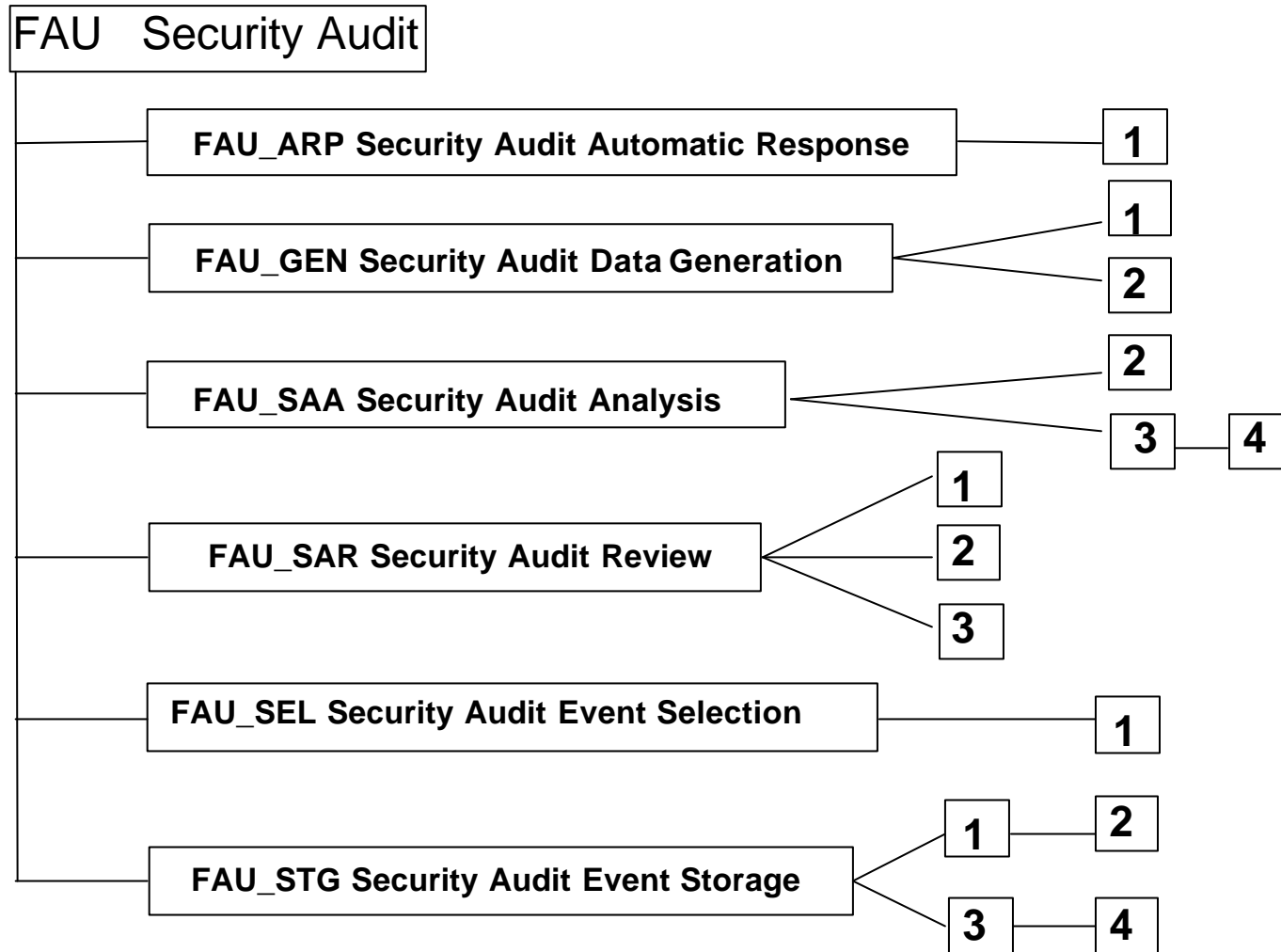


**Components - the construction kit of PP/ST**

Marcel Weinand

Hannover Messe 2005 Interkama

# Example: Class FAU Overview



# Dependencies between components

- Some requirement components are not self-sufficient
- Some functional requirement components have functional and/or assurance dependency
- The **CC** provide a **complete** list of dependencies to other **CC** functional or assurance components.
- All identified dependencies of a selected component have to be satisfied

## Definition of the term „dependency“

A component K1 is dependent on component K2, if K1 requires the functionality of K2 for the complete and correct realisation of its obligations or if K1 can fulfil its obligations only in co-operation with K2.

# What is Confidence?

Common Criteria (CC) Definition:

*Grounds for confidence that an IT product or system meets its security objectives.*

– **does not add functionality to the TOE**

*TOE: Target of Evaluation*

# Common Methodology for Information Technology Security Evaluation (CEM)

## Scope of the CEM

- ➔ Development of a common concept and harmonised methodology for performing evaluations
- ➔ consistent application of the CC for evaluation processes to get comparable evaluation results
- ➔ Basis for assurance of mutual recognition (Harmonisation in implementing the CC)



**Addresses:** Evaluators  
but also sponsors of evaluation and  
certification body representative

## Examples of Certified Products (I)

<b>Processor Resource/ System Manager (PR/SM) for the IBM eServer zSeries 900</b>	<b>Operating System</b>	<b>IBM Corporation</b>	<b>EAL5</b>
<b>Processor Resource/ System Manager (PR/SM) for the IBM eServer zSeries 900</b>	<b>Operating System</b>	<b>IBM Corporation</b>	<b>EAL4</b>
<b>AIX 5L for POWER Version 5.2, Programm Number 5765-E62</b>	<b>UNIX Operating System</b>	<b>IBM Informations-systeme Deutschland GmbH</b>	<b>CC EAL4+</b>
<b>Reliant UNIX 5.43 with Audit 2.0</b>	<b>UNIX Operating System</b>	<b>Siemens-Nixdorf Informations-systeme AG</b>	<b>ITSEC E3</b>

## Examples of Certified Products (II)

<b>B1/EST-X Version 2.0.1 with AIX, Version 4.3.1</b>	<b>Operating System</b>	<b>Bull S.A. und IBM Informations-systeme Deutschland GmbH</b>	<b>CC EAL4</b>
<b>DATA-Defender 1.0</b>	<b>Data protection device</b>	<b>Fachhochschule Aachen</b>	<b>CC EAL1</b>
<b>GeNUGate Version 4.0</b>	<b>Firewall</b>	<b>GeNUA Gesellschaft für Netzwerk- und UNIX-Administration mbH</b>	<b>ITSEC E3</b>
<b>Transport/S-2.0</b>	<b>Security Product for the protection of application to Client-Server</b>	<b>FUN Kommunikations- systeme GmbH</b>	<b>ITSEC E4</b>

## Examples of Certified Products (III)

<b>Setcos 3.1 V3.1.1/ V3.1.1.1</b>	<b>Smartcard Operating System</b>	<b>Setec Oy</b>	<b>ITSEC E4</b>
<b>Hitachi AE45C (HD65145C) Smartcard Integrated Circuit Version 01</b>	<b>Smartcard Controller</b>	<b>Hitachi Ltd.</b>	<b>CC EAL4+</b>
<b>Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a23</b>	<b>Smartcard Controller</b>	<b>Infineon Technologies AG</b>	<b>CC EAL5+</b>
<b>GemXplore'Xpresso V3 – Java Card Platform Embedded Software V3 (Core)</b>	<b>Smartcard Operating System for GSM Applications</b>	<b>Gemplus S.A.</b>	<b>CC EAL5+</b>

## Examples of Certified Products (IV)

<b>KITAS 2171</b>	<b>Motion Sensor (compliant with EWG Directive 3821/85 and EU Directive 2135/98)</b>	<b>Mannesmann VDO</b>	<b>ITSEC E3</b>
<b>Philips Smart Card Controller P8WE6004V0D</b>	<b>Smart Card Controller</b>	<b>Philips Semicon- ductors Hamburg</b>	<b>CC EAL5+</b>
<b>GemXplore'Xpresso V3 - Java Card Platform Embedded Software V3 (Core)</b>	<b>Java Card Platform</b>	<b>Gemplus S.A.</b>	<b>CC EAL5+</b>

## Examples of Certified Products (V)



### UK

- **Sidewinder Firewall Version 5.2.1 (EAL2)**
- **Check Point VPN-1/FireWall-1<sup>®</sup> NG (EAL4)**
- **Symantec Enterprise Firewall v7.0 (EAL4)**
- **Entrust/RA from Entrust/PKI 5.1 (EAL3)**



## Examples of Certified Products (VI)



### USA

- **Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886 Hotfix (EAL4+)**
- **Owl Computing Technologies Data Diode Version 1 and Owl Computing (EAL2)**
- **Persona 5.0 (EAL3)**



## Examples for Smartcard Components

### France

- STMicroelectronics Micro-Circuit ST19SF02ADxyz (EAL4 +)
- Micro-Circuit ATMEL AT05SC3208R (EAL4+)

### UK

- MULTOS Version 3 Smart Card OS (E6)
- MONDEX Purse Release 2.0 (E6)

# Characteristics of **CC** Part 2/Part 3

- Catalogue of functional/assurance security requirements
- Semiformal language - high precision (consistent and evaluable)
- clear structures with high flexibility by operations
- extensibility with new requirements
- complete list of all dependencies on other requirements
- only Part 2: each particular requirement is supplied by
  - all administration aspects
  - all audit aspects

# **CC and ISO/IEC 15408 related websites**

<http://www.cse-cst.gc.ca/cse/english/cc.html>

<http://www.scssi.gouv.fr>

<http://www.bsi.bund.de/>

<http://www.tno.nl/instit/fel/refs/cc.html>

<http://www.cesg.gov.uk/cchtml>

<http://csrc.nist.gov/cc>

<http://www.radium.ncsc.mil/tpep/>

<http://www.iso.ch>

<http://www.commoncriteriaportal.org>

## Contact



Bundesamt für Sicherheit in der  
Informationstechnik (BSI)  
Referat III 2.3

Marcel Weinand  
Godesberger Allee 185-189  
D-53175 Bonn

Tel: +49 (0)1888-9582-152  
Fax: +49 (0)1888-9582-90152



[Marcel.Weinand@bsi.bund.de](mailto:Marcel.Weinand@bsi.bund.de)  
[www.bsi.bund.de](http://www.bsi.bund.de)