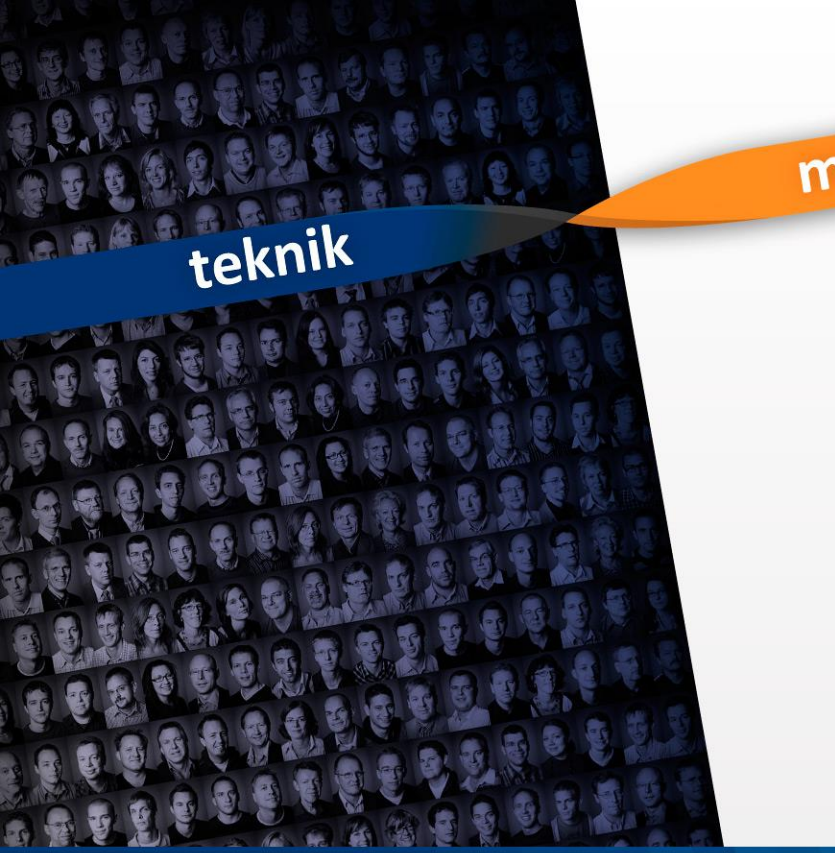
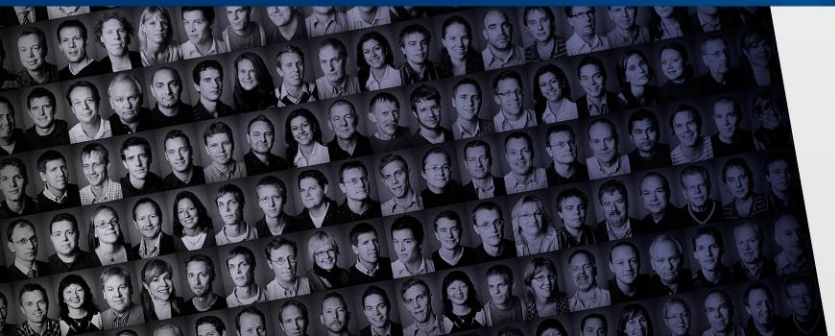


Common Criteria

Introduction

2015-02-23

COMBITECH



Emilie Barse
Magnus Ahlbin

Magnus Ahlbin

Head of EC/ITSEF
Information and Security

Combitech AB
SE-351 80 Växjö • Sweden
magnus.ahlbin@combitech.se •
www.combitech.se •
www.itsef.se

Emilie Barse

Consultant
Information and Security

Combitech AB
Lindholmspiren 3A • Göteborg • Sweden
emilie.barse@combitech.se •
www.combitech.se

Agenda

- Security reviews
- Common Criteria background
- How to do a Common Criteria evaluation?
- Common Criteria, the Standard
- Common Criteria Requirements

SECURITY REVIEWS

Information Security in IT products

A common issue for users of IT products is how they will know that the IT product is secure and suitable for the intended environment!

It is an issue that is anything but trivial to solve!

- Information security is difficult to measure, to set requirements, grade and describe

Common Criteria is the leading standard for evaluating IT security products. The result is a certificate for the product.

Security reviews in general

Purpose

- Independently verify and validate IT-security

Goal

- To give trust that the product is secure to use in its intendent environment

How?

- Threat-/Risk analysis
- Architectural analysis
- Static analysis
  - Code reviews
- Dynamic analysis
  - Test in operational environment
- Penetration tests
- Fuzzing
- Analysis of development environments

COMMON CRITERIA EVALUATED PRODUCTS

Product examples …

- Operating systems
  - MS Windows Server 2008 R2, MS Windows 7, Red Hat Enterprise Linux Version 5.6, Apple Mac OS X 10.6, VMware, …
- Firewalls, Routers, Switches
  - Products from Cisco Systems, Juniper Networks, Huawei Technologies, Brocade Communications Systems, …
- ICs, Smart cards
  - Components from Oberthur Technologies , NXP Semiconductors , Samsung Electronics, Infineon Technologies, Gemalto,…
- Databases
  - Databases from Microsoft, Oracle, IBM, EMC, …
- USB-devices, multifunction printers, biometric systems, …

Common Criteria

… IS …

- mainly useful for products and non-complex systems with fixed interfaces to the environment
- not useful for complex systems
  - Evaluation is based on the requirements posed by security-critical functions and all external interfaces
  - Changes or updates to the configuration, components and environment influences the evaluation
- applicable to both hardware, firmware and software

WHO WANTS COMMON CRITERIA CERTIFIED PRODUCTS?

Who wants Common Criteria certified products?

- Governments
  - Requirement for US governments
    - National Security Directive 42, CNSS Policy 11 and CNSS Directive 502
  - Will be recommended in Sweden by MSB for specific categories of products (www.informationssakerhet.se)
- Vendors
  - VISA, Mastercard
- Military
  - DoD Directives (US) and in Swedish Defense in Sweden
- Organizations
  - Smart Card industries

COMMON CRITERIA BACKGROUND

Common Criteria

What

- Common Criteria (CC) is a standard for evaluation of IT products and to some extent systems
- Evaluation involves to verify and validate a product /a systems IT security functions independently
- Common Criteria comprise of foremost:
  - Protection of information from unauthorized access (secrecy)
  - Protection of information from unauthorized modification (integrity)
  - Disregard of function (accessibility)
  - Traceability (logging)

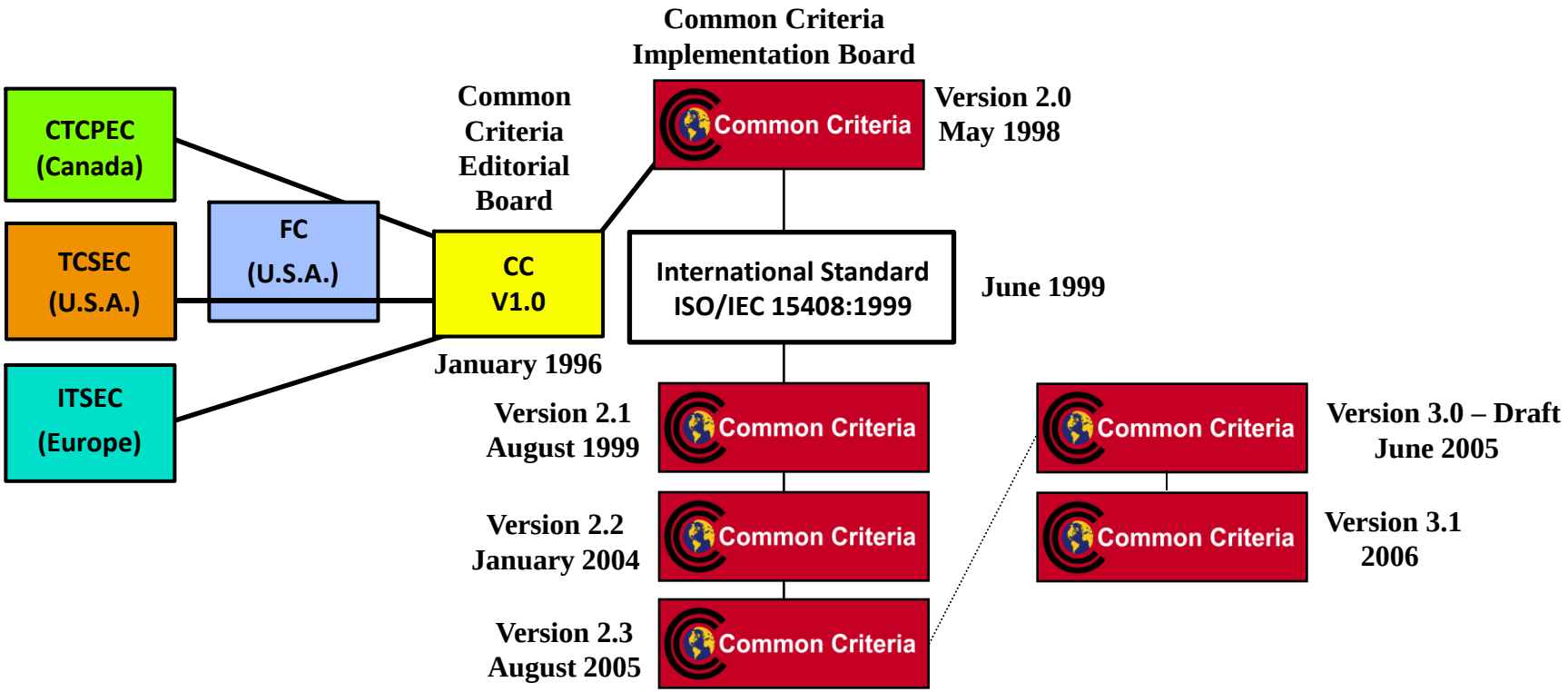
Common Criteria

Why

- The present international standard in terms of verification and evaluation of IT Security
- Provides independent verification of the security features of the product
- Valuable in a marketing context provides a clear mark of quality when it comes to IT security
- Several countries demands in IT security under the Common Criteria, e.g. the U.S.
- The foremost reason to perform an evaluation is to confirm that the claims are meet;
  - From an IT-security perspective, is the product secure?

Common Criteria

History



HOW TO DO A COMMON CRITERA EVALUATION?

Common Criteria – Protection Profile (PP)

Protection Profile (PP)

- An implementation independent description of security objectives and requirements for a category of products
- “Describes what is needed/demanded!”
- Constitutes a security objective
- Usually created by a customer, interest group, authority etc.
- Normally certified

Common Criteria – Protection Profile example

- Protection Profile – Encrypted Storage Device
  - PP USB.pdf
- First PP for Swedish government

Common Criteria – Security Target (ST)

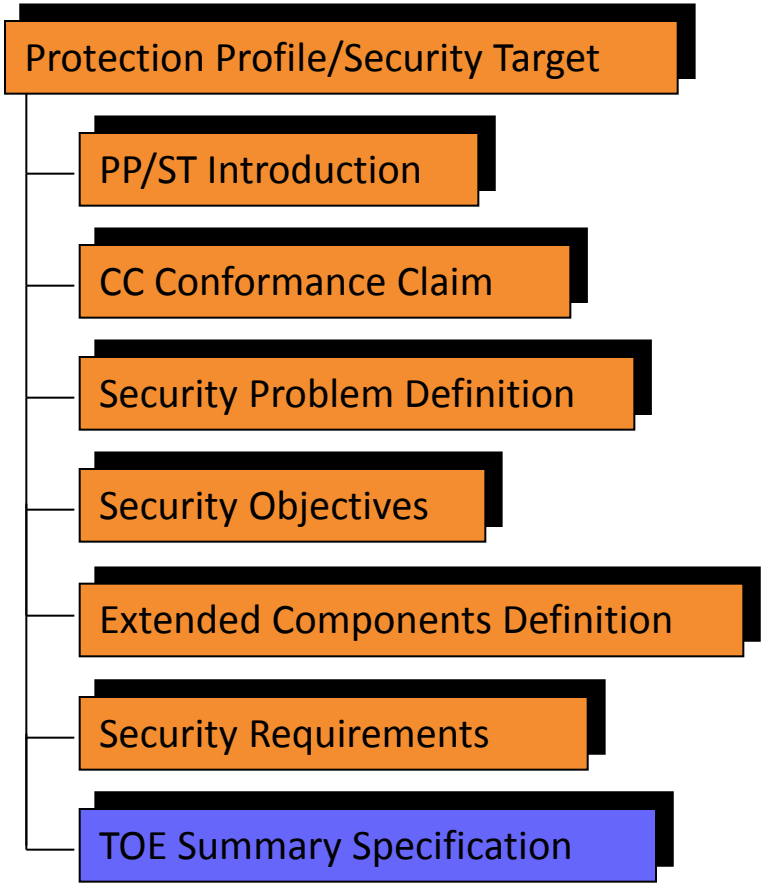
Security Target (ST)

- A implementation dependent description of a product or a system
- Includes the security objectives which are fulfilled by the product/system
- Which threats the product/system meet
- Also includes a description of the roles, policies, assumptions for the environment etc. that are assumed
- “Describes what is offered!”
- Is usually the answer of the developer to one/more PPs
- Must be produced for a evaluation of a product

Common Criteria – The standard

Security Targets and Protection Profiles

- All the headlines that exist for the PP also exists for the ST, though the content differentiates
  - In PP it is described ”to fulfill”
  - In ST it is described ”how to fulfill”
- One more headline is added for the ST
  - TOE Summary Specification

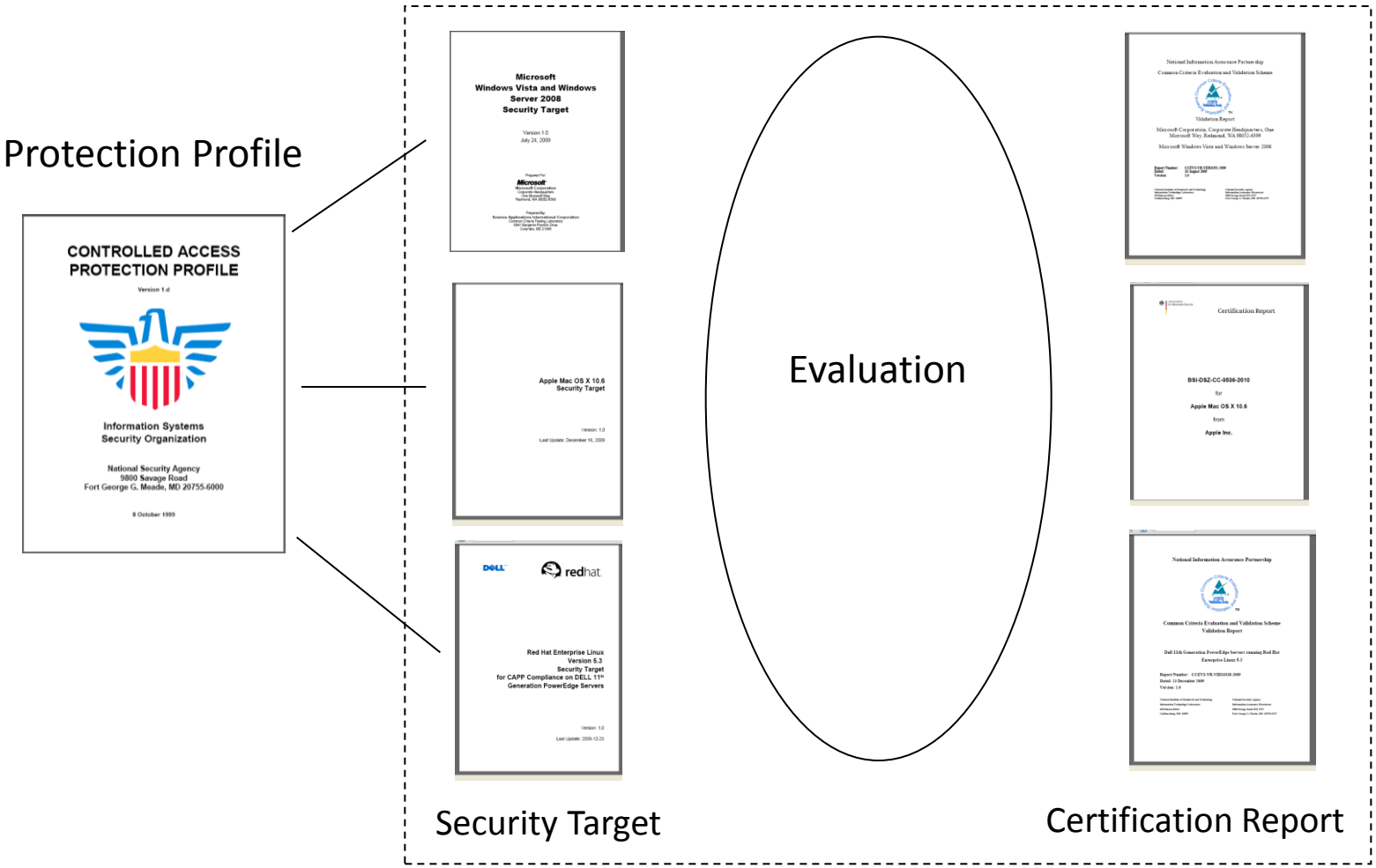


Common Criteria – Target of Evaluation (TOE)

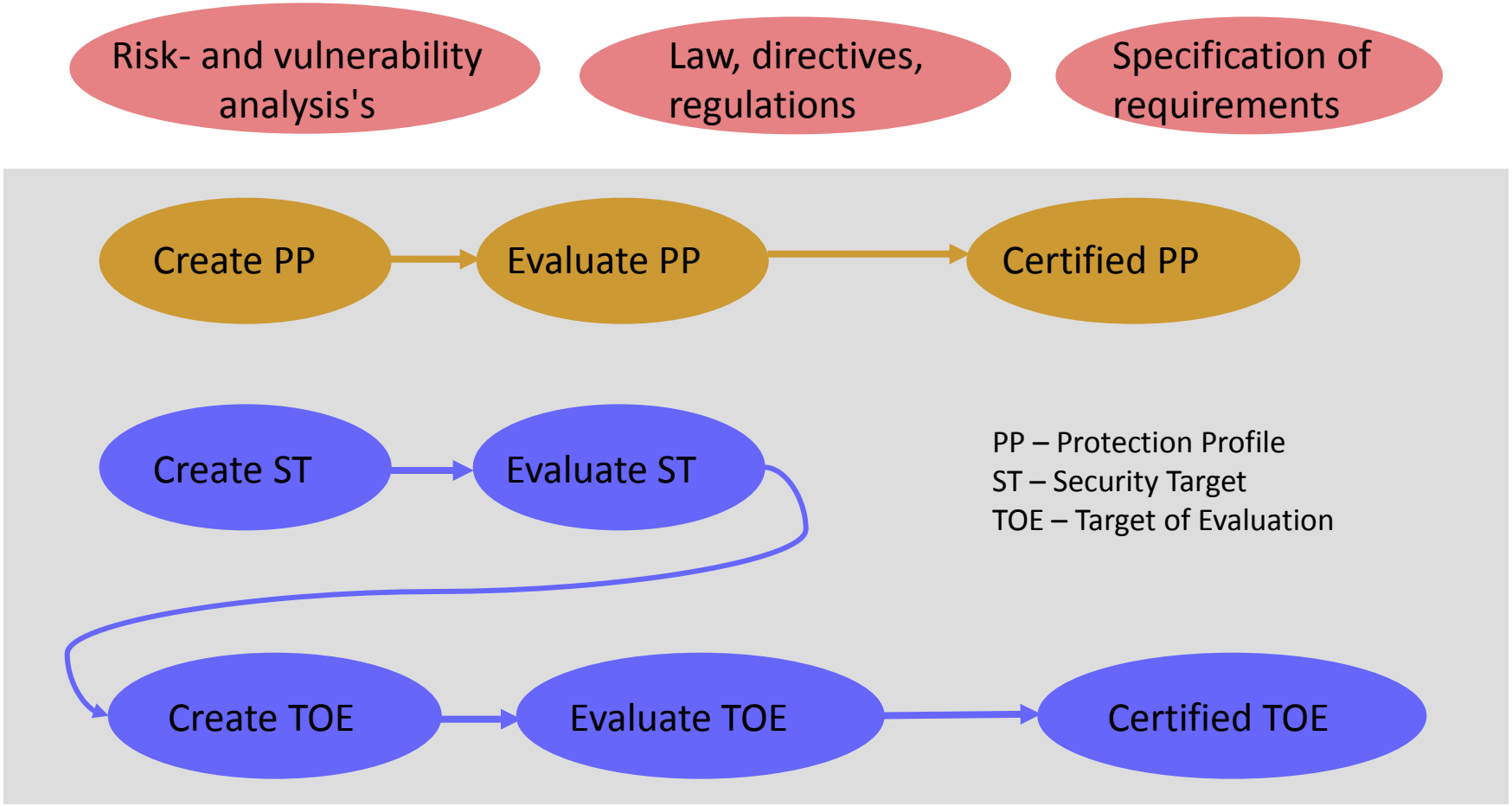
Target Of Evaluation (TOE)

- The product / system to be evaluated, or the part of the product / system to be evaluated
- Defined in the Security Target
- Physical and logical boundaries / interfaces to the environment should be specified
- Can be difficult to define, especially for systems!

Common Criteria – Evaluation



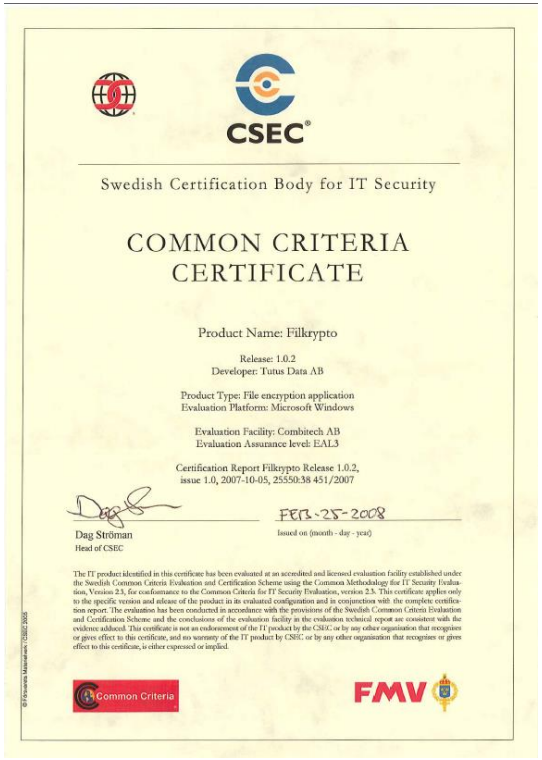
Common Criteria – Evaluation process



Common Criteria – Result

Example

- Certified product (www.csec.se):
  - CertID — CSEC 2006002
  - Product name — Tutus Filkrypto 1.0.2
  - Product category — Filkryptering
  - Security Target — ST Filkrypto 1.0.2
  - Assurance level — EAL3
  - Certification date — 2008-02-25
  - Certification Report — CR Filkrypto 1.0.2
  - Certificate — Filkrypto 1.0.2
  - Sponsor — Tutus Data AB
  - Evaluation facility — Combitech AB



CSEC

Swedish Certification Body for IT Security

COMMON CRITERIA CERTIFICATE

Product Name: Filkrypto

Release: 1.0.2
Developer: Tutus Data AB

Product Type: File encryption application
Evaluation Platform: Microsoft Windows

Evaluation Facility: Combitech AB
Evaluation Assurance level: EAL3

Certification Report Filkrypto Release 1.0.2, issue 1.0, 2007-10-05, 25550:38 451/2007

Dag Ströman
Head of CSEC

FEB-25-2008
Issued on (month - day - year)

The IT product identified in this certificate has been evaluated at an accredited and licensed evaluation facility established under the Swedish Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 2.3, for conformance to the Common Criteria for IT Security Evaluation, version 2.3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Swedish Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the CSEC or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria

FMV

Common Criteria – Evaluation

Execution of review

- Theoretical review of evaluation basis
  - Development descriptions
  - User Manuals
  - Security policies
  - Source code
  - Configuration management routines (CM)
- Practically performing of functional and penetrations tests
- Analysis through performing vulnerability assessment
- Conducting an Site Visit, which means that the developer is visited and that the CM-system, security policies and so on are inspected
- The results are presented in evaluation reports

Common Criteria – Assurance levels

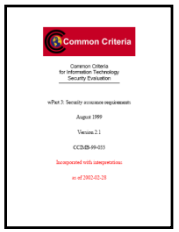
Assurance levels

- Evaluation can be done with varying degrees of accuracy, i.e. assurance levels, EAL
  - Depending on needs, protection values and threat
  - Low assurance - low cost, high assurance - higher cost

COMMON CRITERIA – THE STANDARD

Common Criteria – The standard

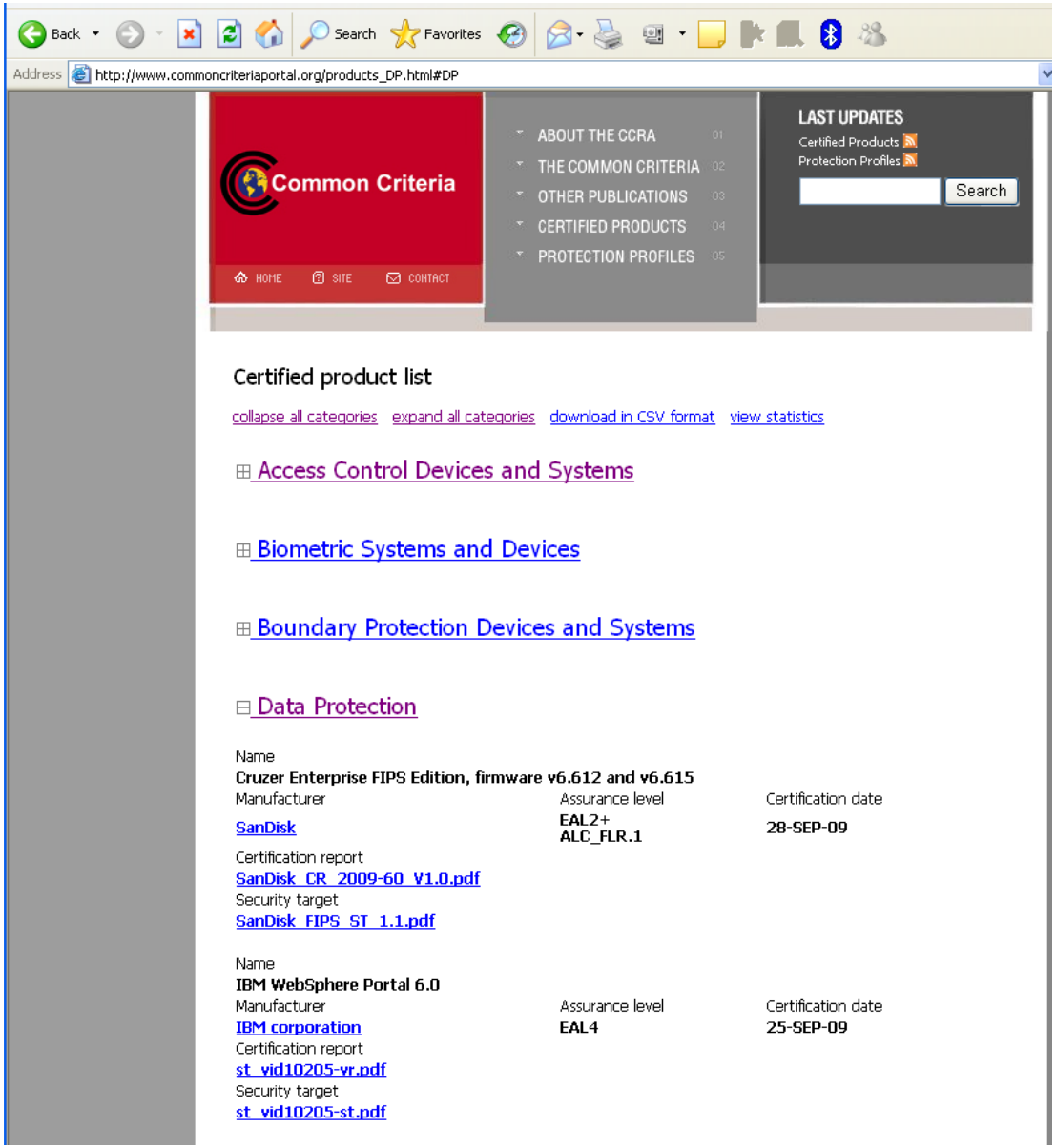
- The Common Criteria standard is comprised of three parts
  - Part 1, describes structure of and how to construct Protection Profiles and Security Targets in general
  - Part 2, Functional requirements
  - Part 3, Assurance requirement
- Methodology is described in Common Criteria Evaluation Methodology (CEM)
  - Describes in detail, what the evaluator must do
- The Standard could be downloaded free of charge, from
  - www.commoncriteriaportal.org
- Common Criteria is also an ISO standard ISO15408



Common Criteria Portal

Example

- *commoncriteriaportal.org*



COMMON CRITERIA SECURITY REQUIREMENTS

Common Criteria – Functional requirements

Functional requirements

1. Security Audit (FAU)
2. Communications (FCO)
3. Cryptographic Support (FCS)
4. User Data Protection (FDP)
5. Identification & Authentication (FIA)
6. Security Management (FMT)
7. Privacy (FPR)
8. Protection of the TOE Security Functions (FPT)
9. Resource Utilization (FRU)
10. TOE Access (FTA)
11. Trusted Path (FTP)

Common Criteria – Functional requirements

Protection Profile

Discretionary Access Control Policy (FDP_ACC.1)

- The TSF shall enforce the Discretionary Access Control Policy on [assignment: *list of subjects*] acting on the behalf of users, [assignment: *list of named objects*] and all operations among subjects and objects covered by the DAC policy.

Security Target

Discretionary Access Control Policy (FDP_ACC.1)

- The TSF shall enforce the Discretionary Access Control Policy on **processes** acting on the behalf of users **as subjects and file system objects (ordinary files, directories, device special files, UNIX Domain socket special files, named pipes), IPC objects (message queues, semaphores, shared memory segments) and TCP ports as objects** and all operations among subjects and objects covered by the DAC policy.

Common Criteria – Assurance requirements

Assurance requirements

- Describes
  - What the developer shall do
  - What shall be proven and presented
  - What the evaluator shall verify/inspect
- Are divided into seven Evaluation Assurance Levels
  - EAL1 – Functionally tested
  - EAL2 – Structurally tested
  - EAL3 – Methodically tested and checked
  - EAL4 – Methodically designed, tested, and reviewed
  - EAL5 – Semiformally designed and tested
  - EAL6 – Semiformally verified design and tested
  - EAL7 – Formally verified design and tested
- Are divided into six assurance classes

Common Criteria – Assurance requirements

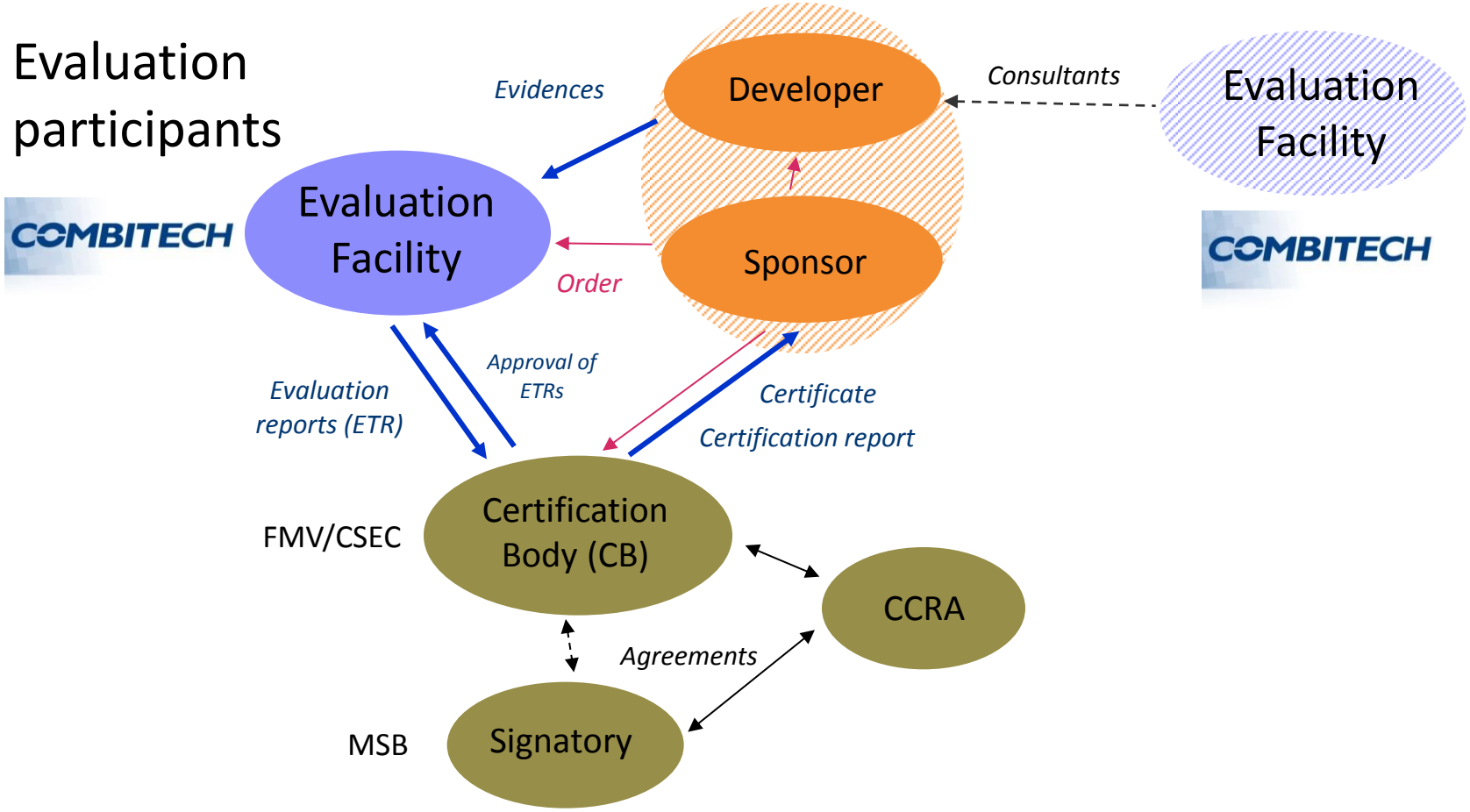
Assurance classes

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

COMMON CRITERIA - ROLES

Common Criteria – Roles

Evaluation participants



COMMON CRITERIA SKILLS

What skills are needed for a Common Criteria *evaluator*?

- At least two, three years of general experience in the area of information security
- Quite deep knowledge of security algorithms and functions
- Knowledge of performing tests and code reviews
- Experience of performing threats-/risk analysis
- Competence in developing well-written reports

COMMON CRITERIA - SUMMARY

Common Criteria

Summary

- The present international standard in terms of verification and evaluation of IT Security
- Provides independent verification of the security features of a product
- It permits comparability between the results of independent security evaluations
- It provides a common set of requirements for the security functionality of IT products and for assurance measures applied to these products during a security evaluation.

Common Criteria – Links

- For more information

  www.commoncriteriaportal.org

  www.ccusersforum.org

  www.csec.se

  www.itsef.se

COMBITECH