Security Certification and Standardization Caught in the Act

A Briefing beyond your Lecture Book's Onepager

Get your Lemons straight

- **Asymmetric Information is about hidden information.**
- **Impact of asymmetric information**
  - *Ex ante* (before contract, rules of the game): **adverse selection** (AS)
  - *Ex post* (after contract, game actions): **moral hazard** (MH)
- **NOTE:** We **primarily deal with uncertainty, risk is of second nature!** This proposition induces a torrent of issues we discuss later.

How to Deal with Lemons?

Signalling by the informed party

- Reputation (AS)
- Advertising (AS)
- Guarantees and Cost Sharing (AS)
- **Standard Conformance (AS)**
- Disclosure policies (AS)
- Overachievement (MH)

Screening by the uninformed party

- Samples (AS)
- Return Policies (AS)
- Test reports (AS)
- **Certification (AS)**
- Incentive schemes (MH)
- Sharing and Pooling (MH)

Common Ground are voluntary or mandatory Quality Standards underpinned by Monitoring.

How to approach insecurity?

- **Risk and threat, both are two sides of the same coin.**
- **Threats need to be handled by mitigation routines.**
- Routines can be **validated, their effectiveness verified.**
- Conditions to operators and assumptions may apply.

Certification

Certus and **facere** *(lat.)*

- *Certus* := **certain, safe**
- *Facere* := **create, establish**
- **Actions:**
  validate and/or **verify**

Valider *(lat.)*

```
int getRandomNumber()
```

Verus and facere *(lat.)*

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

The Brands of BSI Germany

Product Certification

Common Criteria/PP

Conformity Assessment

Technical Guidelines

Management System Certification

ISO 27001/IT-Grundschutz

Certification of Persons
Recognition of Auditing Bodies and Service Providers

I am a Certification Officer at BSI (DE)

1 BSI is a founding member of the Common Criteria and editor of several ISO/IEC standards.

2 One in every two globally certified smart cards was assessed and certified by the BSI.

3 One in every three valid product certificates around the world bears the BSI seal.

5 good reasons to obtain BSI certification: confidentiality, independence, reliability, objectivity, and many years of expertise.

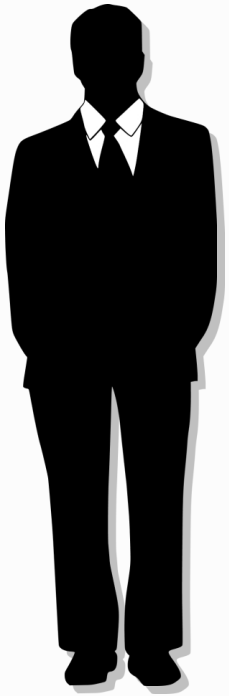
Federal Office
for Information Security

7 out of every 10 product certificates issued in the world (level EAL 5 to 7) come from the BSI.

ISO/IEC Common Criteria & Evaluation Methodology

15408-1: Introduction and Model	CC
15408-2: Security Functional Requirements (SFR)	
15408-3: Security Assurance Requirements (SAR)	
15408-4: Evaluation Activities and Methodologies	
15408-5: Security Packages	CEM
18045: Common Evaluation Methodology	

Common Criteria: Motivation



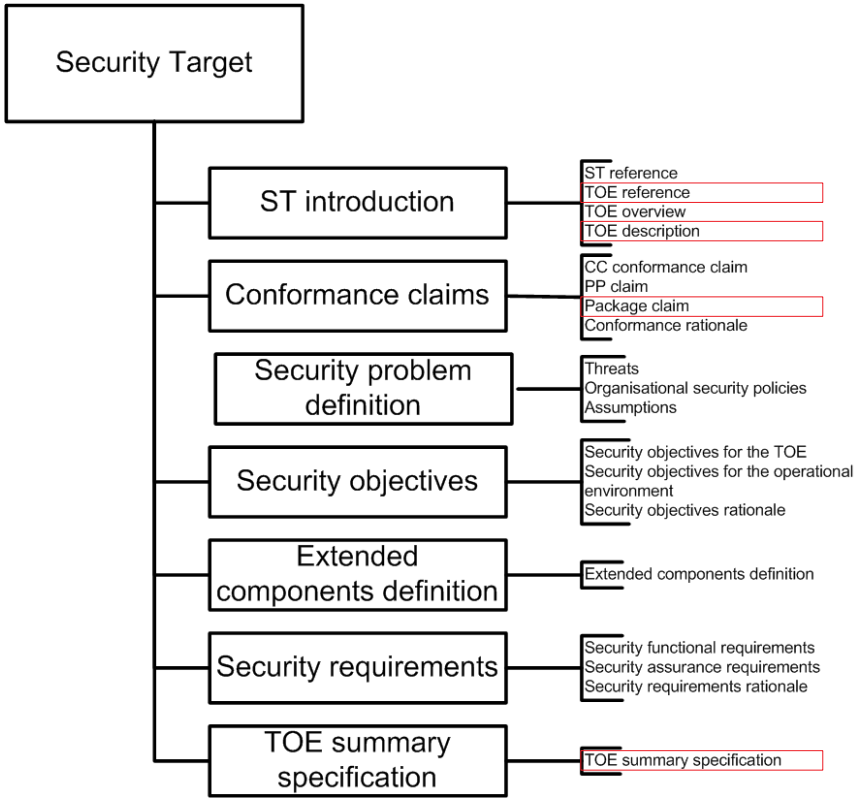
Customers need:

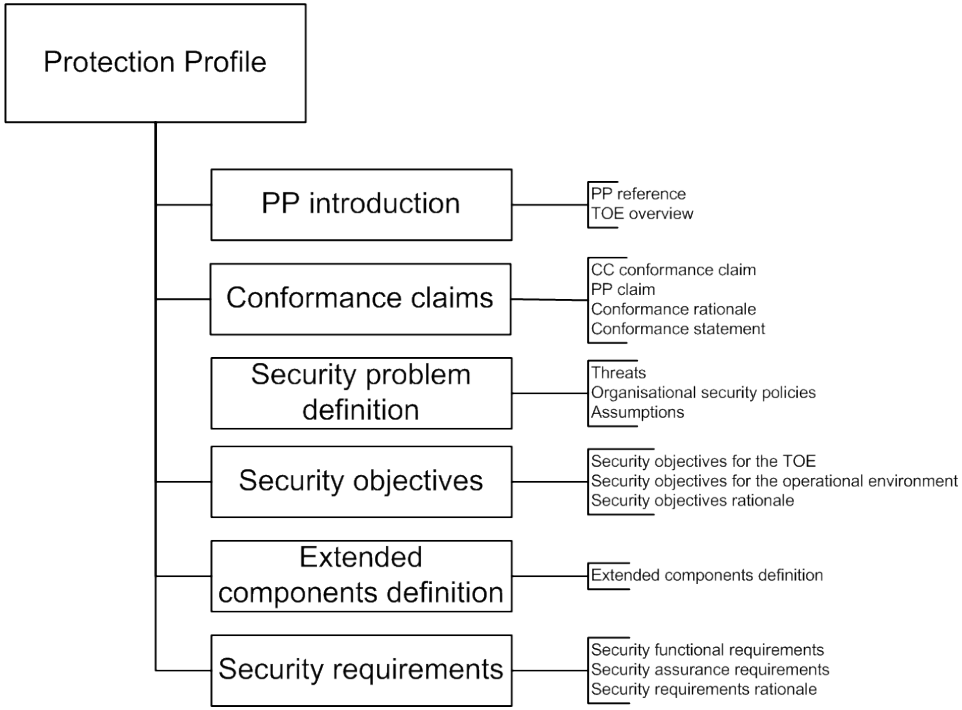
- Reliable Assurance on how a system or application meets their security need.
- Objective and reasonable assessment criteria.
- Independent and competent assessors.

Common Criteria: Specification of Security Needs

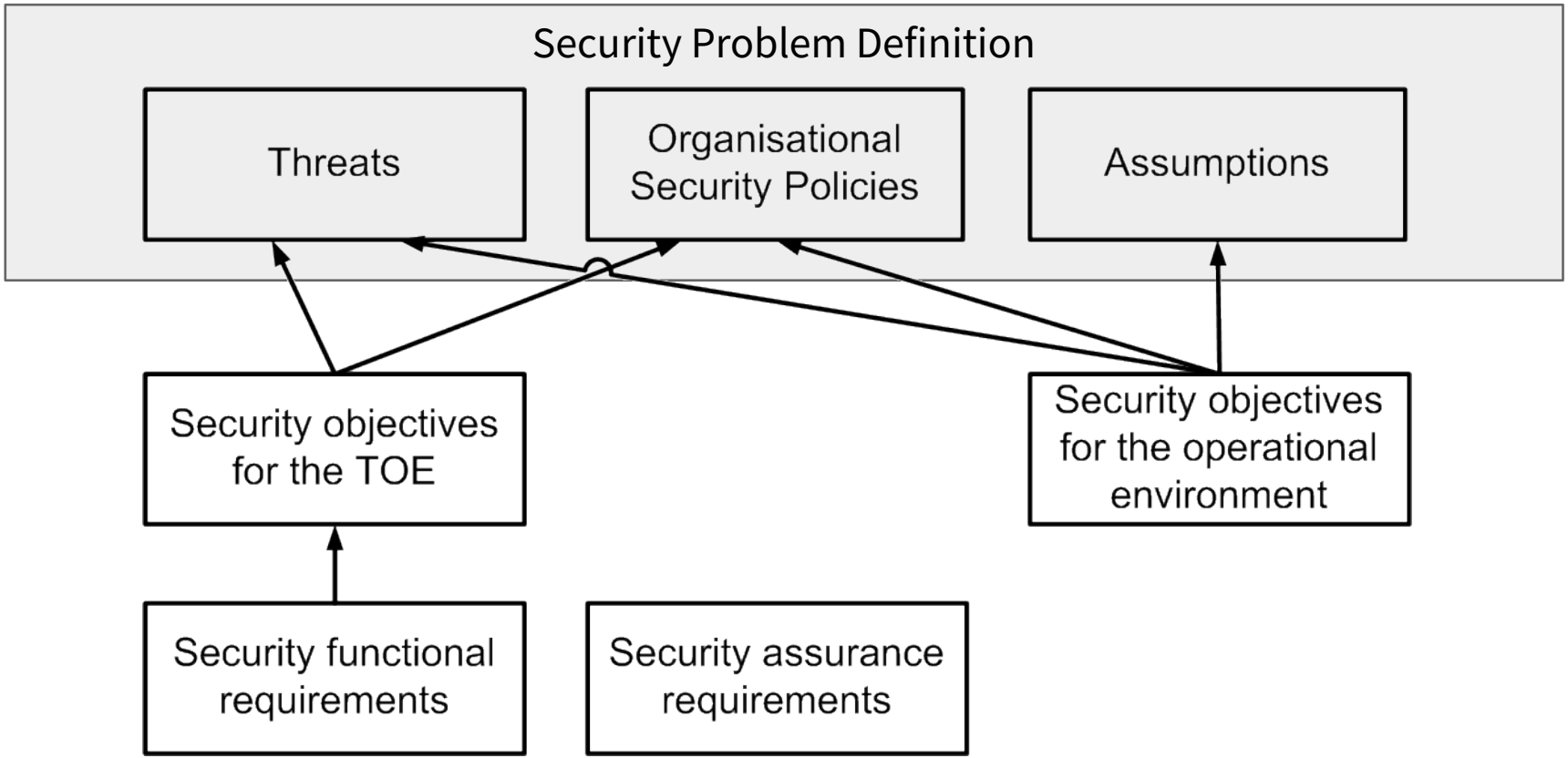
	Security Target - ST -	Protection Profile - PP -
Authors	Developer	Users, Developers and/or National Bodies
Scope	A Product's Security Functionality	Security Functionalities and Assurances for a Product Type
Applicability	Product version/release	Requirements for the Product Type
Utility	Access to security sensitive markets	Unified and Consistent Set of Requirements

Common Criteria: Security Specification Outlines

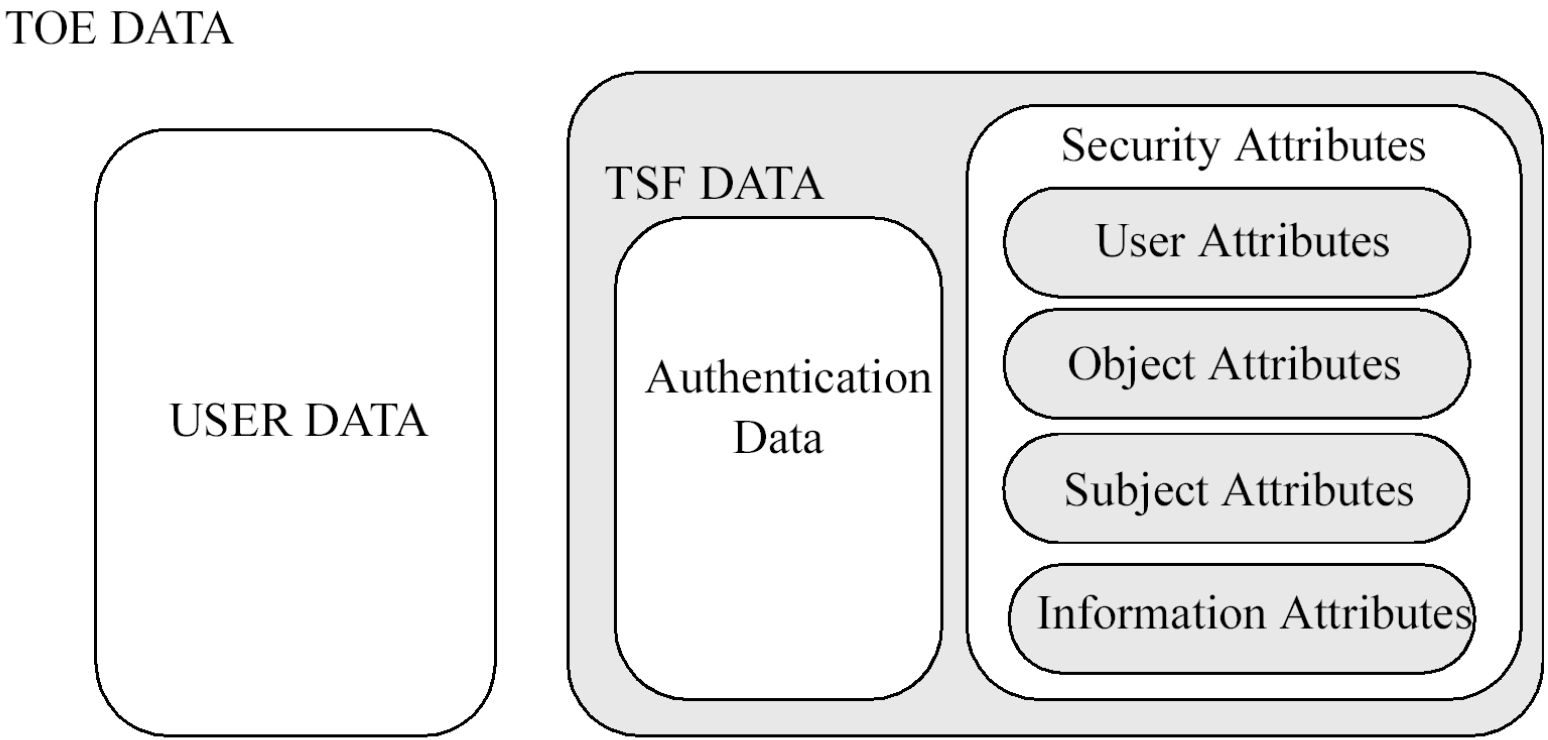




Common Criteria: Security Requirements

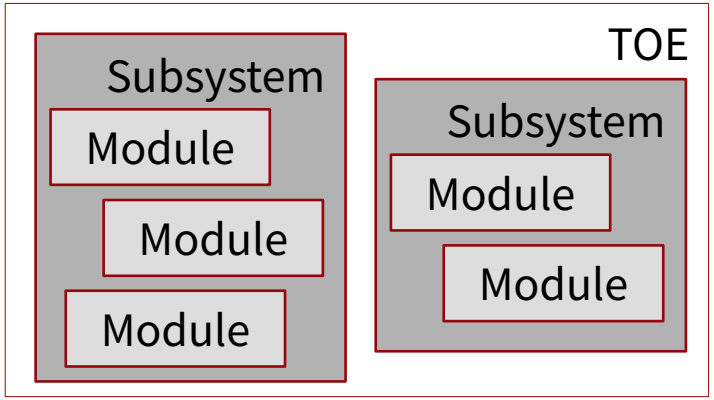


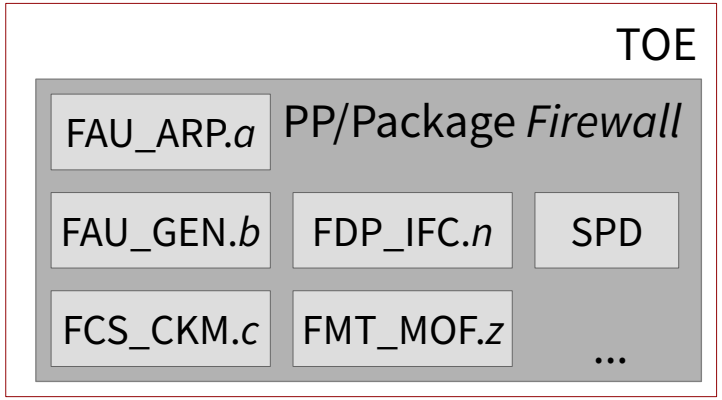
Common Criteria: Modelling Data as Assets



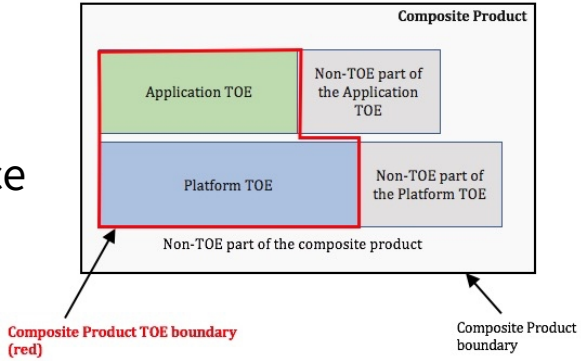
Common Criteria: Architectural Patterns

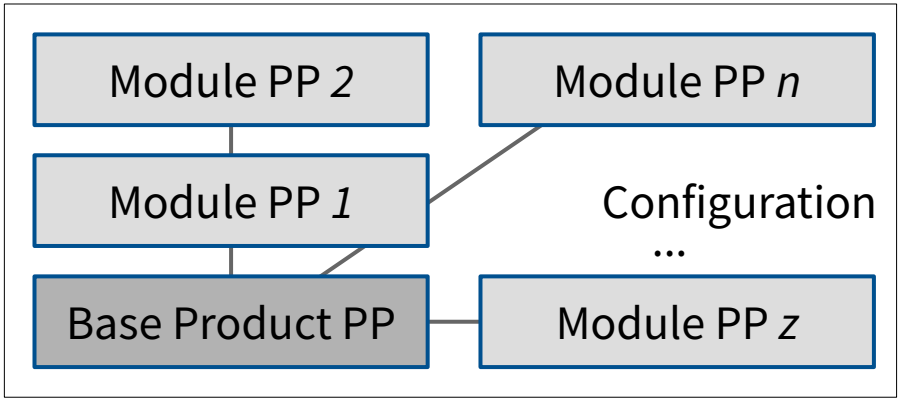
By segmenting a TSF
for structuring evaluations
and SFR representations





By coupling separate
TSF for a given Assurance





TSF: TOE Security Functionality

Common Criteria: SFR Classes

- **FAU:** Security audit (e.g. alarms, responses, logging, analysis)
- **FCO:** Communication (Non-repudiation of origin or receipt)
- **FCS:** Cryptographic support (e.g. key management, cryptographic operation)
- **FDP:** User data protection (e.g. control policy and functions for access and information flow control)
- **FIA:** Identification and authentication (e.g. attribute definition, user authentification and identification, failures)
- **FMT:** Security management (e.g. of the TSF, security attributes, roles)
- **FPR:** Privacy (anonymity, pseudonymity, unlinkability, unobservability)
- **FPT:** Protection of the TSF (fail secure, ‘CIA’ of data exported, internal transmission, physical)
- **FRU:** Resource utilisation (e.g. fault tolerance, resource allocation)
- **FTA:** TOE access (e.g. session locking and termination, access history)
- **FTP:** Trusted path/channels (inter-TSF trusted channel, trusted path)

Common Criteria: SFR Example

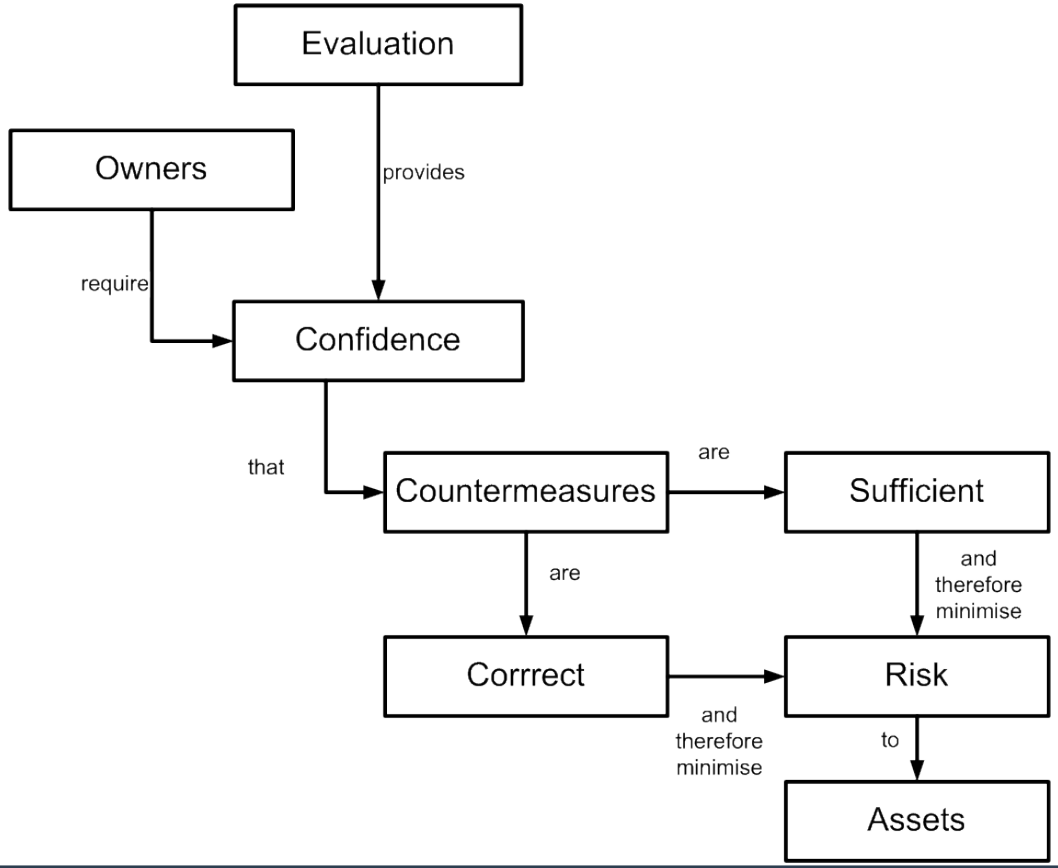
Class FMT: Security Management

- Family Management of Security Attributes (FMT_MSA)
  - Family Behaviour
  - Component levelling
  - Management of FMT_MSA.1, FMT_MSA.2, …, FMT_MSA.5
  - Audit of FMT_MSA.1, FMT_MSA.2, …, FMT_MSA.5
  - FMT_MSA.1 Management of security attributes
  - FMT_MSA.2 Secure security attributes (...)

Common Criteria: SFR Operations

- **Assignment:** assigning a parameter to an element; may be left undone
- **Iteration:** applying multiple requirements to a component; allowed for every component
- **Selection:** choosing from multiple given requirements of a component; may be left undone
- **Refinement:** altering (tightening) a requirement for some but not all entities; allowed for every component → extended component

Common Criteria: Assurance Model and Goal



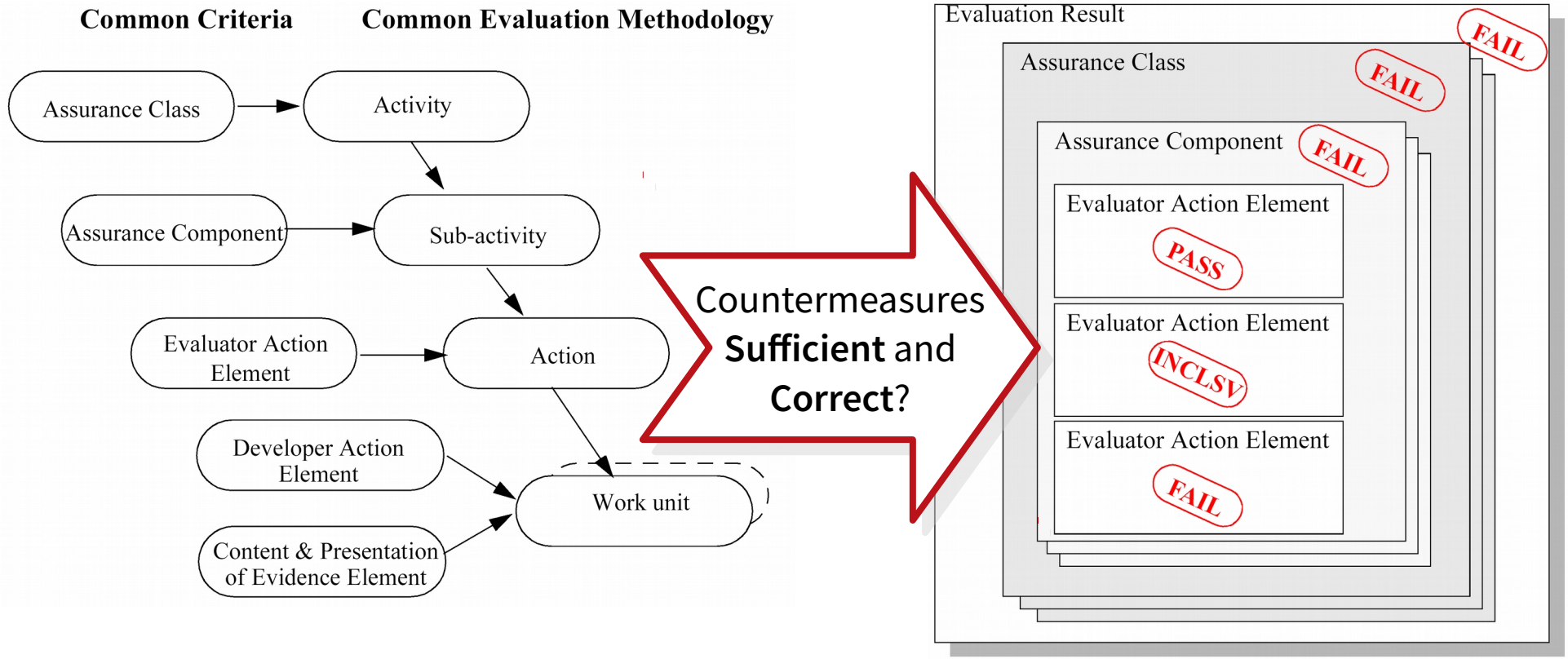
Common Criteria: SAR Overview and Packages

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							

Common Criteria: SAR

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		*EAL1**	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Life-cycle support	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	1	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 Evaluation Methodology



Common Criteria: Assurance Packages

EAL7 - formally verified design and tested

EAL6 - semiformally verified design and tested

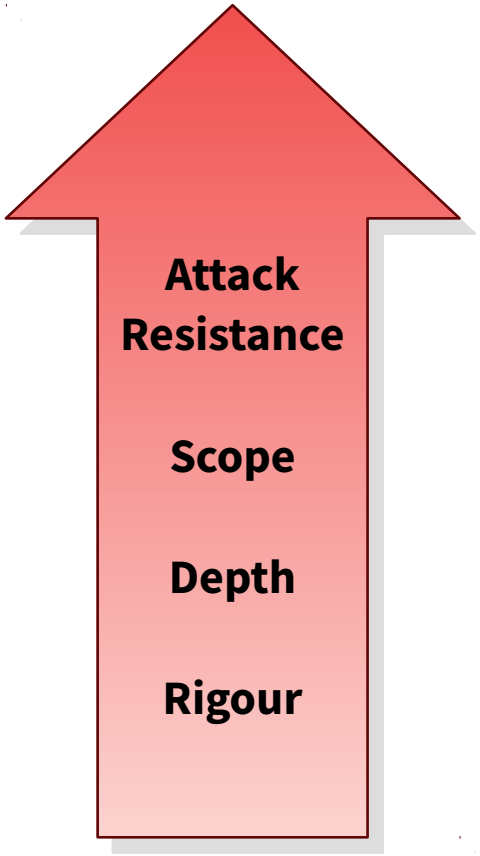
EAL5 - semiformally designed and tested

EAL4 - methodically designed, tested, and reviewed

EAL3 - methodically tested and checked

EAL2 - structurally tested

EAL1 - functionally tested



Common Criteria: SAR Example

Class AVA: Vulnerability assessment

- Family AVA_VAN.1 Vulnerability survey
  - Dependencies
  - Objectives
  - D+C – Developer action elements
    - *D – Action elements*
    - *C – Content and presentation elements*
  - E – Evaluator action elements:
    conduct, determine, examine, record, report

Vulnerabilities

- **Tampering**
- **Bypassing**
- **Direct Attacks**
- **Monitoring**
- **Misuse**

Common Criteria: Attack Potential and Vulnerabilities

Attack Efforts	**Value**
Elapsed Time	Max 19
+ Expertise	Max 8
+ Knowledge of TOE	Max 11
+ Window of Opportunity	Max 10
+ Equipment	Max 9

Σ

Value range	**Attack potential** for *exploit*	**TOE resistant** to attack potential	**Meets** assurance components	Fails assurance components
0-9	Basic	No rating	-	AVA_VAN. {1-5}
10-13	Enhanced-Basic	Basic	AVA_VAN. {1,2}	AVA_VAN. {3,-5}
14-19	Moderate	Enhanced-Basic	AVA_VAN. {1-3}	AVA_VAN. {4,5}
20-24	High	Moderate	AVA_VAN. {1-4}	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN. {1-5}	-

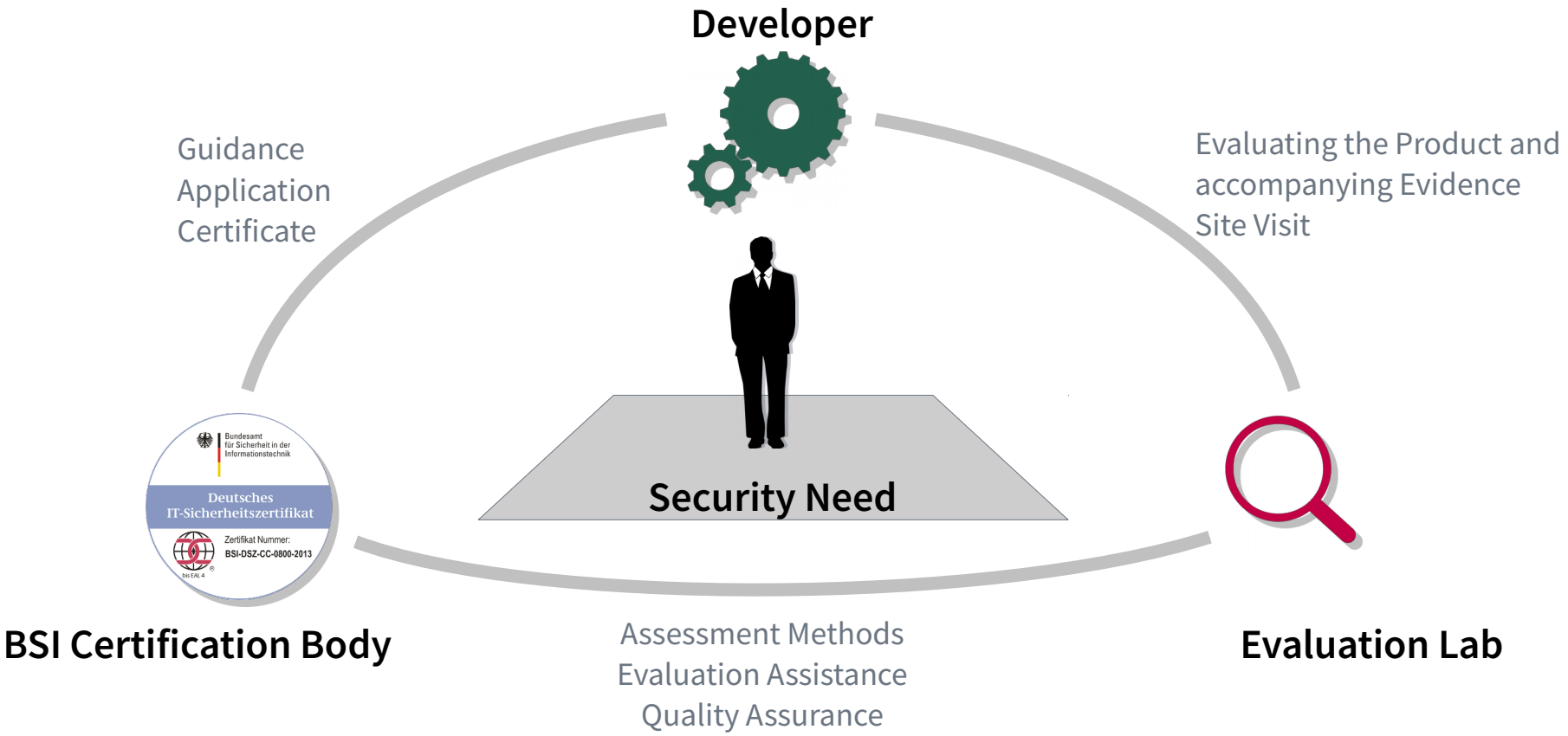
Common Criteria: Attack Potential and Vulnerabilities

What about government-sponsored attacks/back-doors or organized crime?

Attack Efforts	Value
Elapsed Time	Max 19
+ Expertise	Max 8
+ Knowledge of TOE	Max 11
+ Window of Opportunity	Max 10
+ Equipment	Max 9

Value range	**Attack potential** for *exploit*	**TOE resistant** to attack potential	**Meets** assurance components	Fails assurance components
0-9	Basic	No rating	-	AVA_VAN. {1-5}
10-13	Enhanced-Basic	Basic	AVA_VAN. {1,2}	AVA_VAN. {3,-5}
14-19	Moderate	Enhanced-Basic	AVA_VAN. {1-3}	AVA_VAN. {4,5}
20-24	High	Moderate	AVA_VAN. {1-4}	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN. {1-5}	-

Common Criteria: Partners in Certification



Common Criteria: Continuing Evaluation

Maintenance: certificate renewal for an updated TOE following an impact assessment when its **changes are minor**, i.e. security irrelevant.

Re-Certification: certificate renewal for the updated TOE following an assessment when its **changes are major**, i.e. security relevant.

Re-Assessment: certificate renewal for a TOE in an **evolved threat environment** following an updated vulnerability assessment (AVA).

Partial Re-Evaluation: renewing a **developer's site certificate** (after 2 years), primarily focussed on product's life cycle (ALC).

Common Criteria: Evaluated Products

Open Source: Red Hat Enterprise Linux Version 7.1 (EAL4+, DE), **JBoss Enterprise Application Platform 6** V. 6.2.2 (EAL4+, DE), **SUSE Linux Enterprise Server** 11 SP 2 (EAL4+, DE),

Apple Mac OS X 10.6 (EAL3+, DE)

Other players: **Microsoft Windows Server 2008** R2 (EAL4+, DE), **Microsoft SQL Server Database Engine** Enterprise Edition 2012, 2014 and 2016 (EAL4+, DE), **IBM DB2** Version 11 (EAL4+, DE), **Oracle Database 11g** (EAL4+, DE)

Juniper Netscreen Firewall: ScreenOS 6.2.0 and 6.3.0 contained a developer-induced *Q* point replacement flaw due to a NIST-flawed Dual EC DRBG **but not the evaluated versions 6.2.0r3, 5.0.0.r9 (EAL4+) or 6.3.0r6 (EAL2+)**

Smart Meters (SMETS1) in UK were not interoperable whereas the second generation (SMETS2) lacked some security engineering and secure transmission technologies (e.g. *one key for all* meters, *UK bespoke* ZigBee, GPRS) whereas Germany focused on PP 0073

Common Criteria: International Recognition

International and mutual recognition of CC certificates supports developers and userswith **harmonized functional and assurance requirements** and **saves resources** through **avoided multiple certifications**.

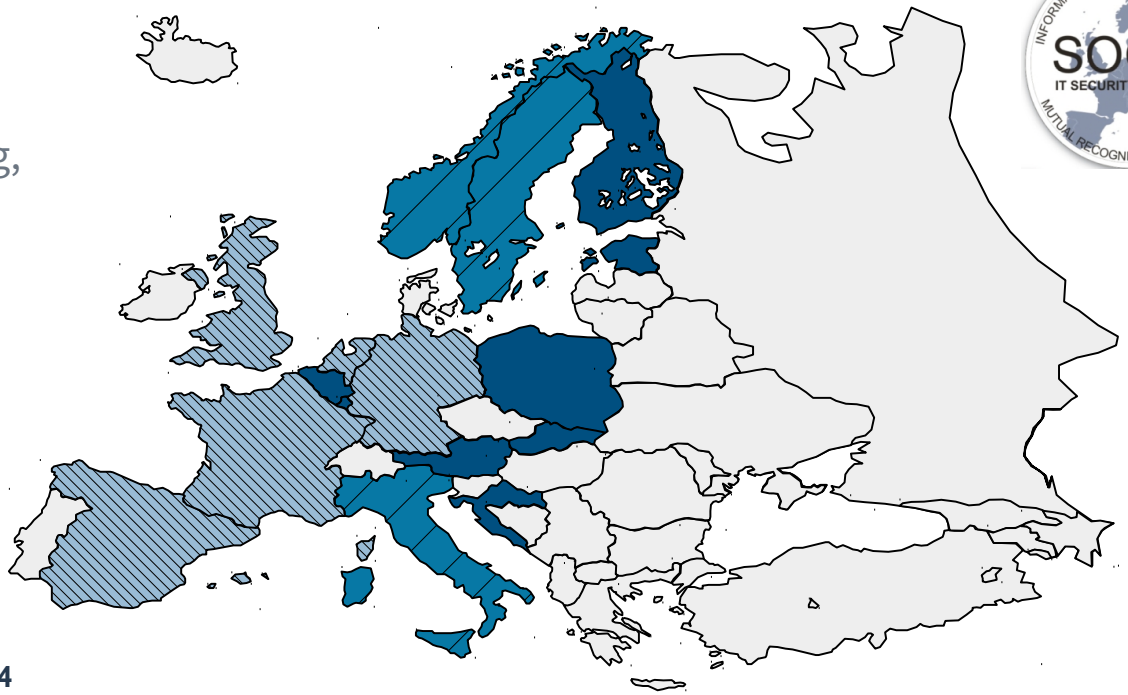
Europe:
SOGIS-MRA

Worldwide:
CCRA

Common Criteria: European-wide – SOGIS-MRA

France
Germany
Italy
Netherlands
Spain
United Kingdom

Austria, Belgium,
Estonia, Finland
Croatia, Luxemburg,
Norway, Poland
Slovakia, Sweden

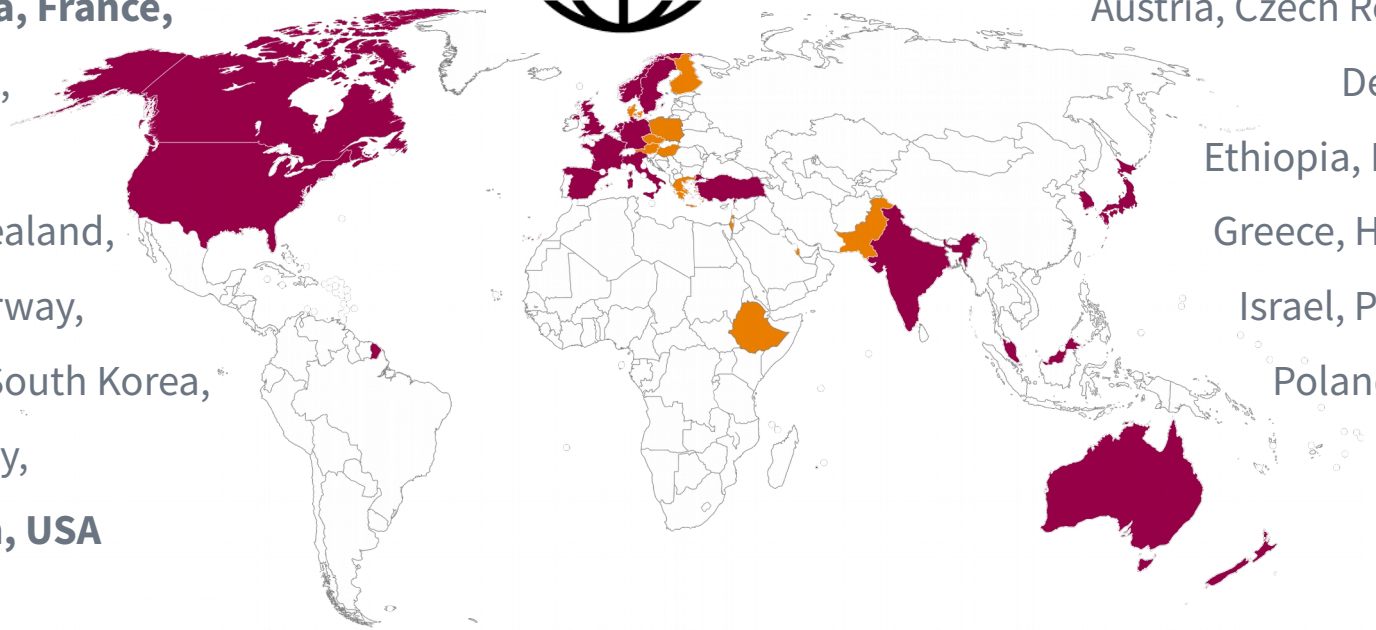


Certificate Consuming Member
Certificate Authorizing Member up to EAL 4
Certificate Authorizing Member up to EAL 7 in certain domains

Common Criteria: International – The CCRA

Authorizing Members

Australia, **Canada, France, Germany**, Japan, India, Italy, Malaysia, New Zealand, Netherlands, Norway, Sweden, Spain, South Korea, Singapore, Turkey, **United Kingdom, USA**



Consuming Members

Austria, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Israel, Pakistan, Poland, Qatar

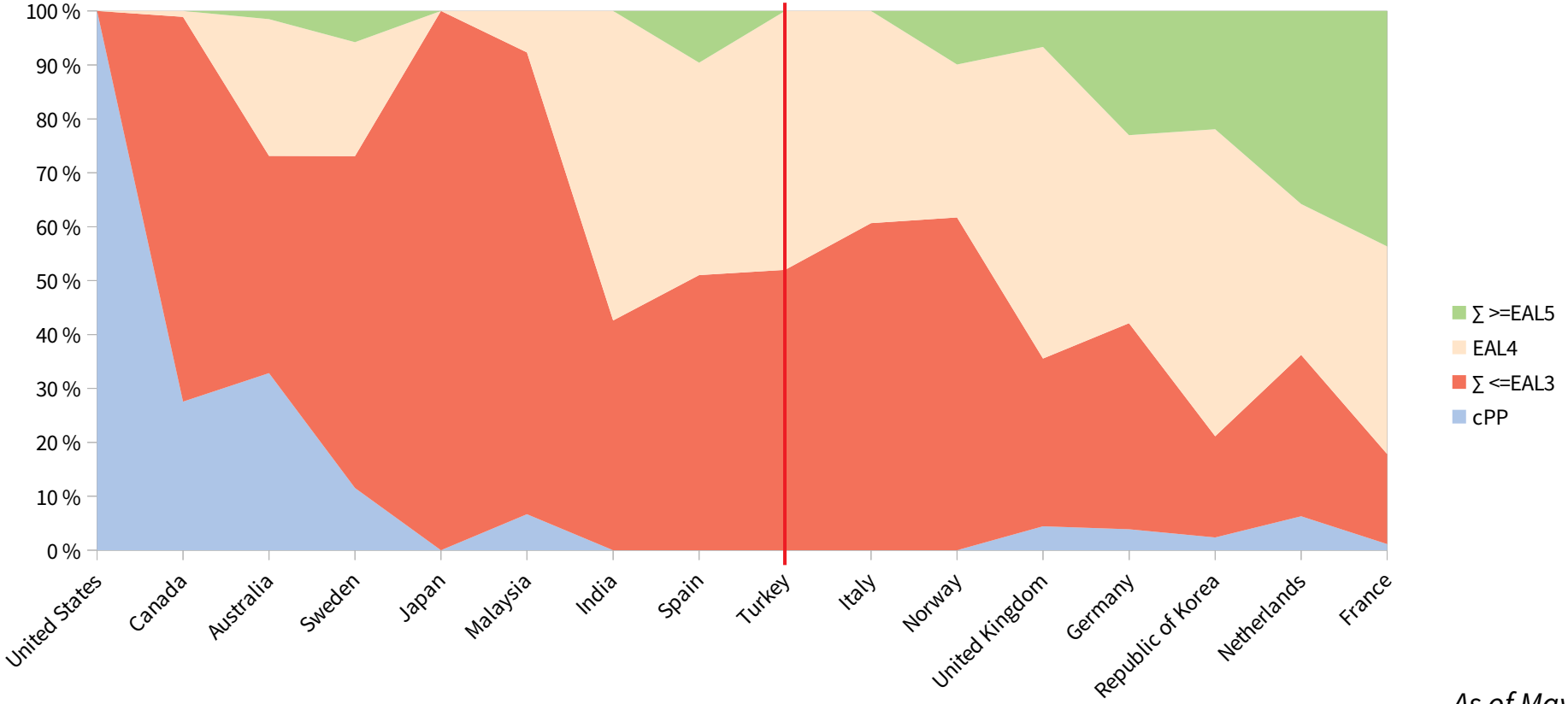
Common Criteria: International – The CCRA since 2014

„Low Assurance Policy“:
No Mutual Recognition
Beyond EAL Level 2

„collaborative Protection Profiles“ (cPP):
Collaborative Development of Protection Profile for COTS Products (EAL Level 1-4)

Motivation:
Establishing Comparable Evaluation Results
Driven by a growing Community

Common Criteria: Issued Certificates by EAL and Country



As of May 2019