Security Assessment and Certification Standards

Security Assurance and Trust

- Security can be assessed, but
  - How can the achieved security be **measured**?
  - How can a user **trust** the security of a product?
- We need
  - Metrics for security **assurance**
  - Ways to **certify** security
    - Provide credible **evidence** that a certain level of security assurance has been achieved
    - Checked by **independent trusted third parties**

Confidence that an entity meets its security requirements

How to Achieve Assurance?

- Use of security controls/mechanisms
- Use of development methodologies
- Use of security assessment techniques
- …
- Assurance Techniques
  - can be classified as formal, semi-formal, informal
  - apply to different development stages
    - policy assurance, design assurance, implementation assurance, operational assurance

Assurance Techniques

How to Evaluate/Certify Assurance?

- Evaluation
  - based on what assurance techniques have been employed (assurance effort) and what results have been obtained
- Certification
  - Based on
    - evidence of employed assurance techniques/results
    - evidence of evaluation methodology
    - Independency/accreditation of evaluators

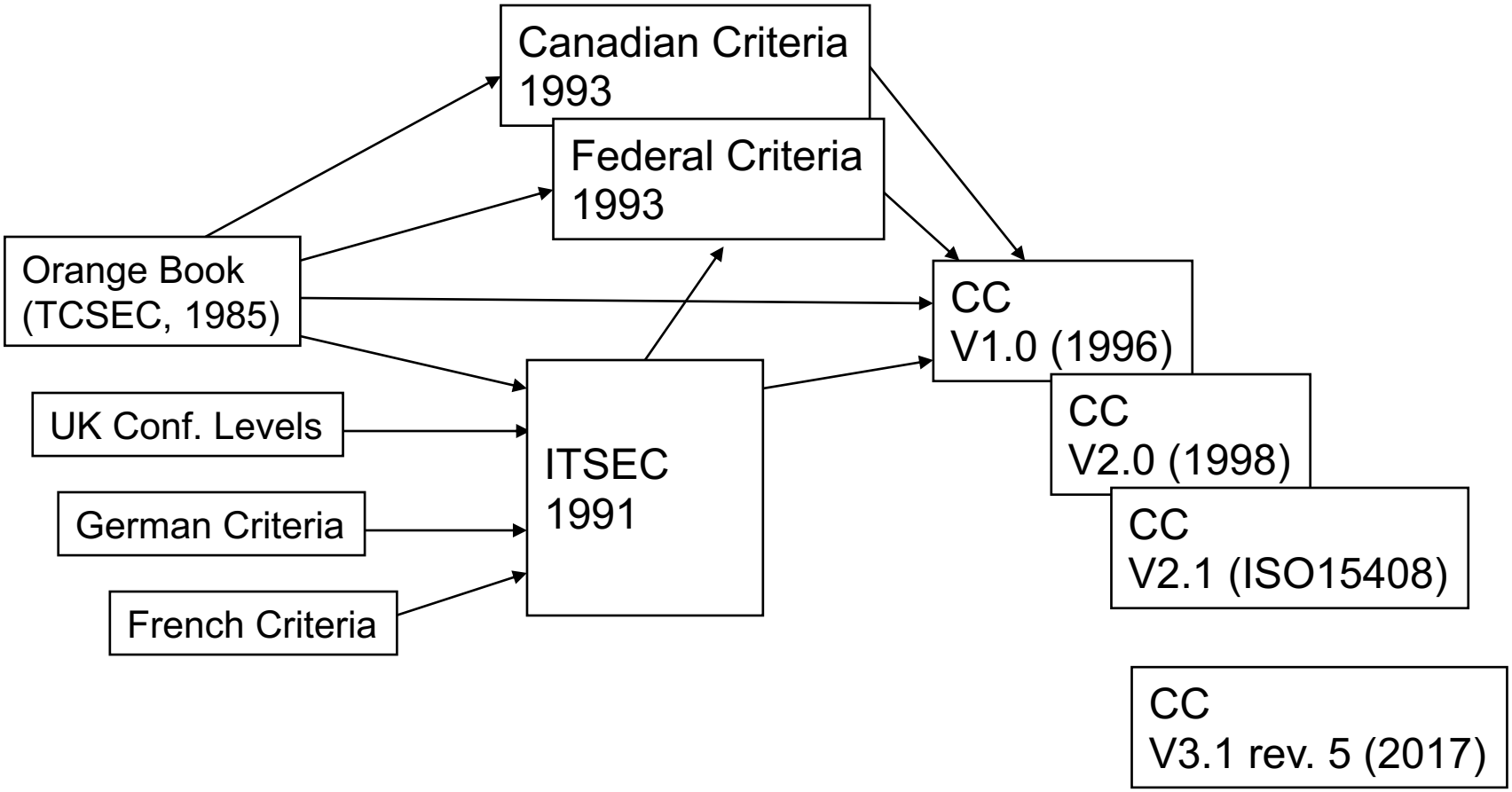
Security Evaluation Standards

- Product Evaluation
  - Common Critera (CC) and its predecessors
  - Field-Specific standards/regulations referring to CC (e.g., in the automotive field, ISO 21434)
  - NIST SP 800-115 "Technical Guide to Information Security Testing and Assessment"
- Process Evaluation
  - Systems Security Engineering Capability Maturity Model (SSE-CMM)

Common Criteria (CC)

- Information Technology **Security Evaluation Standard**
- Fusion of similar national standards (Canada, France, Germany, Holland, Great Britain and United States)
- Also standardized by ISO (ISO 15408)
- Standard documents can be downloaded from the web site https://www.commoncriteriaportal.org

CC History


Canadian Criteria
1993
Federal Criteria
1993
Orange Book
(TCSEC, 1985)
CC
V1.0 (1996)
CC
V2.0 (1998)
CC
V2.1 (ISO15408)
UK Conf. Levels
ITSEC
1991
German Criteria
French Criteria
CC
V3.1 rev. 5 (2017)

CC Objectives

- Provide a common standard reference for evaluating/certifying IT system security.
- "*Confidence in the security of a product, system or service is very much a state of mind. The CC can be used to build such confidence by providing a means of quantifying or measuring the extent to which security has been assessed*" (CC User Guide).

CC Objectives

- Permit comparability between the results of independent security evaluations
- => Achieved by providing a standard/uniform
  - approach to evaluation/certification
  - way of expressing security requirements and assurance levels
  - set of constraints on the evaluation methodology

CC Approach

- CC are just criteria. They do NOT define
  - a particular *development process* (but they refer to typical development phases)
  - a particular *evaluation methodology*
  - a particular *regulatory framework*

CC Approach

- A companion standard defines a common *evaluation methodology*:
  - **Common Methodology for Information Technology Security Evaluation (CEM)**
  - Minimum actions to be taken by evaluators
- Each Nation defines its own regulatory framework (**Evaluation Scheme**)

CC Document Structure

- Part 1: Introduction and General Model
  - general concepts and principles of IT security evaluation, general model of evaluation, constructs for writing high-level specifications.
- Part 2: Security Functional Requirements
  - standard way of expressing security functional requirements
- Part 3: Security Assurance Requirements
  - standard way of expressing security assurance requirements

CC Key Concepts

- Target of Evaluation (TOE)
  - The system or component under evaluation (sw, hw, fw, + guidance)
  - Examples: an OS, a sw app, a sw app running on a specific OS, etc
  - A TOE has Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs)
- TOE Security Functionality (TSF)
  - Parts of the TOE that must be relied on for the correct enforcement of the SFRs

CC Key Concepts

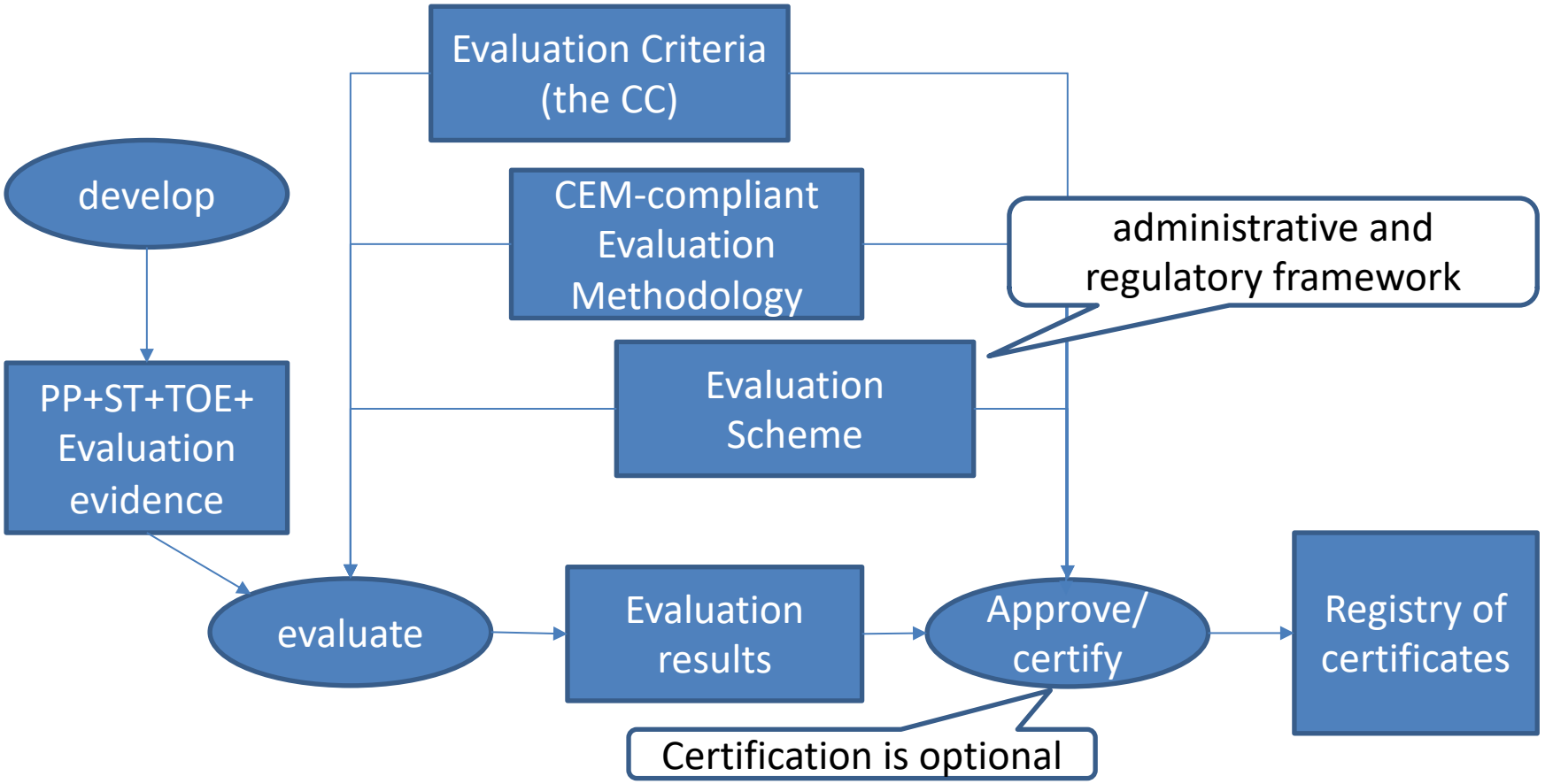
- Protection Profile (PP)
  - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs
- Security Target (ST)
  - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE
- Possibility to evaluate PP or TOE+ST

CC aim of TOE+ST Evaluation

- The aim of Evaluation is to evaluate **sufficiency** and **correctness** of TSF adopted to satisfy security requirements
  - Confidence that the TSF, if assumed correct, is **sufficient** to satisfy the requirements
  - Confidence that the TSF is **correct**

    => also means vulnerabilities are absent/ minimized/monitored

The Context of a TOE+ST Evaluation



CC Recognition Arrangement (CCRA)

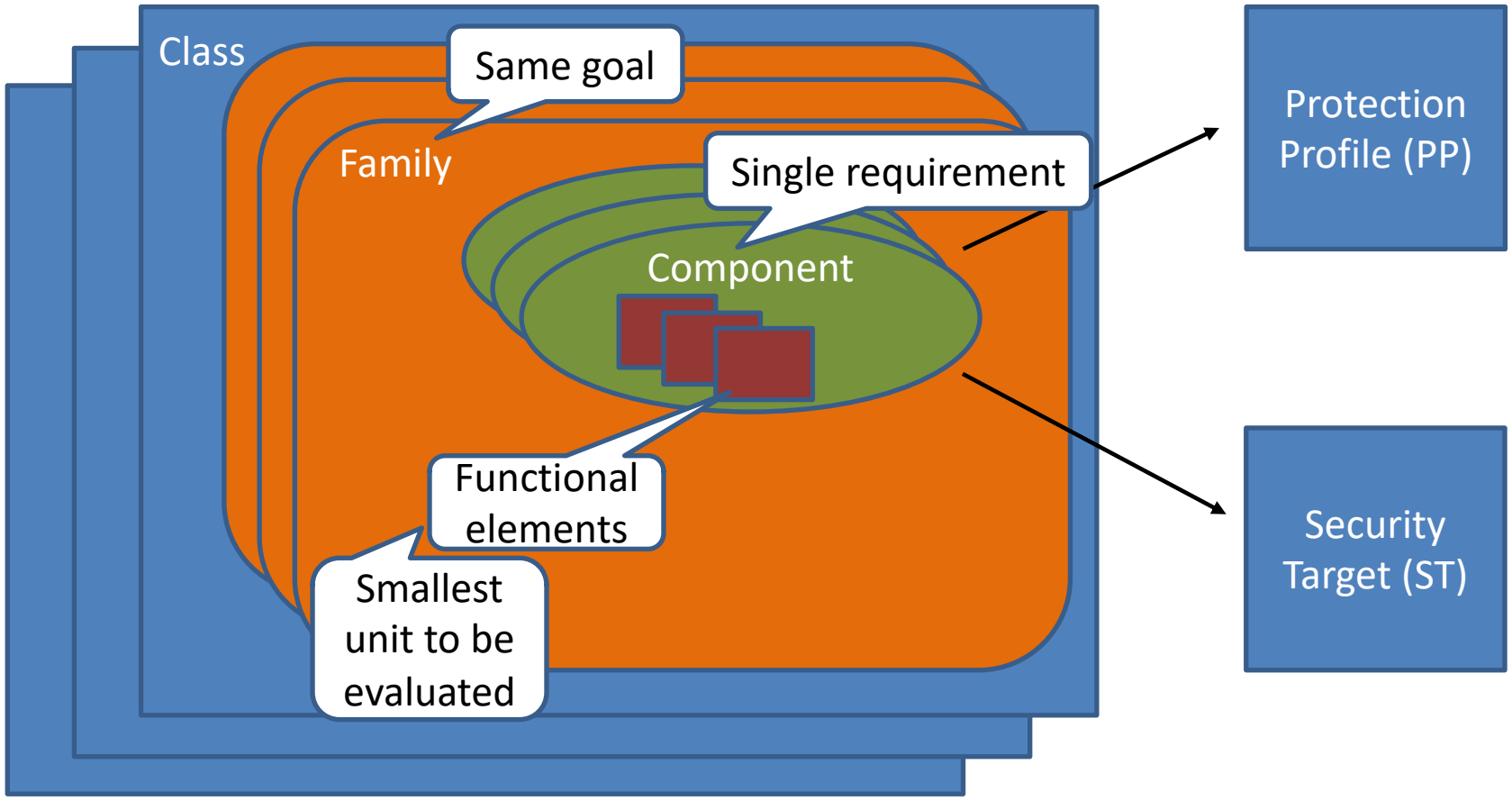
- Authorizing Nations (certificate producing)
  - have developed their own Evaluation Scheme to accredit laboratories to perform CC evaluations
- Consuming Nations (certificate consuming)
  - Don't have their own Evaluation Scheme but want to recognize CC evaluations done by others
- All Nations signers of the CCRA recognize the results of evaluations done by the Authorizing Nations

CC Recognition Arrangement (CCRA)

- Italy: one of the Authorizing Nations
- In Italy, the National Scheme is managed by OCSI (Organismo di Certificazione della Sicurezza Informatica)

  http://www.ocsi.gov.it/
- In 2022, OCSI functions have been transferred to the Italian National Cybersecurity Agency (ACN)

Functional Security Requirements Classification



Example

- **Class** "Identification and Authentication" (FIA)
  - **Family** "User authentication" (UAU)

components

- FIA_UAU.1 Timing of authentication, allows a user to perform certain actions prior to the authentication of the user's identity.
- FIA_UAU.2 User authentication before any action, requires that users authenticate themselves before any action will be allowed by the TSF.
- FIA_UAU.3 Unforgeable authentication, requires the authentication mechanism to be able to detect and prevent the use of authentication data that has been forged or copied.
- ...

Functional elements

FIA_UAU.3.1 The TSF shall [detect/prevent] use of authentication data that has been forged by any user of the TSF
FIA_UAU.3.2 The TSF shall [detect/prevent] use of authentication data that has been copied from any user of the TSF

The Classes

- FAU: Security Audit
- FCO: Communication
- FCS: Cryptographic Support
- FDP: User Data protection
- FIA: Identification and Authentication
- FMT: Security Management
- FPR: Privacy
- FPT: Protection of the TSF
- FRU: Resource Utilization
- FTA: TOE Access
- FTP: Trusted Path Channels

Assurance Requirements

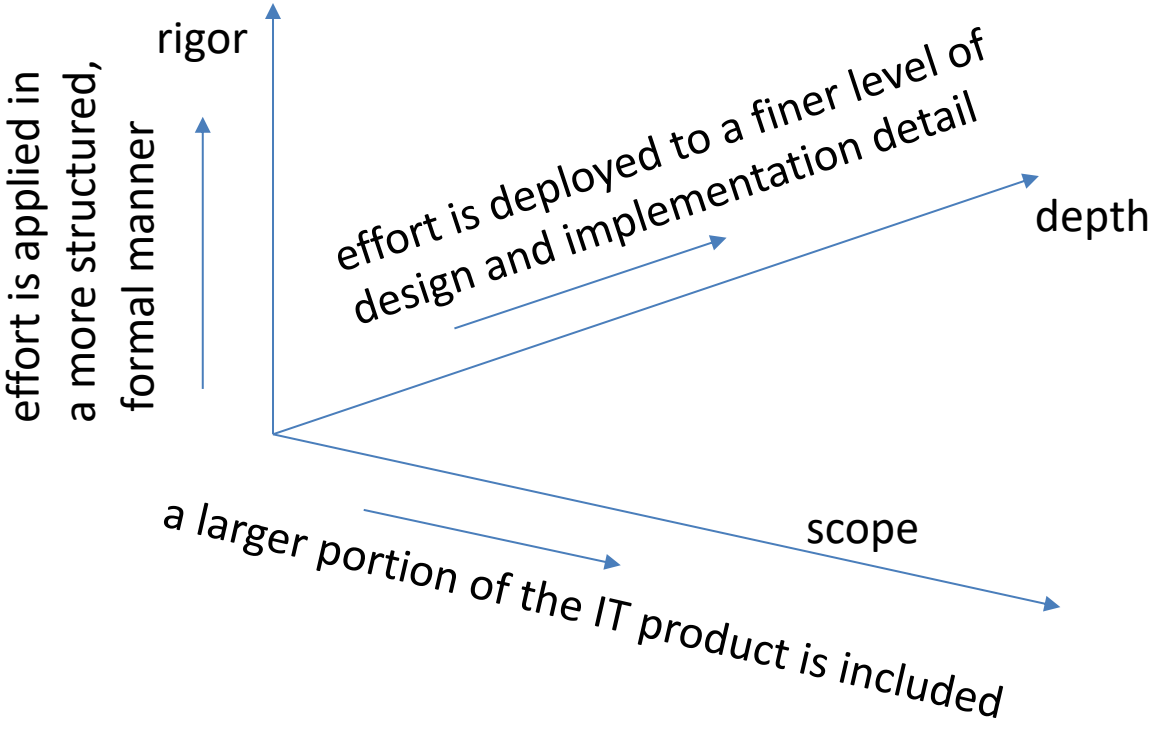
- Assurance Requirements correspond to the intended Assurance Techniques
- Assurance is achieved by
  - evaluating the evidence that the intended Assurance Techniques have been applied
  - performing independent verification/testing activities

Assurance Evaluation Techniques

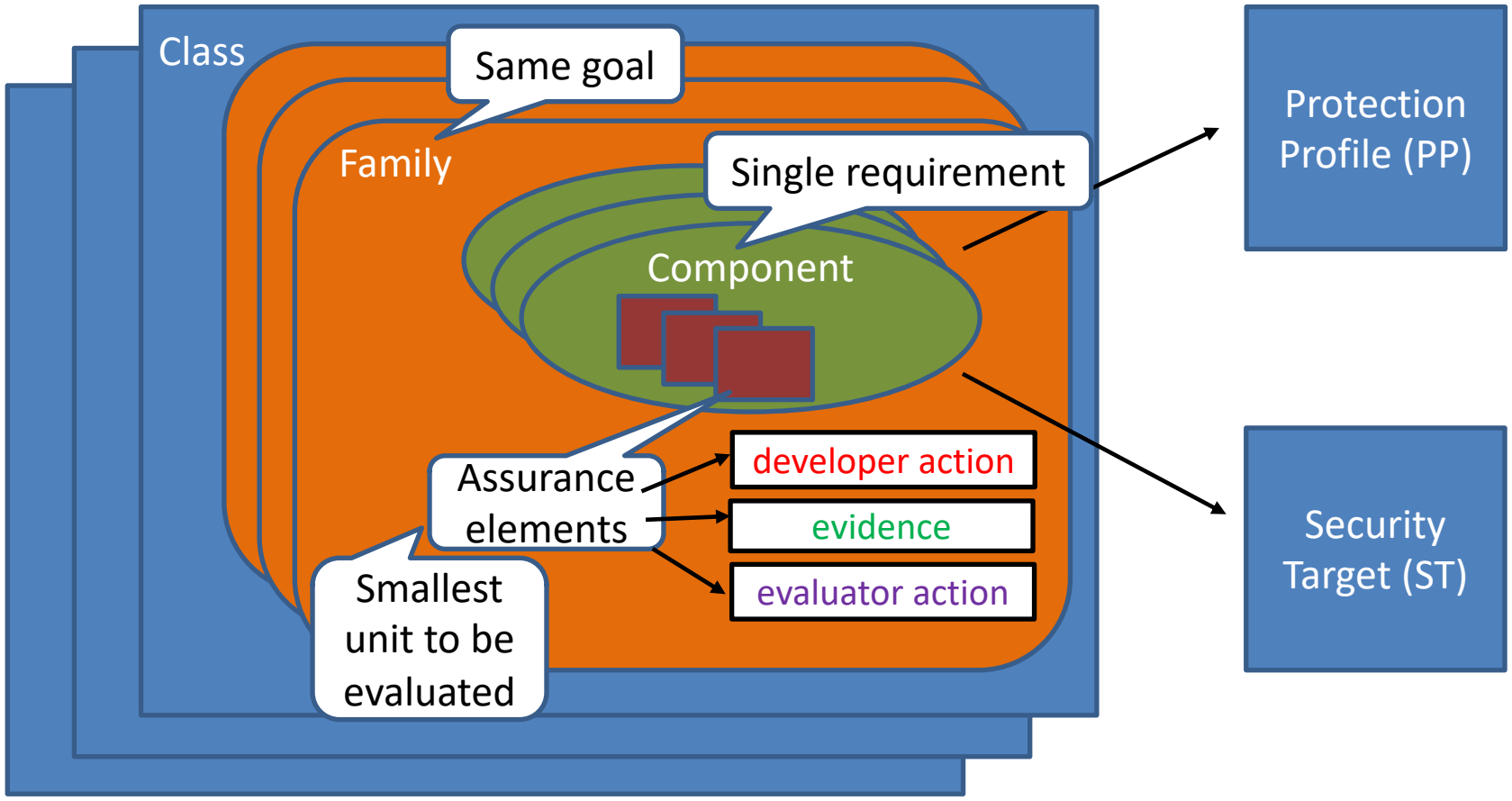
- Analysis and checking of processes and procedures
- Checking that processes and procedures are being applied
- Analysis of the correspondence between TOE design representations
- analysis of the TOE design representation against the requirements
- Verification of proofs
- Analysis of guidance documents
- Analysis of the functional tests developed and of the results provided
- Independent functional testing
- Analysis for vulnerabilities
- Penetration testing

Assurance Effort Scale

- Assurance Effort is measured along three dimensions



Assurance Requirements Classification



Example

- **Class** "Vulnerability Assessment" (AVA)
  - **Family** "Vulnerability Analysis" (VAN)

components

- AVA_VAN.1 Vulnerability Survey, the evaluator performs a vulnerability survey and penetration testing to confirm.
- AVA_VAN.2 Vulnerability Analysis, the evaluator performs a vulnerability analysis and penetration testing to confirm.
- …

Assurance elements

AVA_VAN.2.1D The developer shall provide the TOE for testing
AVA_VAN.2.1C The TOE should be suitable for testing
AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for evidence
AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to find vulnerabilities in the TOE
AVA_VAN.2.3E The evaluator shall perform an independent VA
AVA_VAN.2.4E The evaluator shall conduct PT (basic attack potential)

The Classes

- APE: PP Evaluation
- ACE: PP Configuration Evaluation
- ASE: ST Evaluation
- ADV: Development
- AGD: Guidance Documents
- ALC: Life-Cycle Support
- ATE: Tests
- AVA: Vulnerability Assessment
- ACO: Composition

The Development Class

- ADV_ARC
  - developer must provide description of **TSF security architecture**
- ADV_FSP
  - developer must provide **functional specification of TSF interfaces** (6 components with increasing levels of detail and rigor)
- ADV_IMP
  - Developer must provide **implementation representation of the TSF** in a form that can be analyzed (2 components. The higher one requires complete mapping and demonstration of correspondence with TOE design)

The Development Class

- ADV_INT
  - developer must design and implement TSF with well-structured internals and minimum complexity (2 components)
- ADV_SPM
  - developer must provide formal Security Policy Model (SPM) and a proof of correspondence with the functional specifications
- ADV_TDS
  - Developer must provide the design of the TOE with mapping to functional TSF interfaces (6 components with increasing levels of detail and rigor)

The Tests Class

- ATE_COV: Coverage
  - Developer must provide evidence of test coverage and its analysis (3 components with increasing requirements about coverage)
- ATE_DPT: Depth
  - developer must provide evidence of depth of testing
- ATE_FUN: Functional Testing
  - Developer must perform functional tests and provide the results and documentation showing the tests have passed (2 components with increasing requirements about the tests)
- ATE_IND: Independent Testing
  - Evaluator must confirm developer tests and perform other tests

The Vulnerability Assessment Class

- The developer provides the TOE, the evaluator performs VA and PT.
- Only 1 family, with 5 components requiring increasing
  - rigor of vulnerability analysis done by the evaluator
  - attack potential required by an attacker to identify and exploit the potential vulnerabilities found

	Rigor of VA	Attack potential
1	Survey based on searches in public repositories	Basic
2	Real VA done by evaluator	Enhanced-Basic
3	Focused VA (based on more information)	Enhanced-Basic
4	Methodical VA	Moderate
5	Methodical VA	High

Assurance Levels

- The assurance achieved is quantified by means of discrete **Evaluation Assurance Levels (EAL)**
- Each EAL requires a set of components
- A higher EAL is obtained from the previous one by
  - Including other components (other families)
  - replacing components with higher level assurance components (same family)

Predefined EALs

- 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, designed and tested
- EAL7 - formally verified, designed and tested

Class	Family	Assurance Components						
		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
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
VA	AVA_VAN	1	2	2	3	4	5	5

EAL1 Functionally Tested

- Some confidence in correct operation is required, but the **threats to security are not viewed as serious**
- No need for derivation of SFR from threats
- No developer assistance necessary to conduct evaluation
- Independent testing against specification and guidance doc (vulnerability survey)

EAL2 Structurally Tested

- **Low to moderate level of independently assured security** in the absence of ready availability of the complete development record (e.g. legacy systems) is required
- Co-operation of the developer in terms of the delivery of design information and test results
- Real vulnerability analysis

EAL3 Methodologically Tested and Checked

- A **moderate level of independently assured security is required**, and a thorough investigation of the TOE and its development, **without substantial re-engineering**.
- Additional requirements about what is required from developer and its analysis

EAL4 Methodologically Designed Tested and Reviewed

- A **moderate to high level of independently assured security in conventional commodity TOEs** is required
- Positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources
- Includes evaluation of implementation design and more focused VA and PT

EAL5 Semi-formally Designed and Tested

- A **high level of independently assured security** in a planned development and a **rigorous development approach** without incurring unreasonable costs attributable to specialist security engineering techniques is required
- Requires more complete and rigorous development artifacts
- Requires increased depth in testing and methodological VA and PT, assuming moderate attack potential

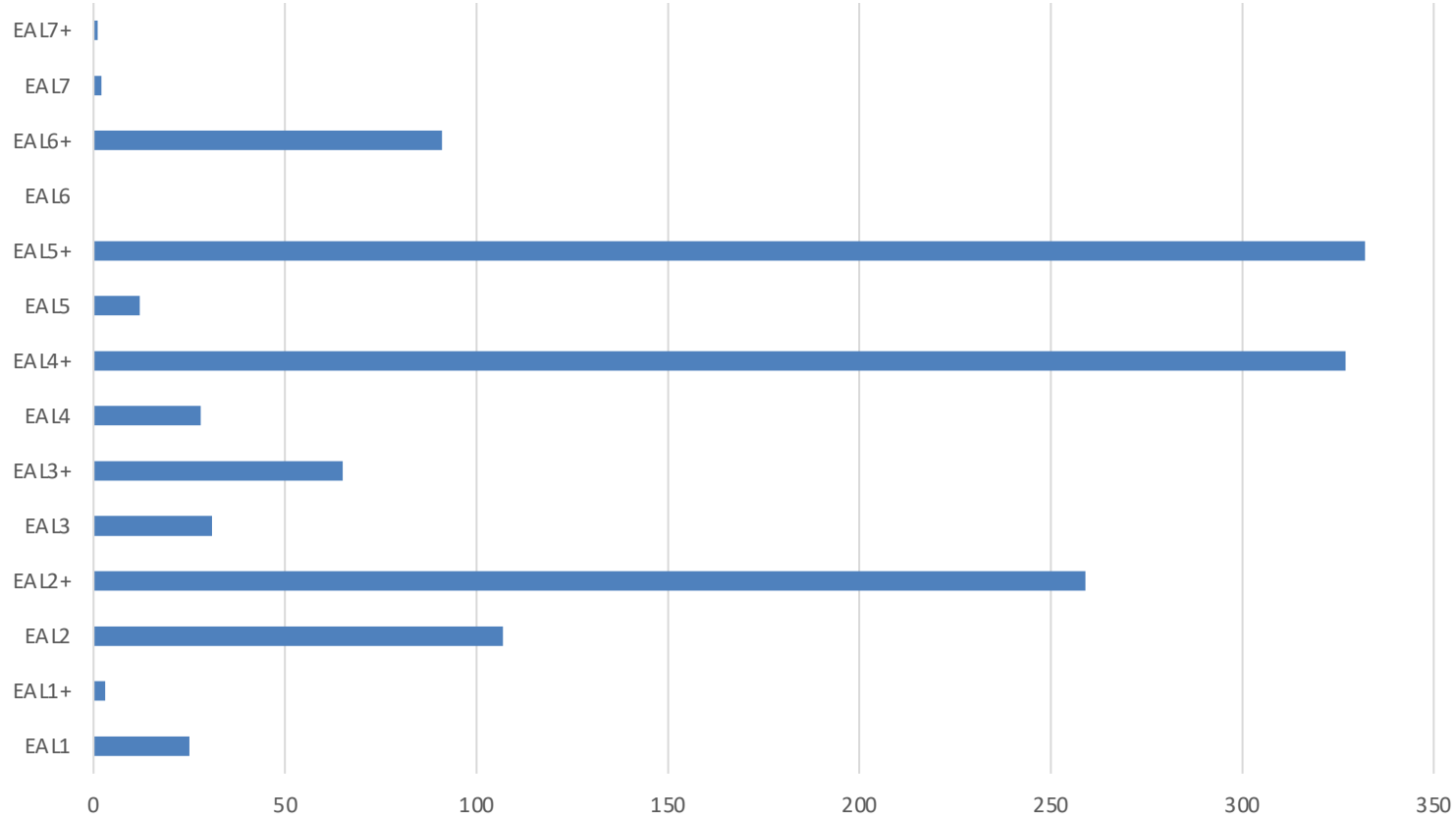
EAL6 Semi-formally Verified Designed and Tested

- **High assurance from application of security engineering techniques to a rigorous development environment** in order to produce a premium TOE for protecting **high value assets** against **significant risks** is required.
- Requires formal security policy models and correspondence demonstration
- Requires methodological VA and PT, assuming high attack potential

EAL7 Formally Verified Designed and Tested

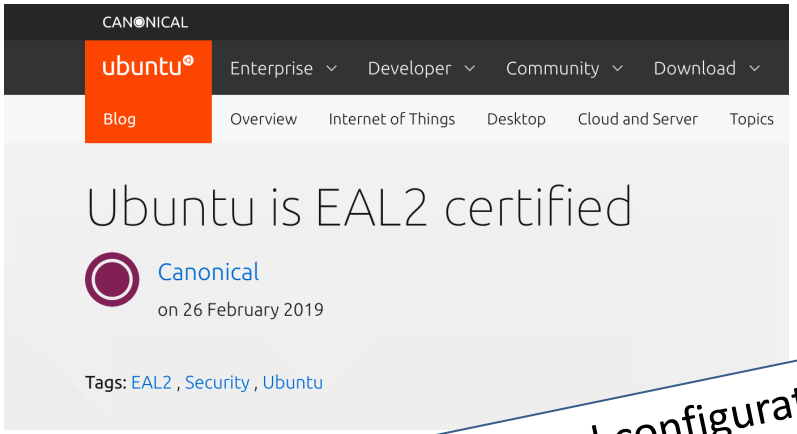
- Applicable to the development of security TOEs for application in **extremely high risk situations** and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

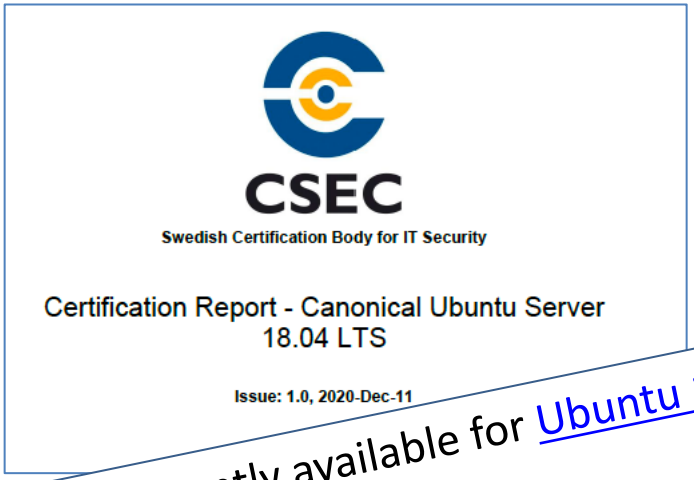
CC Certifications by EAL



From CC web site, 2021

Examples: Operating Systems





Common criteria evaluated configuration is currently available for Ubuntu 16.04.4 LTS (Server) and Ubuntu 18.04.4 LTS (Server).

A Myriad of Other Standards for Specific Application Areas

- ISA/IEC 62433 (Security for Industrial Automation and Control Systems)
- GSMA Network Equipment Security Assurance Scheme
- FIPS 140-2 (Security evaluation of Cryptographic Modules)
- OWASP Application Security Verification Standard (including OWASP Top Ten)
- IoT Security Testing Framework
- ISO-SAE 21434 (Road Vehicles – Cybersecurity Engineering)
- ...