the information security provider

NEW in CC:2022 & CEM:2022

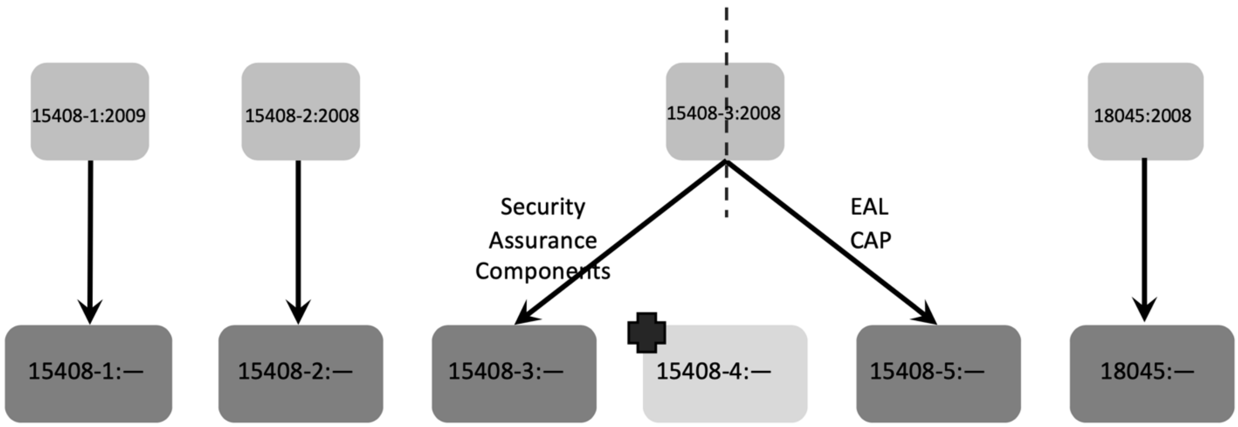
CC:2022 & CEM:2022 (https://www.commoncriteriaportal.org/cc/)
(share the same content with ISO/IEC 15408:2022 and ISO/IEC 18045:2022)

CC 3.1R5 new evaluations NOT accepted after June 30, 2024.

CC:2022 & CEM:2022 Documentation

- Part 1 Introduction
- Part 2 SFRs
- Part 3 SARs
- Part 4 defines methods for the specification of evaluation methods and evaluation activities
- Part 5 includes pre-defined assurance packages
- CEM Evaluation methodology

Structure and mapping from CC 3.1R5 to CC:2022 (i.e., ISO/IEC 15408:2008/2009 (all parts) and ISO/IEC 18045:2008)



Change Overview

New conformance type: Exact Conformance
Added Direct Rationale PPs (and STs) - threats map directly to SFRs and/or security objectives for the Operating Environment
Removed low assurance PPs
New and updated functional requirements
New and updated assurance requirements
New Part 4 defines methods for the specification of evaluation methods and evaluation activities
New Part 5 includes pre-defined assurance packages from CC 3.1R5 Part 3 plus PPA (PP assurance), STA (ST assurance), and COMP (Composite product) as new packages.
Added composition of assurance for

- **layered composition,**
- **network/bi-directional**
- **embedded composition**

Added multi-assurance evaluation which use a PP-Configuration

	Terminology updated
PP Conformance and Approaches	- **Specification-based approach** • **Exact conformance** • ST derives all requirements from the PP or PP-Configuration**.** • ST can only claim exact conformance to one PP**-**Configuration allowed • May use Direct Rationale PPs and STs - **Attack-based approach**: • Strict Conformance (P1, E.3) • Demonstrable Conformance (P1, E.2) • Uses EALs but may use exact conformance if appropriate • May use standard or Direct Rationale PPs and STs - **Multi Assurance** A single TOE may have components needing differing assurance levels, but a global TOE assurance level must include: • conformance with ONLY one multi-assurance PP configuration (P1, 6.3.4.3) - *Multi-assurance PP-Configuration* • SARs in PP-Configuration components are NOT identical (P1,11.3.1)
Part 2 New Functional Requirements	- **FCS_RBG (Random Bit Generation):** this family requires random bit generation to be performed in accordance with selected standards. - **FCS_RNG (Generation of Random Number):** this family defines requirements for the generation of random numbers to use for cryptographic purposes. - **FDP_IRC (Information Retention Control)**: this family defines how to securely manage or delete Information used by the TOE but no longer needed by the TOE. - **FDP_SDC (Stored Data Confidentiality):** this family addresses protection of user data that is stored in areas protected by the TSF. - **FIA_API (Authentication Proof of Identity**): this family allows a TOE to prove its own identity. - **FMT_LIM (Limited Capabilities and Availability)**: this family assures that the TSF provides / restricts capabilities and functions that are required by the TOE’s purpose. - **FPT_EMS (TOE Emanation**): this family covers limiting emanations which may lead to leakage of data. - **FPT_INI (TSF Initialization):** this family sets requirements for the TOE to securely and correctly initialize the TSF. - **FTP_PRO (Trusted Channel Protocol):** this family defines establishment of a trusted channel to transfer the TSF data and user data securely.

Part 3 New and Updated Assurance Requirements	**<u>New Requirements</u>** **PP-Configuration Evaluation** - **ACE_REQ.2 (PP-Module Derived Security Requirements):** Evaluation of the security requirements is required to ensure that they are clear, unambiguous, and well-defined. **Composite Product Evaluation** - **ASE_COMP (Consistency of Composite Product Security Target):** The goal is to determine whether the ST of the composite product does not contradict the ST of the related base component. - **ADV_COMP (Composite Design Compliance):** the goal of this family is determined whether the requirements from the base component to the dependent component are fulfilled in the composite product. - **ALC_COMP (Integration Composition Parts and Consistency Check of Delivery Procedure**s): The goal of this family is to show that the evaluated version of the dependent component has been installed into the evaluated version of the related base component and that delivery processes are compatible. - **ATE_COMP (Composite Functional Testing**): The goal of this family is to determine whether composite product satisfies the functional requirements of its composite product ST. - **AVA_COMP (Composite Vulnerability Assessment):** The goal of this family is to determine the exploitability of flaws/weaknesses in composite product in intended environment. **Life-cycle Support Evaluation** - **ALC_TDA (TOE Development Artifacts):** the goal of this family is to generate artefacts to be used in determining if the development process is a trusted process. **<u>Updated Requirements</u>** - APE_OBJ.1: new element for security objective rationale - APE_REQ.1: new elements for security requirement rationale - ACE_INT.1: new elements for PP-Module Base - ACE_CCL.1: new elements for conformance statement - ACE_MCO.1: new elements for assurance rationale - ACE_CCO.1: TOE overview, consistency rationale, and evaluation methods - ASE_INT.1: multi-assurance ST, evaluation methods and activities identification - ASE_OBJ.1 new element for security objective rationale - ASE_REQ.1 new elements for single and mutli-assurance STs, security rationale, evaluation methods and activities - ADV_SPM.1 Updated to require formal TSF model
Part 4 Framework for EMs/EAs	- Framework for specification of **evaluation methods (EMs)** and **evaluation activities (EAs).** - Specifies methods for definition new evaluation activities can be derived from CEM work units for TOE type or technology type. • A **PP/PP-Module/PP-Configuration** must specify one or more EMs/EAs in its **conformance statement.** • A **package** must specify one or more EMs/EAs in its **security requirement section**. • An **ST** must identify the EMs/EAs used in its **conformance claim.**

	- New EMs/EAs may start either from an SAR or an SFR. Guidelines are provided in P4, 4.2. - Verb usage must align with those define in P1. - EM structure is described in P4, 5 & Figure 3. - EA structure is described in P4, 6.
Part 5 Pre-defined Packages	- Includes EALs 1-7 from CC 3.1R5 - Includes Composed Assurance Package (CAP) from CC 3.1R5 **New Packages:** - **COMP:** Composite product package (P5, 6 & Table 13) - **PPA: PP Assurance packages** (P5, 7) • PPA-DR: PP Assurance Direct rationale PP packages (P5, Table 15) • PPA-STD: PP Assurance Standard packages (P5, Table 16) - **STA: ST Assurance packages** (P5, 8) • STA-DR: ST Assurance Direct rationale packages (P5, Table 18) STA-STD: ST Assurance Standard packages (P5, Table 19)
Composition of Assurance	**Layered composition** - base is independent from dependent component, is not modified by dependent. Dependent component uses base functionality (P1,14). - ***Example*:** a hardware integrated circuit (base component) and a software part on top of it (dependent component). - Supports two evaluation techniques: ACO (CC3.1R5) and COMP (new). - Added SARs for COMP: (P1, Table 3 & P5, Table 13) • ASE_COMP.1 • ADV_COMP.1 • ALC_COMP.1 • ATE_COMP.1 • AVA_COMP.1 - ETR (ETR_COMP) contains ETR of base component and its evaluation. Content is described in P1, 14.3. - May require additional evaluation activities to confirm security assurance of entire product **Network / bi-directional –** a component uses functionality of another component via communication channel (P1,14); - Interdependency if specified and controlled - Both products are separated such that no other channel than the defined one - Both products implement functionality required to protect the communication channel. - ***Example***: An application (component A) using functionality of an external LDAP server (component B) **Embedded** – a component is used as part of the larger component and so interdependency is contained. Usually, no separation and each part can influence the other (P1,14) - ***Example:*** A library or subsystem providing specific security functions as part of a larger product - If separation is specified, ADV_ARC from Part 3 describes requirements.

Modularization	- No modularization, i.e., the entire TOE - Modular: Base PP and PP-Modules (P1,11) - Package family: assurance & functional (P1,9.1) APE, ACE or ASE - Multi-assurance: PP-Configuration) P1, 6.3.4 & P3, 11 Global set of SARs applicable to all PP-Configuration components and each component has own set of SARs.
CEM Additions and Updates	**PP-Configuration evaluation** - ETR for PP-Configuration Evaluation (CEM, 9.4.5.3) - APE_CCL includes PP-Configuration - Added ACE_OBJ.2 **Exact Conformance evaluation** - Added to APE_CCL, ASE_CCL, ACE_CCL, ACE_CCO **Multi-assurance evaluation** - Added to ACE_CCO, ASE_INT, ASE_REQ **Composite product evaluation** - Added ASE_COMP.1, ADV_COMP.1, ALC_COMP.1, ATE_COMP.1, AVA_COMP.1 **Development evaluation** - Added evaluation guidelines for ADV_SPM **Life-cycle evaluation** - Added ALC_TDA **Others** - Added Annex C: Evaluation Techniques and Tools