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)

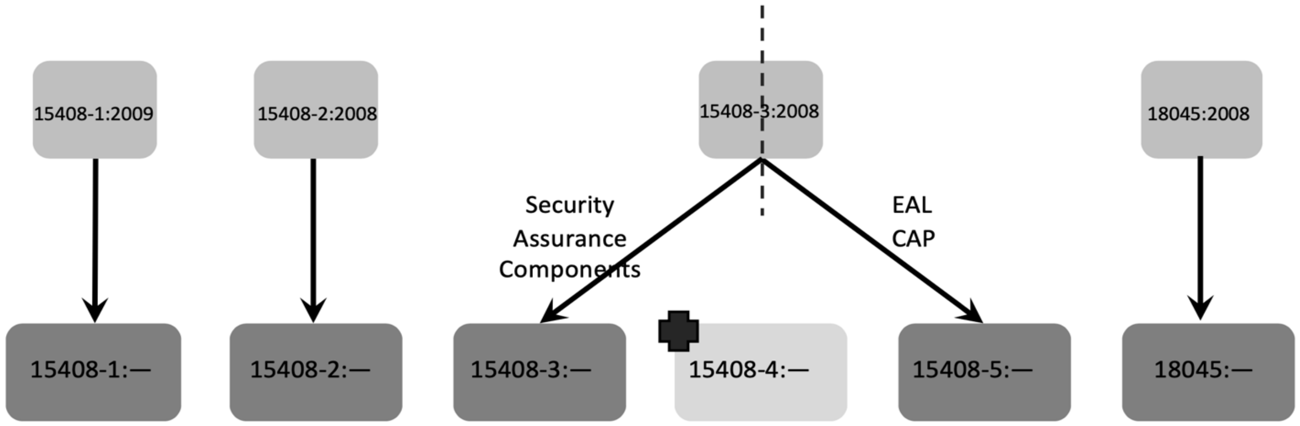
Transition Policy (https://www.commoncriteriaportal.org/cc/)

- **CC 3.1R5 new evaluations NOT accepted after June 30, 2024.**
- **CC 3.1R5 new evaluations with exact conformance NOT accepted after December 31, 2026.**
- **CC:2022 new evaluations using CC3.1R5 PPs NOT accepted after December 31, 2027.**

CC:2022 & CEM:2022 Documentation

- Part 1 Introduction and general model
- Part 2 Security functional components
- Part 3 Security assurance components
- Part 4 Framework for the specification of evaluation methods and activities
- Part 5 Pre-defined packages of security requirements
- CEM Evaluation methodology

Structure and mapping from CC & CEM V3.1R5 (ISO/IEC 15408:2008/2009 (all parts) and ISO/IEC 18045:2008) to CC:2022 & CEM:2022 (ISO/IEC 15408:2022 (all parts) and ISO/IEC 18045:2022)



Change Overview

New conformance type: Exact Conformance
Added Direct Rationale PPs/STs as replacement for low assurance PPs/STs - threats map directly to SFRs and/or security objectives for the Operational Environment
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 EALs and CAPs 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 updates**
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 - **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/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 defines requirements for RBG including: noise sources (external & internal) and seeding (single & multiple) and combined sources and interface for external entities to access RBG output. - **FCS_RNG (Generation of Random Number):** this family defines quality requirements for RNG. - **FDP_IRC (Information Retention Control)**: this family deals with secure management or deletion of data no longer in use. - **FDP_SDC (Stored Data Confidentiality):** this family addresses protection of user data confidentiality while stored in areas protected by the TSF. - **FIA_API (Authentication Proof of Identity**): this family requires the 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 TSF to securely and correctly initialize. - **FTP_PRO (Trusted Channel Protocol):** this family requires a trusted channel for secure transfer of TSF data and user data.
Part 3 New and Updated Assurance Requirements	**New Requirements** **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):** this family ensures that the composite product ST does not contradict the ST of the related base component. - **ADV_COMP (Composite Design Compliance):** this family ensures that requirements from base component to dependent component are fulfilled in the composite product. - **ALC_COMP (Integration Composition Parts and Consistency Check of Delivery Procedure**s): this family ensures 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**): this family ensures that the composite product satisfies the functional requirements of its composite product ST. - **AVA_COMP (Composite Vulnerability Assessment):** this family addresses exploitability of flaws/weaknesses in composite product in the intended environment. **Development Evaluation** - **ADV_SPM (Formal TOE Security Policy Model)**: this family covers the evaluation of formal TOE security policy model. **Life-cycle Support Evaluation** - **ALC_TDA (TOE Development Artifacts):** this family requires artifacts to be used in determining if the development process is trusted. **Updated Requirements** - 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 multi-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 defining new evaluation activities which can be derived from CEM work units for TOE type or TOE technology type. • A **PP/PP-Module/PP-Configuration** must specify one or more EM/EA in its **conformance statement**. • A **package** must specify one or more EM/EA in its **security requirement section**. • An **ST** must identify the EM/EA 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 defined 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 other 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) **Note: this model is not covered in CC:2022.** **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. **Note: this model is not covered in CC:2022.**
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