INTERNET OF TRUST

New concepts and changes in the 2022 edition of the CC standard

Carolina Lavatelli

Toledo, 16th November 2022

In a nutshell

- ISO/IEC 15408:2022 series and ISO/IEC 18045:2022
  - Includes substantial changes and additions for addressing the multiple evaluation paradigms and supporting different user communities
  - Ensures compatibility with currently existing practices and processes.

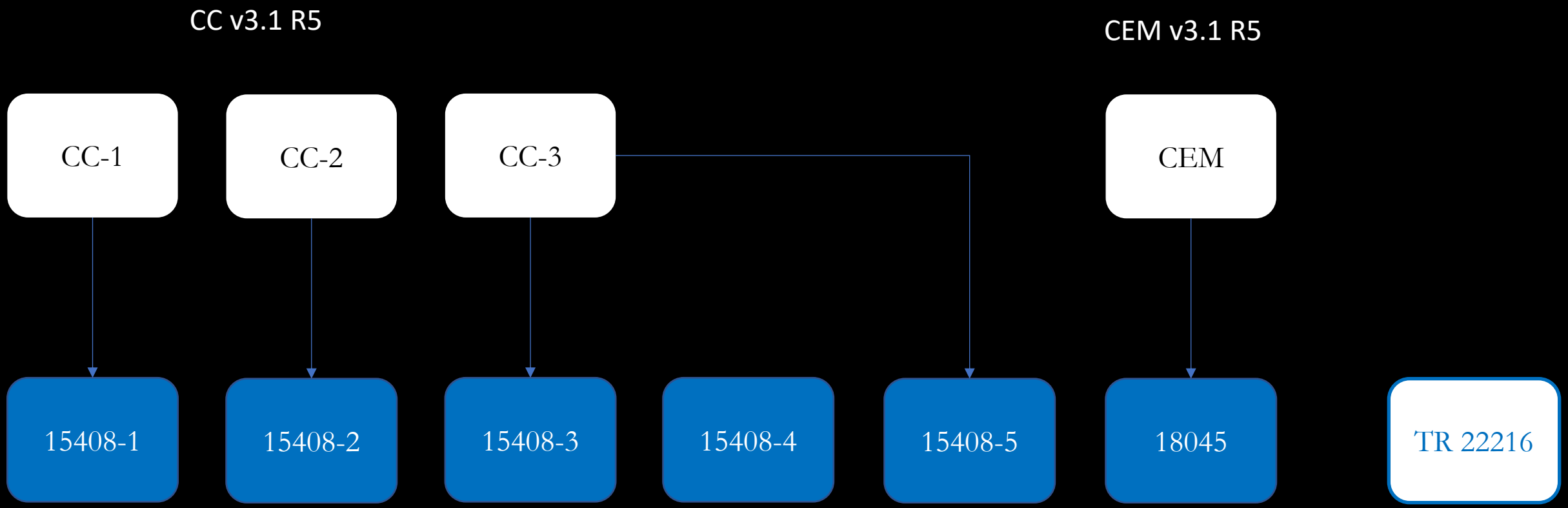
- TR 22216:2022 was developed simultaneously with the new edition to support the transition by
  - Providing an overview of the revision of the CC standard
  - Summarizing the new concepts and related evaluation approaches.

Agenda

Concepts
Impact

- Structure
- Modularity
- Assurance
- Update on SFRs
- Changes in SARs

Structure of the standard



New standard

New Part 4 - Evaluation methods / evaluation activities

Conformance to evaluation methods/evaluation activities can be claimed in packages, PPs, PP-Modules, PP-Configurations and STs.
Derivation rationale required

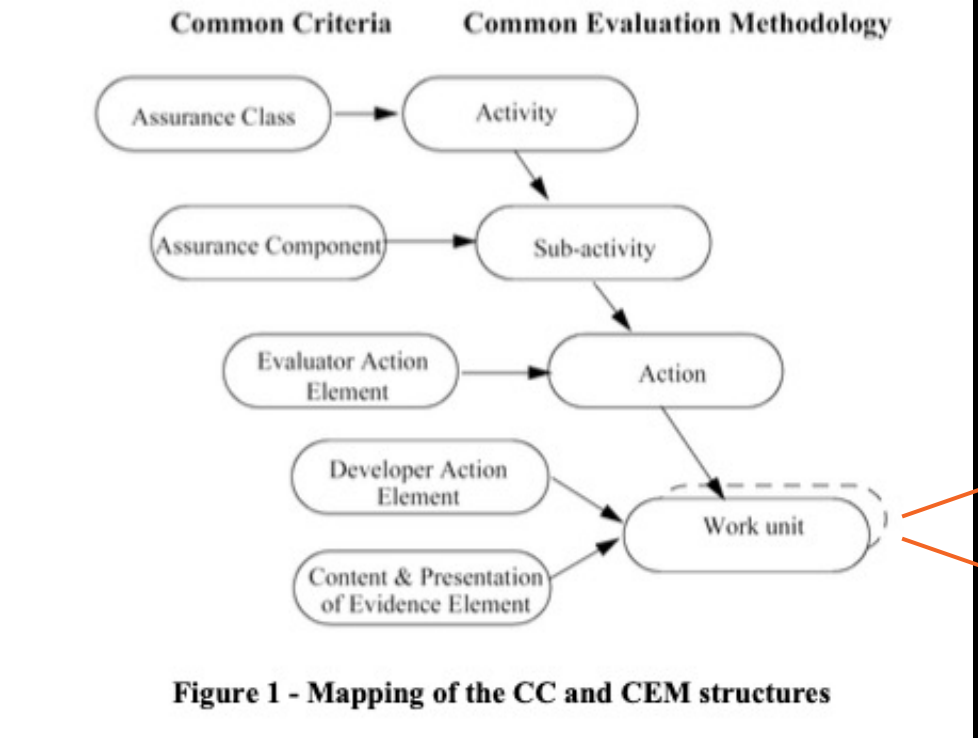
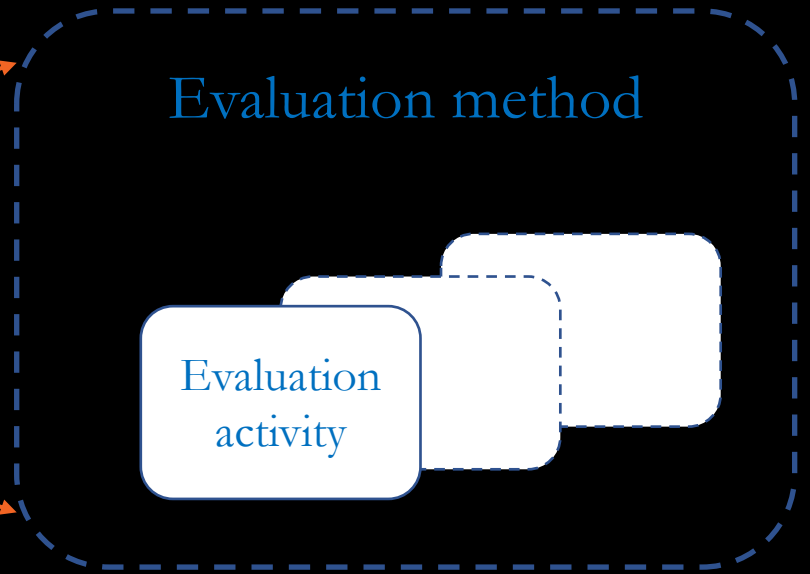


Figure 1 - Mapping of the CC and CEM structures

CC v3.1 R5 & CEM v3.1 R5

derivation n:m

ISO/IEC 15408-4:2022



Modularity

Optional SFRs

Elective type

- The ST author decides to include the SFR or not
- Conformance does not depend on their inclusion in the ST

Conditional type

- Required if the TOE implements the functionality covered by the requirement

Can be used in packages, PPs/PP-Modules.
Optional SFRs may require specific threats/OSPs/security objectives

Functional packages

Include

- Unique package identification (name, version, date, etc.)
- Purpose of the package
- One or more SFRs
- Rationale for the selected SFRs

Optionally

- Dependencies on other functional packages
- Identification of evaluation methods(s) and/or activities
- An SPD and security objectives

Functional packages can be claimed in PPs, PP-Modules and STs.

PP-Modules

Overview

- Unique identifier
- PP-Module Base(s)
- TOE type extends/refines the TOE type of the PP-Module Base(s)
- Optionally, SPD and objectives
- Non-empty set of SFRs and SARs
- Consistency rationale vs PP-Module Base(s)

Enhanced definition

- PP-Module Base may contain other PP-Module(s)
- SARs may be specific to the PP-Module

Used only in conjunction with PP-Configurations

PP-Configurations

Overview

- Unique reference
- TOE type definition
- At least two components:
  - One or more PPs
  - Zero or more PP-Modules
- Consistency rationale for the union of the components' SPD, objectives, SFRs

SAR statement

- Single-assurance
- Multi-assurance
  - Global set of SARs for the TOE
  - Specific sets of SARs for sub-TSFs
- Consistency rationale for SARs

Used only in conjunction with STs.

Update on SFRs

examples

Augmented dependencies

SFR with a selection operation

FDP_ITT.1 Basic internal transfer protection

Dependencies: [FDP_ACC.1 or FDP_IFC.1]

Selection-based dependencies: FCS_COP.1/D …

FDP_ITT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to prevent the [selection: *disclosure, modification, loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

Selection-based SFRs

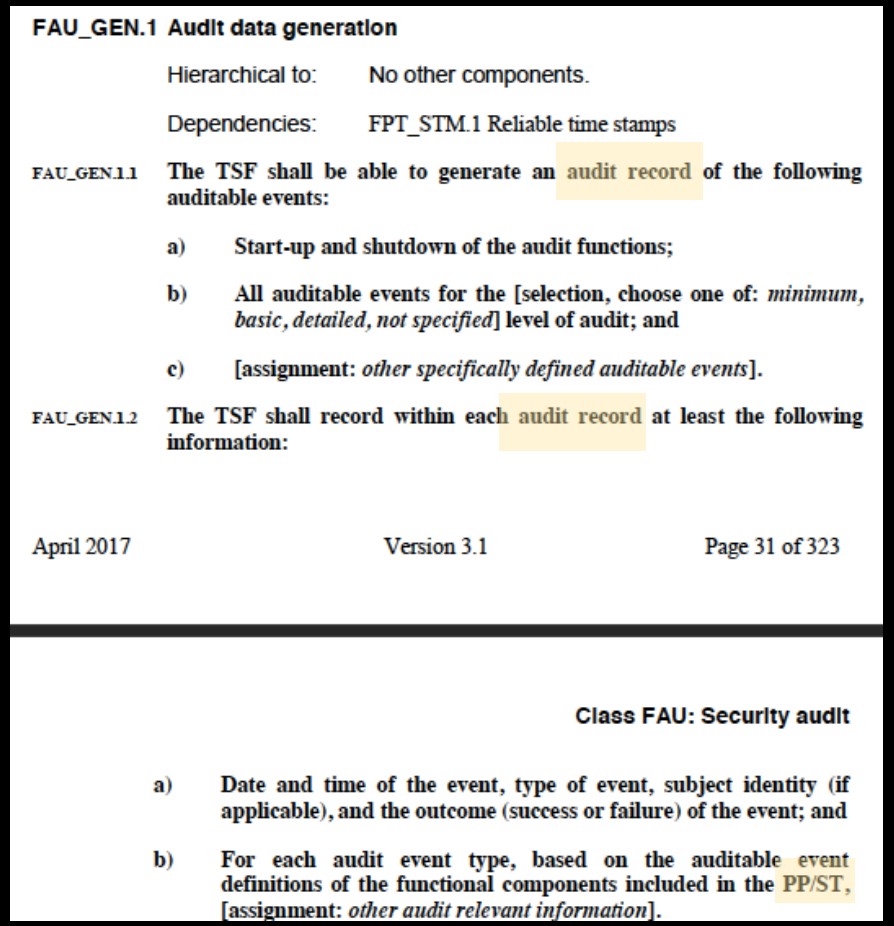
- If *disclosure* is selected:

FCS_COP.1.1/D The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

- If *modification* is selected …

A PP may contain several selection-based SFRs,
only those that correspond to the selected options are included in the ST

FAU_GEN.1 – Updated



FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 **The TSF shall be able to generate an audit record of the following auditable events:**

a) **Start-up and shutdown of the audit functions;**

b) **All auditable events for the [selection, choose one of: *minimum*, *basic*, *detailed*, *not specified*] level of audit; and**

c) **[assignment: *other specifically defined auditable events*].**

FAU_GEN.1.2 **The TSF shall record within each audit record at least the following information:**

April 2017 Version 3.1 Page 31 of 323

Class FAU: Security audit

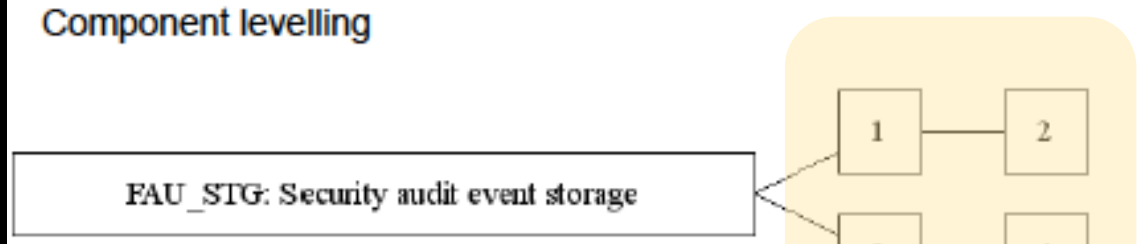
a) **Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and**

b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].**

- Audit record → audit data
- PP/ST → PP, PP-Module, functional package or ST

FAU_STG family - Updated

Component levelling



At FAU_STG.1 Protected audit trail storage, requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

FAU_STG.2 Guarantees of audit data availability, specifies the guarantees that the TSF maintains over the audit data given the occurrence of an undesired condition.

FAU_STG.3 Action in case of possible audit data loss, specifies actions to be taken if a threshold on the audit trail is exceeded.

FAU_STG.4 Prevention of audit data loss, specifies actions in case the audit trail is full.

- FAU_STG.1-4 → FAU_STG.2-5
- New FAU_STG.1 to specify the location where the audit data is stored

FCS class – Updated

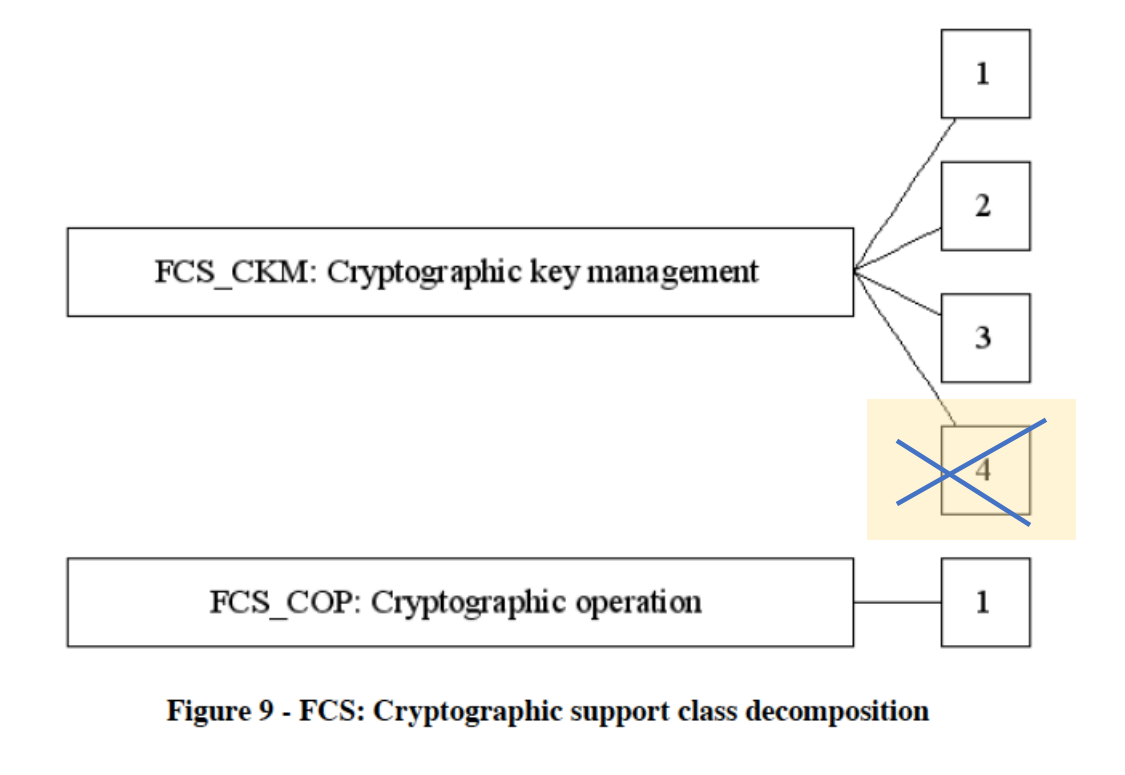


Figure 9 - FCS: Cryptographic support class decomposition

- New FCS_CKM.5 for cryptographic key derivation
- New FCS_CKM.6 for timing and event of cryptographic key destruction
- FCS_CKM.4 for cryptographic key destruction → deprecated

FTP_PRO Trusted channel protocol – New family

- Non-hierarchical components (3)
- Apply to the transfer of TSF data and user data
- FTP_PRO.1 for the specification of the protocol
- FTP_PRO.2 for the key establishment
- FTP_PRO.3 for the specification of the protection that applies to the transferred data

Assurance

Exact conformance

Definition

- An ST conforming to a PP in an exact manner contains:
  - an identical SPD
  - identical security objectives
  - the same SFRs with all the assignments and selections resolved
  - the same SARs and evaluation methods/activites

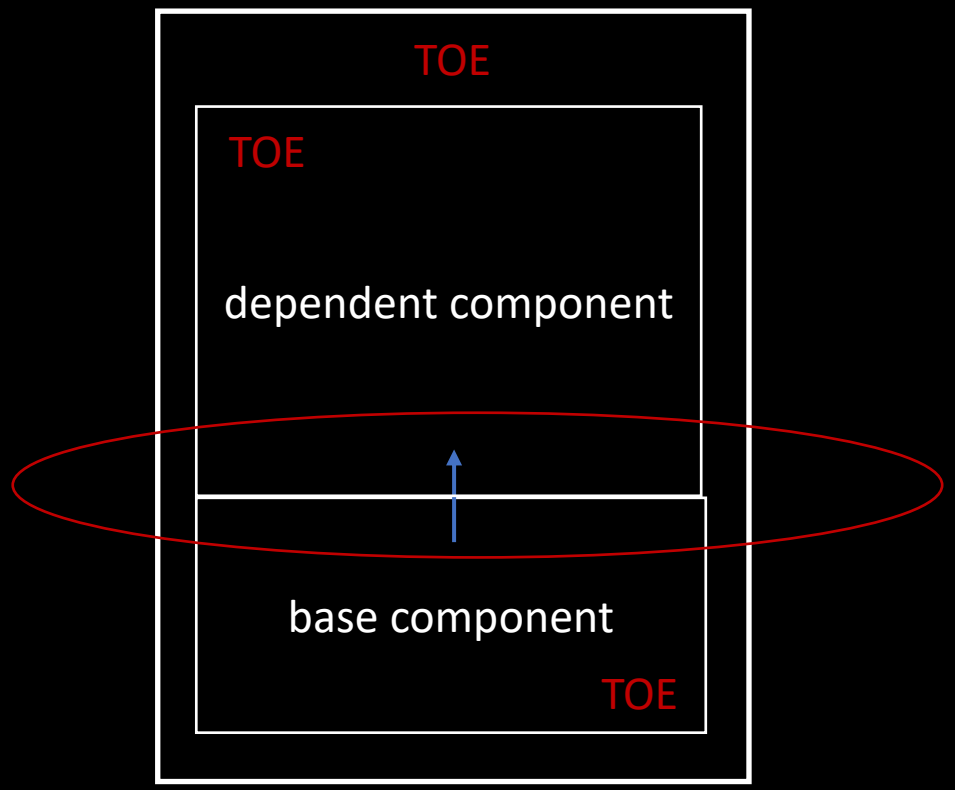
« Allowed-with » statement

- Included in exact conformance PPs and PP-Modules
- Used to define which combinations of PPs and PP-Modules are allowed in a PP-Configuration or in an ST

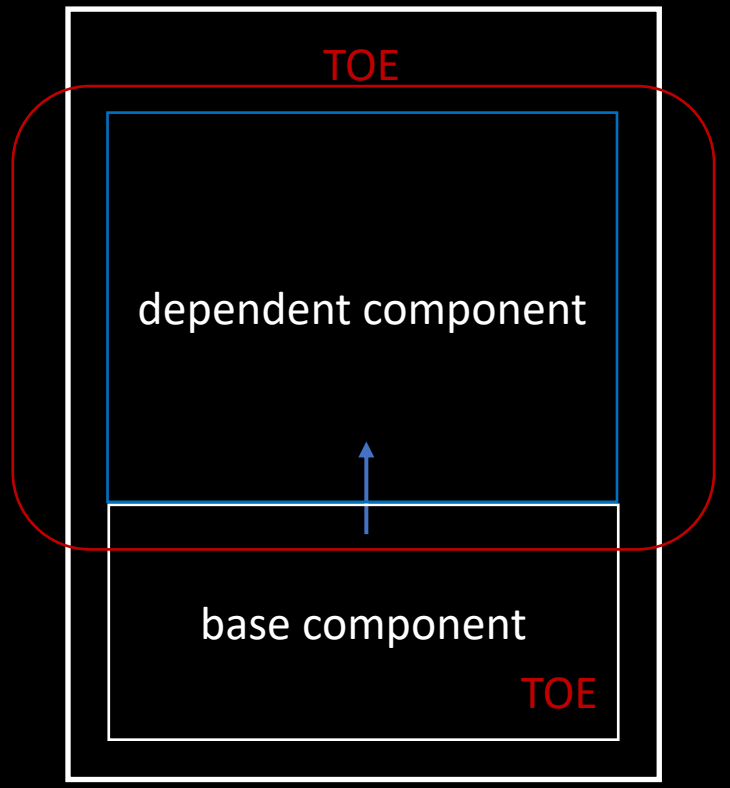
An exact conformance PP cannot claim conformance to another PP
An exact conformance PP cannot be allowed with strict/demonstrable conformance PPs

Evaluation by composition

Composed TOE ACO-based

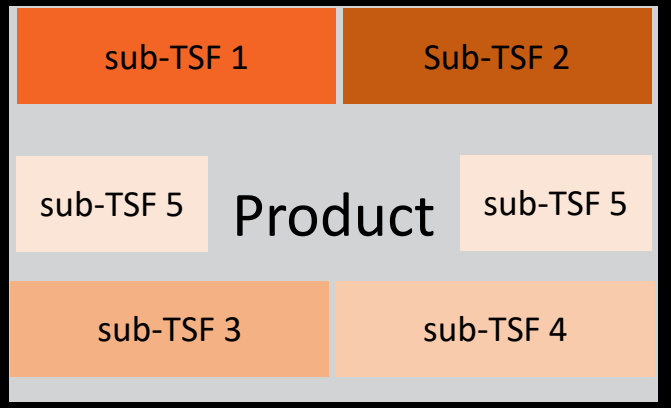


Composite TOE _COMP-based



Multi-assurance evaluation

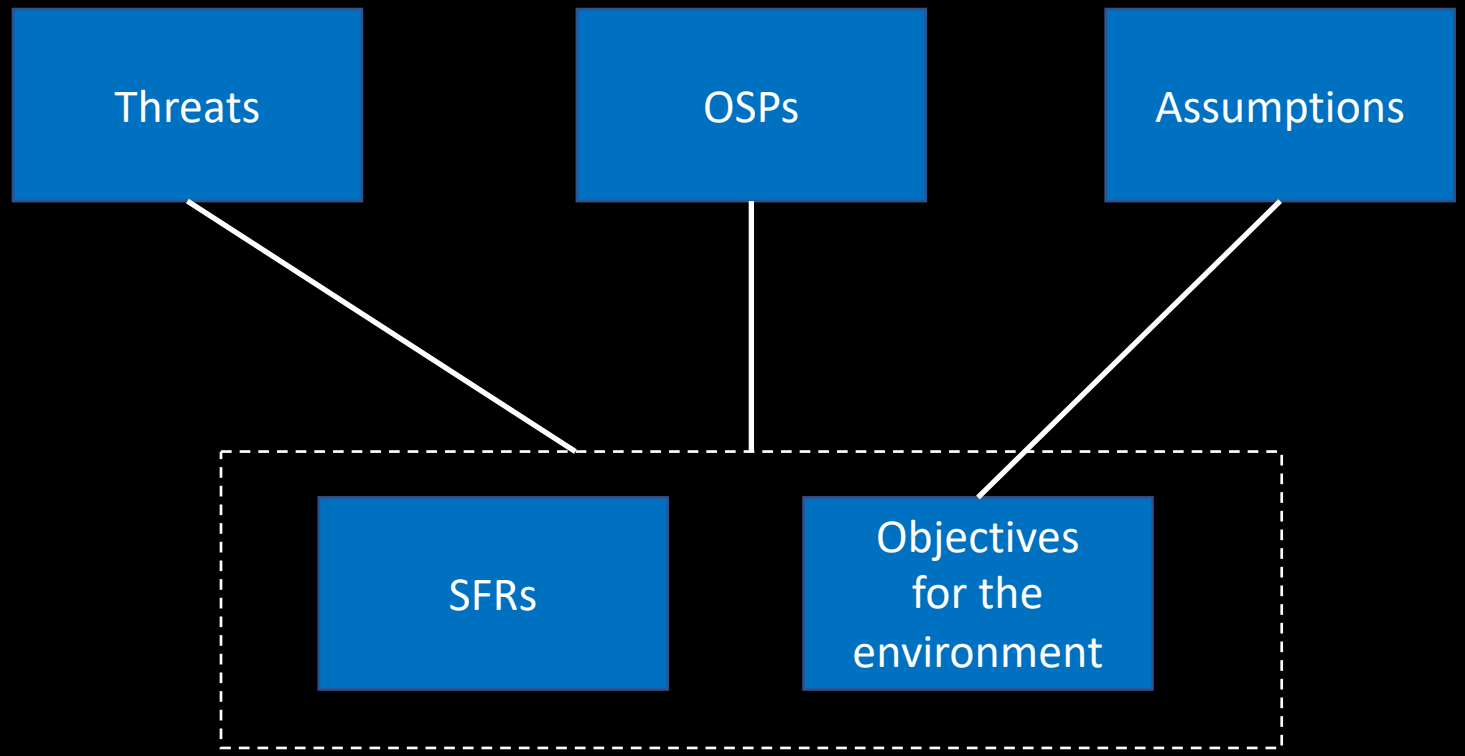
The TSF is split in parts (sub-TSFs).
Each sub-TSF is evaluated against a specific set of assurance requirements.
One global set of assurance requirements holds for the entire TOE.



1 multi-assurance evaluation

Multi-assurance and composition can be used together

Direct rationale approach



Replaces low assurance PPs.

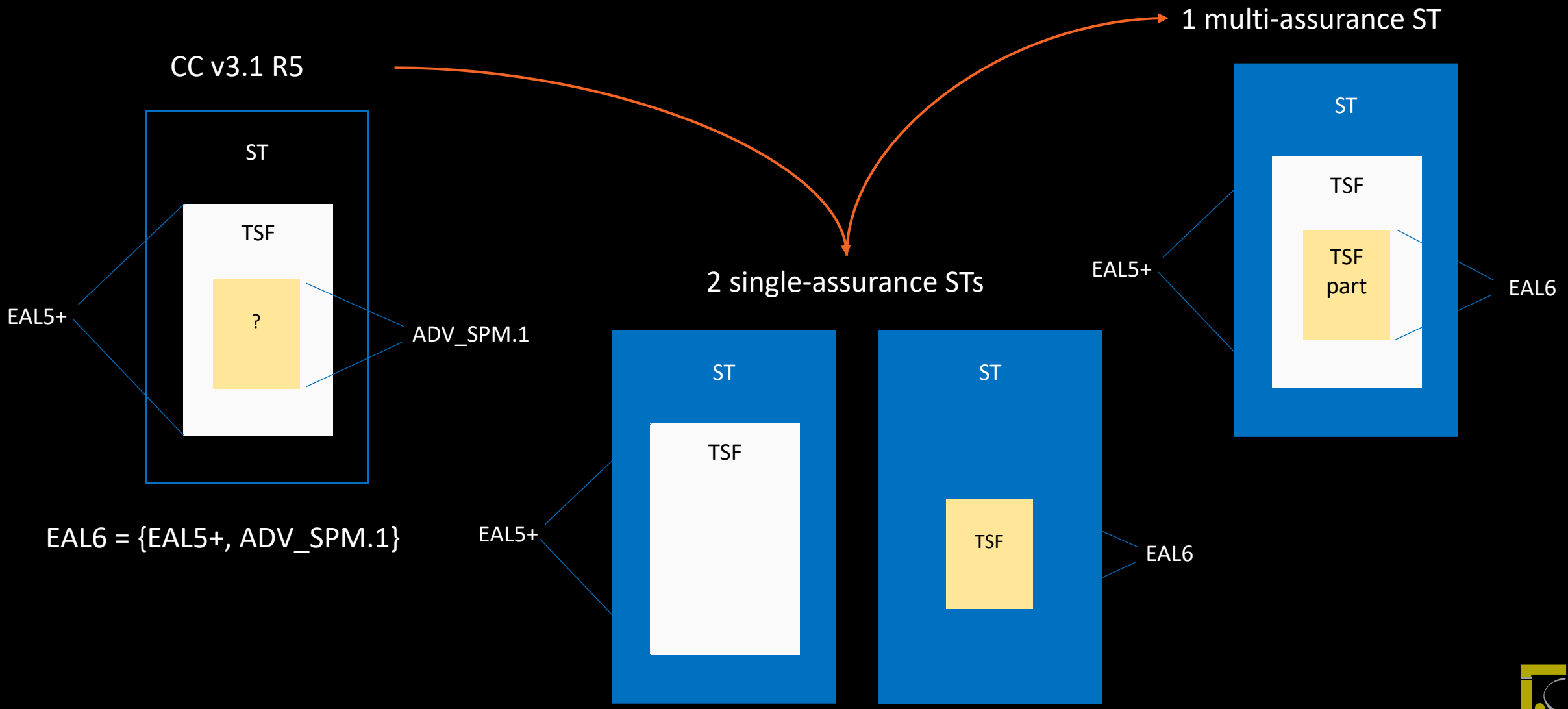
May be used in functional packages, PPs, PP-Modules and STs.

Cannot be combined with the standard approach.

Changes in SARs

examples

ADV_SPM.1 Security policy model



AVA_VAN.2 to .5 update

- The scope of the public vulnerabilities search consists not only of the TOE but also the third-party components and the IT products that the TOE depends on.

Composite evaluation families - addition

- ADV_COMP.1 Composite design compliance
- ALC_COMP.1 Integration of compositon parts and consistency check of delivery procedures
- ASE_COMP.1 Consistency of composite product security target
- ATE_COMP.1 Composite functional testing
- AVA_COMP.1 Composite vulnerability assessment


INTERNET
OF TRUST