Common Criteria Recognition Arrangement
Management Committee

Policies and Procedures

Document Number: *CCMC-2023-04-001*

Date: *April 20th, 2023*

Subject: *Transition Policy to CC:2022 and CEM:2022*

Introduction

The goal of this procedure is to ensure an orderly and timely transition from CC v3.1 to CC:2022. The transition phase started with the publication of CC:2022 Revision 1. This document is intended to give developers, ITSEFs and certification bodies enough time for the necessary adjustments.

This document outlines until when a product or Protection Profile certification based on CC v3.1 R5 may be started or reused. Unless otherwise specified, the current rules outlined in the CCRA and CCRA Supporting Documents for certifications based on CC v3.1 apply during the transition phase [1][2][3,3b][4].

This document also describes in which cases Protection Profiles and evaluation results of a certification based on CC v3.1 may be (re)used in a certification based on CC:2022 and vice versa. These compatibility rules are intended to encourage an early transition to CC:2022.

The following basic rules were adopted by CCMC after publication of CC:2022 in November 2022:

1. CC v3.1 R5 is the last revision of version 3.1 and may optionally be used for evaluations of Products and Protection Profiles starting no later than the 30th of June 2024[1].
2. Security Targets conformant to CC:2022 and based on Protection Profiles certified according to CC v3.1 will be accepted up to the 31st of December 2027.
3. After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date.

This document provides further details.

[1] Note: It is not recommended to perform Protection Profile evaluations on the basis of CC v3.1 after the beginning of 2024, as product evaluations on the basis of CC v3.1 will no longer be possible 6 months later.

Terms and Definitions

For the purposes of this document, CC v3.1 or CC:2022 stands for all revisions of the respective version. A CC v3.1 Protection Profile is therefore a Protection Profile based on any revision of CC v3.1.

Exceptions

A certification body may deviate from the proposed rules in exceptional cases. These exceptions should be rare and indispensable.
Exceptions may be justified, for example, in national projects or procurement regulations.

Product and Protection Profile Certifications

Overview

All statements in this section refer to product or Protection Profile certifications. It is highly recommended to base all future initial certifications on CC:2022.

Initial certifications

New initial certifications based on CC v3.1 R5 may be started until 30th of June 2024. Product certifications based on CC v3.1 R5 against a PP or PP configuration claiming exact conformance may be started until 31st of December 2025. The PP authors must update the PP or PP configuration to CC:2022 as soon as possible, and any new or updated PPs or PP configurations published after 30th of June 2024 must be based on CC:2022.

Re-evaluations and Re-assessments

After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date.

Upward and Backward Compatibility

Overview

The compatibility rules for product certifications are illustrated in Table 1. The re-evaluation, re-assessment or maintenance of a certified product based on CC v3.1 R5 may reuse ALC evaluation results based on CC:2022. Product certifications based on CC:2022 may claim conformance to a Protection Profile based on CC v3.1, reuse ALC evaluations result based on CC v3.1 R5 and use platform certificates based on CC v3.1 R5 in a composite certification. The details are outlined in the following sections.

Compatibility rules for the use of certification results in a product certification

		Protection Profile		ALC Evaluation Results		Platform Certificate	
		v3.1	CC:2022	v3.1 R5	CC:2022	v3.1 R5	CC:2022
Product Certification	v3.1 R5	✓	✗	✓	*	✓	**
	CC:2022	✓	✓	✓	✓	✓	✓

The rows and columns stand for the version of the product certification or the respective certification result.
A checkmark indicates that the combination of the corresponding versions is permitted.

* Only applicable to re-evaluations, re-assessments and maintenance of products.

** Only applicable if the platform certificate do not use concepts introduced in CC:2022 (in particular multi assurance) if not already established by Supporting Documents.

Table 1: Compatibility rules for the use of certification results in a product certification

Protection Profiles

A Security Target based on CC:2022 may claim conformance to a Protection Profile based on CC v3.1 until 31st of December 2027.

The maintainer of a CC v3.1 Protection Profile may transition to CC:2022 in stages by mixing old and new requirements. They may stipulate if and how the security functional components and security assurance components of the CC v3.1 Protection Profile are replaced by their CC:2022 counterparts.

If the PP maintainer has not stipulated transition details the following basic principle should be used as a guideline when resolving the conflicts that arise when a Security Target based on CC:2022 claims conformance to a CC v3.1 Protection Profile:

A Security Target based on CC:2022 should also pass the CC:2022 ASE class if we were to ignore the conformance claim to the CC v3.1 Protection Profile and treat the Security Target as stand-alone.

The following list highlights some of the points where conflicts might arise and gives recommendations on how to resolve them. The certification body should ensure that level of assurance is not reduced when deviating from these recommendations:

1. **Changed families and components**
   Changed families and components should be replaced by their counterparts in CC:2022. The conformance claim rationale should summarize the necessary adjustments to the security functional components and the security assurance components of the Protection Profile based on CC v3.1 to which conformance is being claimed.
2. **Extended components**
   Extended components should be replaced by components in CC:2022 Part 2 or Part 3 if possible. The conformance claim rationale should state if and how the

security functional components and security assurance components of the CC v3.1 Protection Profile were replaced by their CC:2022 counterparts, perhaps using a correspondence table. Furthermore, the conformance claim rationale should demonstrate that the new security requirements are equivalent to the old extended security requirements.

3. **Evaluation methods and activities**
   The assurance elements ASE_CCL.1.13C should also be applied to the Evaluation methods and activities included in any extended security assurance component or supporting document of a (low assurance or collaborative) Protection Profile based on CC v3.1. The Evaluation methods and activities may need to be adapted or augmented to be compliant with the Evaluation methodology defined in CEM:2022.
   In particular, the chapters "Rationale for the Evaluation method/activity" of CC:2022 Part 4 can be used as a guideline, when combining the Evaluation methods and activities of a CC v3.1 Protection Profile with the CEM:2022 Evaluation methodology. In some cases, it might suffice to perform newly added or modified work units in CEM:2022 in addition to the (unchanged) Evaluation methods or activities.

The recommendations in this section apply analogously to Protection Profile Modules and Protection Profile Configurations.

Security target evaluation

The ITSEF shall reflect in their ETR the verification they have performed to assess the relevance of the transposition of a ST according to CC:2022 claiming conformance to a PP CC v3.1 (according to ASE_CCL.1-18, ASE_CCL.1-19 and ASE_CCL.1-20).

ALC Evaluation Results

A product certification based on CC:2022 may reuse ALC evaluation results of a certification based on CC v3.1 R5. The current rules outlined in [4] for the reuse of ALC evaluations results based on CC v3.1 R5 apply.

A re-evaluation, re-assessment or maintenance of a certified product based on CC v3.1 R5 may reuse ALC evaluation results of a certification based on CC:2022.

Composite Certifications

A platform certificate based on CC v3.1 R5 may be used in a composite certification based on CC:2022. The current rules outlined in [2] for the usage of the ETR for Composition for platform certifications based on CC v3.1 R5 apply.
Chain of PPs (PP describing of composite product for example) should be treated in the same way: a platform PP certificate based on CC v3.1 R5 may be used in a PP certification for composite products based on CC:2022.

Supporting documents (SD)

Mandatory supporting documents (SD) written according to CC v3.1 shall be applied by ITSEFs and CBs during CC:2022 evaluations, as far as it is applicable.

References

[1] Assurance Continuity, Version 2.2, September 2021.

[2] Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.

[3] Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, May 2017.

[3b] Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 2.0, 30 September 2021.

[4] Reuse of Evaluation Results and Evidence, Version 1 Final, 26 October 2002.