Joint Interpretation Library

Interpretation on Assurance Continuity

JIL Interpretations on Assurance Continuity for adding the ALC_FLR assurance component from CC part 3 to a baseline certificate

Version 1.0

October 2023

This page is intentionally left blank.

Table of contents

1 Introduction 4

1.1 General Information 4

1.2 Background and Problem Description 4

2 Interpretations 4

3 Abbreviations 6

4 References 6

1 Introduction

1.1 General Information

1 This document provides interpretation and guidance on how to apply the Supporting Document [AC1] and [AC2] with the aim to add ALC_FLR to an existing CC product certificate.

2 The Supporting Documents [AC1] and [AC2] define approaches and processes to maintain a certificate issued under SOGIS-MRA and CCRA in case of changes to the certified product or to product life cycle aspects (ALC). It outlines a separation into Minor Changes or Major Changes in the context of impacting the product assurance statement provided by the baseline certificate issued. A modification categorized as a Major Change results into the need for a reevaluation and formal recertification. A modification categorized as a Minor Change results into an amendment to a certificate issued, e.g. by adding an additional product version of a changed TOE to a certificate or by confirming updated and reevaluated TOE-life cycle aspects. The latter one is currently limited to updates of the ALC assurance components part of the baseline certificate.

1.2 Background and Problem Description

3 A baseline certificate can of course be upgraded with adding Flaw Remediation (ALC_FLR) by a standard re-certification process. Such re-certification includes a full update of the assurance claimed including AVA categorized as assurance continuity with a Major Change.

4 The need came up to add ALC_FLR or a higher level of ALC_FLR to a baseline certificate without performing a full re-certification including AVA. But to add ALC_FLR (or a higher level) by issuing a (maintenance) amendment to a baseline certificate. This can be done after having the relevant ALC_FLR evaluation tasks performed by the evaluation facility (ITSEF) and confirmed by the evaluation authority (certification body).

2 Interpretations

5 [AC1, chp. 3.2] as well as [AC2, chp. 3.2] define a change on the set of claimed assurance requirements as a Major Change.

6 Interpretation:
Adding the CC Part 3 assurance component ALC_FLR.x to the set of assurance components selected in the baseline certificate or increasing the ALC_FLR component level, does normally not impact the product TOE itself, but leads to additional security requirements on the development and production environment and associated security procedures and measures to be evaluated. Therefore, the baseline certificate can be amended after a successful partial evaluation covering the updated or added ALC_FLR part in case the product TOE assurance itself is not impacted. Formally, such ALC_FLR related partial reevaluation will be categorized as Minor Change according to [AC1] and [AC2] and issuing a related Maintenance Addendum is an allowed path.

7 In case the product TOE assurance itself is affected (e.g. because the additional IT environment involved in ALC_FLR affects the IT environment involved in TOE development and/or production and as such the new IT environment breaks TOE

confidentiality and/or integrity) the change is classified as a Major Change resulting in a re-certification.

8 The assumptions as outlined in [AC1, chp. 2.3] and [AC2, chp. 2.3] still apply.

Developer Evidence:

9 The developer has to provide an IAR that outlines the ALC_FLR related change and show how and why the addition of the (a higher level of) ALC_FLR of_FLR change does not impact ALC of the certified TOE. It has to include a developers investigation on interference of the ALC changes and the implementation of the flaw remediation concept with the product TOE itself.

10 The ST needs to be editorially updated according to the ALC change only and provided.

11 ALC related developer evidences have to be provided as usual and required by the CC part 3 requirements applied.

12 An update of the configuration list has to be provided.

13 Site audits have to be supported if specifically required, e.g because the results are outdated or the outcome of ALC_FLR has an impact on other ALC classes that eventually result in having to do site-audit activities.

Subset Evaluation:

14 The documents [AC1, chp. 2.2 o)] and [AC2, chp. 2.2 o)] define a subset evaluation as applicable where minor changes to the TOE include changes to the development environment. A qualified CC evaluation facility identifies those assurance components that are impacted by the changes to the development environment, and re-evaluates only those assurance components in light of the changes, producing a partial ETR.

15 According to[AC1, chp. 2.2 p)] and [AC2, chp. 2.2 p)] a partial ETR is an output from the subset evaluation. It is created by the qualified CC evaluation facility that performed the subset evaluation and provides, for the impacted assurance components, a level of detail that is commensurate with the corresponding sections of the ETR for the original certified TOE.

16 According to [AC1, chp. 2.4.2.1] and [AC2, chp. 2.4.2.1] a qualified evaluation facility performs a subset evaluation, focusing only on those development environment assurance components for which the assurance measures have been modified. The evaluation facility conducts this evaluation in the same way that they would normally perform a CC evaluation for that functionality, and produces a partial ETR that provides sufficient evidence to the evaluation authority that the assurance baseline has been preserved, for those changes to the development environment.

Interpretation and evaluation tasks:

17 The ITSEF has to be the same as the one who has evaluated the ALC part of the baseline certificate.

18 The ITSEF has to perform all evaluation tasks related to the added or changed ALC components. [CC], [CEM] and applicable supporting documents (e.g. [MSSR], ALC-related supporting documents, rules on performing site audits) apply.

19 The scheme rules for ALC evaluation within a product evaluation apply including evaluation plan, evaluation activities including site audits (if required in the specific case) and reporting.

20 The ITSEF has to check that the ST update includes the ALC change only.

21 The ITSEF has to examine that the ALC update has no impact on the product TOE and the product assurance of the baseline certificate and has to confirm this within the reporting of the subset evaluation results.

CB approval:

22 The CB has to be the same as the one who has issued the baseline certificate.

23 The scheme rules on monitoring an CC-evaluation by the CB apply.

24 The partial ETR has to be approved by the CB.

25 The CB provides a Maintenance Addendum to the baseline certificate outlining the scope of the subset evaluation and the technical result, confirms the new ALC assurance claim and states that the Maintenance Result does not include a re-assessment or re-confirmation of AVA.

26 The CB publishes the Maintenance Addendum and updated ST with the related baseline certificate.

3 Abbreviations

CC	Common Criteria
CEM	Common Criteria Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
JIL	Joint Interpretation Library
MSSR	Minimum Site Security Requirements
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
ST	Security Target
TOE	Target Of Evaluation

4 References

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
http://www.commoncriteriaportal.org

CC:2022 R1 "Common Criteria for Information Technology Security Evaluation
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
https://www.commoncriteriaportal.org/cc/

Including the related ISO versions

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
http://www.commoncriteriaportal.org

CEM:2022 R1 Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org/cc/

Including the related ISO versions

[AC1] Joint Interpretation Library, Assurance Continuity, Version 1.1, June 2023, SOGIS-MRA JIWG
https://www.sogis.eu/uk/detail_operation_en.html

[AC2] Assurance Continuity: CCRA Requirements, Version 2023, CCDB
https://www.commoncriteriaportal.org/cc/

[MSSR] Joint Interpretation Library, Minimum Site Security Requirements, version as valid at the point in time of subset evaluation, SOGIS-MRA JIWG
https://www.sogis.eu/uk/supporting_doc_en.html