Joint Interpretation Library

ADV_SPM.1 interpretation for [CC:2022] transition

Version 1.0

May 2024

This page is intentionally left blank.

Table of contents

1 Introduction and scope

1 In [CC:2022], the evaluation of formal models according to ADV_SPM.1 requires the formal modelling of the entire TSF. In the case of a single-assurance Security Target, this means a formal model of the entire TSF as defined in the ST. For a Security Target that is conformant to a multi-assurance PP-Configuration, the parts of the TOE security functionality (sub-TSFs) to which ADV_SPM.1 applies must be entirely modelled. Experience has shown that a formal and comprehensive model (as in the case of a single-assurance Security Target) can be challenging for complex products due to the high efforts associated with development, proofing, evaluation and assessment. Regarding the second case, suitable multi-assurance PP-Configurations are not yet available.

2 To ensure a smooth transition to [CC:2022], the JIWG allows the optional formal modelling of parts of the security functionality of a TOE that are meaningful for assurance purposes and adopts a practical interpretation that is limited in time.

3 For IC products that comply with [PP-0084] and for Java Card open or closed platforms that comply with [PP-0099] or [PP-0101], which have accounted for almost all high-level certifications at EAL6 or EAL7 in the last 20 years, the approach is described in section 2. This note could be extended to other PPs based on the process described in section 3.

4 Section 4 presents the applicability timeline of this note.

5 It should be noted that the present note provides a temporary interpretation to deal with ADV_SPM.1 in [CC:2022]. Developers whose TOEs already fulfil the assurance requirements of ADV_SPM.1 from [CC:2022] would not need then to change or adapt their approach for ADV_SPM.1 formal modelling.

6 Hereby, the multi-assurance approach outlined in section 2.1 is a possible way to address the assessment of a formal model; however this approach is neither mandatory nor it rules out any other approach that is conformant to [CC:2022]. Moreover, the update of the PP should still permit EAL4+ evaluation without any ADV_SPM.1 activity for any sub-TSF. .

2 Interpretation for [PP-0084], [PP-0099] and [PP-0101]

2.1 Intermediate multi-assurance approach

7 For a product that meets one of the [PP-0084], [PP-0099] or [PP-0101] Protection Profiles, it is possible to carry out the ADV_SPM.1 requirements on a subset of the TSF under the following rules:

1) For a [PP-0084]-conformant microcontroller (IC), the minimum scope of formal modelling consists of:
   - The MPU/MMU memory management sub-TSF, if this functionality is present in the product, and
   - The code loading sub-TSF, i.e. Loader 1 and/or Loader 2 in [PP-0084] terminology, if this functionality is present in the product.
2) For a [PP-0099]-conformant or [PP-0101]-conformant Java Card platform, the minimum scope of formal modelling consists of:
   - The application firewall sub-TSF, based on the FIREWALL and JCVM SFPs in [PP-0099] and [PP-0101] terminology, for the protection of the confidentiality and integrity of applications and data.

3) In both cases, IC and Java Card, the formal proofs demonstrate the properties corresponding to the TOE's security objectives which are associated with the sub-TSFs identified in rules 1) and 2).

4) In both cases, IC and Java Card, the scope of the model and the formal proofs may be wider than the minimum scope defined in rules 1) to 3), if it is based on a set of well-defined sub-TSFs as defined in [CC:2022].

5) The Security Target is conformant to [PP-0084], [PP-0099] or [PP-0101] and meets the following conditions:

   a. It unambiguously identifies the modelled sub-TSFs, i.e. the set of SFRs that are modelled, and the proven TOE security objectives, conformant with rules 1) to 4).

   b. It describes the TSF organization in terms of the sub-TSFs.

   c. It defines the global set of SARs for the TOE (and entire TSF) to the EAL defined in the PP or higher, excluding ADV_SPM.1. For [PP-0084], [PP-0099] and [PP-0101] this stands for EAL4+ (ALC_DVS.2, AVA_VAN.5) or higher, excluding ADV_SPM.1.

   d. It defines the set of SARs for the formally modelled sub-TSFs to the global set of SARs augmented with ADV_SPM.1.

6) The evaluation of a Security Target that satisfies rule 5) is performed in accordance with the ASE work units defined in [CEM:2022], whereby the Security Target is modularized as a multi-assurance ST in the sense of [CC:2022][1] and all multi-assurance evaluation activities that are specified for a multi-assurance PP-Configuration are applied analogously to the multi-assurance ST.

   Based on this rule, the evaluator is permitted to assign a PASS verdict to the work units associated with ASE_INT.1.7C and ASE_REQ.2.3C.

   When performing the work units associated to ASE_CCL.1.9C, ASE_CCL.1.10C and ASE_CCL.1.11C the evaluator shall take into account, respectively, the work units associated to ACE_MCO.1.3C, ACE_MCO.1.4C and ACE_MCO.1.5C where the modelled sub-TSF and the applicable PP are the inputs of the evaluation activities, instead of the PP-Module and the PP-Module Base.

7) The TOE evaluation against a Security Target that satisfies rule 5) is performed as follows:

   a. The TOE and its TSF are entirely evaluated by applying all the evaluation sub-activities from [CEM:2022] that are associated with the global SARs defined in the Security Target.

   b. The sub-TSFs' model and proofs, which satisfies the rules 1) to 4), are evaluated by applying the evaluation sub-activities associated with ADV_SPM.1 in [CEM:2022][2] where 'TSF' stands for the modelled sub-TSFs.

8 The evaluator shall consider the interpretation defined through the rules 1) to 7) to establish the verdicts of the evaluation of the Security Target and the TOE.

[1] The set of SARs for the modelled sub-TSF is an augmentation of the global set of SARs, therefore the two sets are consistent.

[2] Note that the evaluation of the global SARs on the sub-TSF is achieved through the evaluation of the global SARs on the TOE and its entire TSF.

2.2 Other approaches

9 Any other approach fulfilling the requirements of ADV_SPM.1 in [CC:2022] remains applicable and is not impacted by the intermediate approach defined in section 2.1.

3 Process for extending the interpretation

10 A PP owner of a PP not already listed in section 2 that is interested in making use of the interpretation depicted in section 2.1 shall propose a PP including the minimum scope of sub-TSFs to be formally modelled according to ADV_SPM.1 from [CC:2022] and shall provide that proposal to the JIL Chair (see French CB email address available on www.sogis.eu).

11 For such PP proposal, it should be considered if and how the modularization into sub-TSFs with their dedicated assurance levels suits the needs of PP users and of further PPs that are linked to the PP in focus.

12 The JIWG will analyse the proposal and update this note (section 2.1) if the proposed minimum scope for formal modelling is considered meaningful for the PP and its TOE type.

13 The JIWG will analyse the proposal to check if it satisfies the rules 1-7, JIWG would also identify possible impacts of the required assurance restructuring on suitability for subsequent composite certifications. For composite certifications with ADV_SPM.1 it has to be taken care that the ADV_SPM.1 related parts of the base component (platform) and of the dependent component (application) fit together regards assurance requirements / levels.

4 Applicability

14 This interpretation will be in place from the date of the commitment of the PP owner to update the PP in a way that it supports the multi assurance approach conformant with this note.

15 The commitment must not be understood as a requirement of the PP-Owner to force the evaluation of sub-TSFs according to ADV_SPM.1 for all TOEs that claim conformance to such updated PP, i.e. the same PP update can provide both an option for the ST author to select either a standard EAL4+/EAL5+ ‘base’ approach or to choose a multi-assurance approach with some sub-TSFs augmented by ADV_SPM.1.

16 The interpretation described in section 2.1 and the support of multi-assurance in STs and PPs is not required by JIL. It is merely a possibility from the JIL point of view to support the interests of PP users in the optional evaluation of Sub-TSFs including a formal security policy model as described in ADV_SPM.1

17 According to the multi-assurance concept, when this interpretation has been successfully applied, the resulting multiple assurance certificate and certification report will clearly identify

- the assurance level reached by the whole TOE,
- and the assurance level including ADV_SPM.1 reached by the identified sub-TSFs.

18 The interpretation depicted in chapter 2.1 is applicable until the updated PP / PP-Configuration is certified or until SOG-IS ceases to produce effects.

5 Abbreviations

CC	Common Criteria
CEM	Common Criteria Evaluation Methodology
JIL	Joint Interpretation Library
PP	Protection Profile
ST	Security Target
SAR	Security Assurance Requirements
TOE	Target Of Evaluation

6 References

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

Including the related ISO versions

[PP-0084] Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, certified under the reference BSI-CC-PP-0084-2014

[PP-0099] Java Card System Protection Profile - Open Configuration, certified under the reference BSI-CC-PP-0099-V2-2020

[PP-0101] Java Card System Protection Profile - Closed Configuration, certified under the reference BSI-CC-PP-0101-V2-2020