EUROPEAN UNION AGENCY
FOR CYBERSECURITY

STATE-OF-THE-ART DOCUMENT

ADV_SPM.1 interpretation for CC:2022 transition

Version 1.1, October 2025

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
22/05/25	V1 draft1	Creation	Version submitted to EsEm Based on JIL-SPM-Interpretation-v1.0 (sogis.eu)
04/07/2025	V1 draft 2	Addresses comments received on draft 1, as agreed during EsEm meeting #12	Version submitted to the EsEm
19/09/2025	V1	No further comments received at EsEm	Version submitted to the ECCG opinion
17/10/2025	V1.1	Clarifications that applicability rules are defined in the EUCC and minor editorial changes	Version endorsed for publication by the ECCG

LEGAL NOTICE

DISCLAIMER

This draft version of the state-of-the-art document is published for information only. Following endorsement by the European Cybersecurity Certification Group (ECCG), it was submitted for inclusion in the list of applicable state-of-the-art documents listed in Annex I of Commission Implementing Regulation (EU) 2024/482.

It received a positive opinion from the ECCG but has not yet been adopted by the Commission via an amendment to Implementing Regulation (EU) 2024/482. State-of-the-art documents will only become applicable and legally binding following their inclusion in the Implementing Regulation and in line with relevant transition rules specified by such Regulation.

Therefore, this document should not yet be considered as final and legally binding. Furthermore, changes might be introduced in state-of-the-art documents in the context of the comitology procedure.

LEGAL NOTICE

This publication is a draft state-of-the-art document as defined in Article 2 point 14 of Commission Implementing Regulation (EU) 2024/482.

This document is established and endorsed by the ECCG in accordance with Article 48 paragraphs 2 and 3 of Commission Implementing Regulation (EU) 2024/482.

This document shall be updated whenever needed to reflect the developments and best practices in the field of multi-assurance evaluations. Updates of this document shall be submitted to the ECCG for endorsement.

This document shall be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes, and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf for the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

CONTACT

Feedback or questions related to this document can be sent via the European Union Cybersecurity Certification website (https://certification.enisa.europa.eu/index_en)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

This state-of-the-art document provides requirements on the application of ADV_SPM.1 in the transition from Common Criteria version 3.1 (CC3.1) to Common Criteria version 2022 (CC:2022).

In CC:2022, the evaluation of formal models according to ADV_SPM.1 requires the formal modelling of the entire TOE security functionality (TSF). In the case of a single-assurance Security Target (ST), this means a formal model of the entire TSF as defined in the ST. For a ST 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 ST) 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.

To ensure a smooth transition from CC3.1 to CC:2022, this state-of-the-art document establishes a practical interpretation allowing the optional formal modelling of parts of the security functionality of a TOE that are meaningful for assurance purposes.

For IC products that comply with PP-0084 and Java Card open or closed platforms that comply with PP-0099 or PP-0101, which have accounted for most of the high assurance certifications (EAL6 or EAL7) relying on formal models in the last 20 years, the approach is described in section 2. Section 3 presents the outcome of this interpretation.

It should be noted that the present document provides a temporary interpretation to deal with ADV_SPM.1 in CC:2022 when claiming conformance to a CC:3.1 PP. 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.

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. It is merely a possibility to support the interests of PP users in the optional evaluation of the formal models of some sub-TSFs as defined in ADV_SPM.1. Moreover, the updated PP should still permit to perform PP-conformant evaluations without ADV_SPM.1 activity for any sub-TSF.

1.2 REFERENCES

1.2.1 Normative references

Regulations

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)[1], as amended by Implementing Regulation 2024/3144

Standards

Note: Unless otherwise specified, the versions of the Common Criteria and Common Evaluation Methodology standards defined in Article 2 of the EUCC scheme apply.

[1] Available at http://data.europa.eu/eli/reg_impl/2024/482/oj

CC:2022:

ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model.

ISO/IEC 15408-2:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components.

ISO/IEC 15408-3:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components.

ISO/IEC 15408-4:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities

ISO/IEC 15408-5:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements.

CEM:2022:

ISO/IEC 18045:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation.

EUCC state-of-the-art documents[2]

Note: Unless otherwise specified, the latest version of referenced state-of-the-art documents applies.

Composite product evaluation and certification for CC:2022, version 1 (draft), February 2025.

1.2.2 Informative references

[PP-0084] Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014

[PP-0099] Java Card System - Open Configuration, (V3.1), BSI-CC-PP-0099-V2-2020.

[PP-0101] Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020.

1.3 ACRONYMS AND DEFINITIONS

1.3.1 Acronyms

CC	Common Criteria for Information Technology Security Evaluation as defined the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined the EUCC
EAL	Evaluation Assurance Level
EC	European Commission
ENISA	European Union Agency for Cybersecurity
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
PP	Protection Profile
SAR	Security Assurance Requirement
SOG-IS	Senior Officials Group – Information Systems Security
TSF	TOE security functionality
ST	Security Target
TOE	Target of evaluation

1.3.2 Definitions

[2] Available at https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

The definitions used under Article 2 of Regulation (EU) 2019/881 (Cybersecurity Act) and under Article 2 of the Implementing Regulation (EU) 2024/482 apply to this document.

2. INTERPRETATION FOR PP-0084, PP-0099 AND PP-0101

2.1 INTERMEDIATE MULTI-ASSURANCE APPROACH

For a product that meets one of the PP-0084, PP-0099 or PP-0101 Protection Profiles as referenced in 1.2.2, it shall be 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:
   a. the MPU/MMU memory management sub-TSF, if this functionality is present in the product, and;
   b. 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:
   a. 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 ST 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 organisation 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 augmented by ALC_DVS.2 and AVA_VAN.5, or higher, and 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 an ST that satisfies rule 5) is performed in accordance with the ASE work units defined in CEM:2022, whereby the ST is modularised as a multi-assurance ST in the sense of CC:2022[3] 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 shall be 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,

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

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 an ST 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 ST;

   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:20224 where 'TSF' stands for the modelled sub-TSFs.

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

2.2 OTHER APPROACHES

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.

[4] 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.

3. OUTCOME OF THIS INTERPRETATION

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

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

For each of the PPs listed in section 2.1, this interpretation shall remain in effect **in accordance with the rules defined in Annex I to the EUCC.**

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu