EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

GUIDELINES

Evaluation methodology for Product series

Version 1, July 2025

DOCUMENT HISTORY

Date	Version	Modification	Author’s comments
21/05/25	V1 draft 1	Creation	Based on JIL-Evaluation-methodology-for-product-series-v1-0.pdf
08/07/25	V1	Editorial update for publication	

LEGAL NOTICE

LEGAL NOTICE

This publication is a guidelines document supporting Commission Implementing Regulation (EU) 2024/482.

This document is established with the support of the European Cybersecurity Certification Group (ECCG) sub-group on EUCC maintenance and review (EsEm) and may be updated whenever needed to reflect the developments and best practices in the field of the evaluation of product series.

This document should 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)](https://certification.enisa.europa.eu/index_en)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

The EUCC scheme and the Common Criteria (CC) methodology allow naturally developers to apply for the evaluation and certification of single ICT products.

In some cases, developers may wish to apply for the evaluation and certification of Product series as defined in paragraph 1.3.2 instead of a single product: these guidelines provide recommendations to developers, Information Technology Security Evaluation Facilities (ITSEFs) and Certification Bodies (CBs) as how to handle an EUCC evaluation and certification, when the Target of Evaluation (TOE) is a Product series.

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.

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.

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

1.3 ACRONYMS AND DEFINITIONS

1.3.1 Acronyms

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

CAB	Conformity assessment body
CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation as defined the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined the EUCC
CSA	Cybersecurity Act
DAR	Differential Analysis Report
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation technical report
EU	European Union
ICT	Information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information technology
ITSEF	Information Technology Security Evaluation Facility
SFR	Security functional requirement
SOG-IS	Senior Officials Group – Information Systems Security
ST	Security target
TOE	Target of evaluation
TSFI	TOE security function interfaces
TRR	Testing reuse rationale

1.3.2 Definitions

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. The following definitions also apply to this document.

Product series: A Product series is a set of products by a developer, built upon the same functional basis, in order to address the same security needs. However, their design, hardware, firmware or software may vary from a product to another. These differences may come from a different underlying hardware or platform or may consist in additional functions due to different requirements in scope or performance.

Reference TOE: The product chosen by the developer (or sponsor) as the most representative of the Product series. This Reference target of evaluation (TOE) will be the main target of the evaluation activities.

Other declared products: All the products that belong to the Product series, except the Reference TOE.

Reference evaluation: The results of the evaluation activities for the Reference TOE.

2. PREREQUISITES

2.1 DIFFERENTIAL ANALYSIS REPORT (DAR)

In order to distinguish between different products within a Product series, the developer should produce a document called Differential Analysis Report (DAR). This document should identify the shared features and differences between the considered products, and how these differences may affect the security objectives and SFRs declared in an applicable Security Target.

The content of the DAR could take inspiration from the Impact Analysis Report as defined in paragraph 2 of EUCC Annex IV.3 “Changes to a certified ICT product”.

2.2 SELECTION OF THE REFERENCE TOE

The developer should select, within the Product series, a Reference TOE.

If no single TOE is representative of the whole series, the developer should either chose several Reference TOEs in order to cover the whole series, or restrict the scope of the series.

2.3 TESTING REUSE RATIONALE (TRR)

The developer should produce a rationale describing its strategy for the reuse of test results of the Reference TOE(s), based upon the DAR. This Testing Reuse Rationale (TRR) should justify how a sample of tests could be executed on a sample of products, in order to ascertain the security behavior of all the products within the Product series declared in the applicable Security Target.

The TRR should also contain the rationale for the selection of the Reference TOE(s).

2.4 DELIVERABLES

The developer should provide to the ITSEF the whole Product series, i.e., the Reference TOE and the other declared products. At any moment during the evaluation, the ITSEF may require the access to any product belonging to the series.

The ITSEF should independently decide which product(s) is needed to execute a given test and justify this choice in the Evaluation technical report (ETR).

3. EVALUATION METHODOLOGY

3.1 STEP 1: APPLYING TO AN EVALUATION FOR A PRODUCT SERIES

The developer should submit a request for evaluation, along with the elements required by Chapter 2.

The ITSEF should establish an evaluation plan specifying the expected workload for the ATE and AVA evaluation activities, based upon the TRR provided by the developer. The contents of the DAR should also be taken into account by the ITSEF in order to define the workload for the ADV, AGD and ALC evaluation activities.

Remark: The ITSEF and Certification Body may challenge the selection of Reference TOE(s) at any moment during the evaluation, and may require additional workload to be allocated, in order to perform further tests on the Product series.
In that case, the developer may restrict the scope of the evaluation to the Reference TOE(s) only.

3.2 STEP 2: REFERENCE EVALUATION

The ITSEF should perform the evaluation activities on the Reference TOE(s) according to the selected evaluation criteria, and according to the targeted evaluation assurance level.

3.3 STEP 3: EVALUATION OF THE OTHER DECLARED PRODUCTS

In addition to the Reference evaluation, the ITSEF should evaluate the following requirements:

ASE
The ITSEF should ensure that the Security Target clearly identifies the Product series, and the products that belong to this series.

ADV
The ITSEF should ensure that the DAR is complete and correct.

AGD
The ITSEF should ensure that the whole Product series is addressed by the AGD_OPE and AGD_PRE classes.

ALC
The ITSEF should ensure that each product within the Product series is uniquely and unambiguously identified.

The ITSEF should check that all Product series components and any unique identifiers declared in the security target and associated with them, are consistent with the identifier(s) assigned to the Product series evaluated in work units related to ALC_CMC.x.1C and the configuration list evaluated in work units related to ALC_CMS.x.2C.

The ITSEF should verify whether the lifecycle of the Reference TOE(s) also applies to the Other declared products. Any deviation in the lifecycle should require additional evaluation activities.

ATE FUN, COV, DPT
Based upon the developer rationale, the ITSEF should ensure that the Reference TOE(s) selected by the developer is (are) representative of the whole Product series.

Based upon the DAR and the TRR, the ITSEF should ensure all the SFR enforcing subsystems, modules and TSFIs that may differ between different products have been separately tested and that all the Product series meets the security objectives declared in the applicable security target.

The ITSEF should eventually give a formal agreement on the TRR.

ATE_IND
The ITSEF should perform this activity according to the TRR.

However, the ITSEF may perform additional tests, which are not required by the TRR. Depending on the results of these tests, the evaluator may question the relevance and completeness of the DAR.

AVA
The ITSEF should perform this activity according to the TRR, in order to optimise the penetration testing workload.

The ITSEF should perform dedicated tests on the Other declared products if the DAR or the results in the ATE or ADV evaluation activities suggests a possible difference in behavior between different products.

3.4 STEP 4: CERTIFICATION

The CB should issue a single certificate for the whole Product series, so as to avoid issuing multiple certificates. The certificate should identify all the products within the Product series.

The certification report should include, in addition to the elements required for the certification of the Reference TOE as defined in Annex V of EUCC:

- an identification of the products within the Product series;
- a reference to the documents provided by the developer for the Product series evaluation as defined in Chapter 2;
- the ETR established to cover specific activities defined in 3.3.

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