EUROPEAN UNION AGENCY
FOR CYBERSECURITY


# EUCC SCHEME

## STATE-OF-THE-ART DOCUMENT

Hardware assessment in EN 419221-5 (HSM PP): interpretation of the FPT_PHP requirements

Version 1, February 2025

# DOCUMENT HISTORY

| Date | Version | Modification | Author's comments |
|---|---|---|---|
| September 2024 | 1.0 draft 1 | Creation | Based on Guidance for Hardware assessment in EN 419221-5 (HSM PP) |
| February 2025 | V1 | Version based on the EUCC maintenance subgroup feedback | Endorsed for publication on 11/03/2025 by the ECCG |

# LEGAL NOTICE

## LEGAL NOTICE

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

This document is endorsed by the European Cybersecurity Certification Group (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 TSP Cryptographic Modules certification. 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 of 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

EN 419221-5 version 1.0 “Protection Profiles for TSP Cryptographic Modules, Part 5: Cryptographic Module for Trust Services” contains requirements on FPT_PHP, which are refined in the PP towards the ISO/IEC 19790:2012 standard.

The endorsement notice in the current version of ISO/IEC 19790:2020 states that the 2012 version of the standard has been kept without any modifications in the text. When applying the protection profile (PP), the security target shall refer to ISO/IEC 19790:2020, and this change does not have any impact on the requirements and interpretations as they are in the PP.

This document provides to developers and evaluators additional established interpretations of the FPT_PHP requirements and their application notes in the evaluation and certification of products according to this PP, considering the current active version ISO/IEC 19790:2020 of the standard.

## 1.2 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

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

**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.

EN 419221-5] CEN, Protection Profiles for TSP Cryptographic Modules, Part 5: Cryptographic Module for Trust Services, EN 419221-5, version 1.0.

[ISO/IEC 19790:2020] Information technology – security techniques – security requirements for cryptographic modules (ISO/IEC 19790:2012 (Cor. 2015-11) IDT)[2].

## 1.3 ACRONYMS

| | |
|---|---|
| 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 |
| EAL | Evaluation Assurance Level |
| EC | European Commission |
| ENISA | European Union Agency for Cybersecurity |

[1] Available at http://data.europa.eu/eli/reg_impl/2024/482/oj
[2] The text of ISO/IEC 19790:2012 has been approved by CEN as EN ISO/IEC 19790:2020 without modification

| | |
|---|---|
| ETR | Evaluation technical report |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| HSM | Hardware Security Module |
| ICT | Information and communications technology |
| IT | Information technology |
| ITSEF | Information Technology Security Evaluation Facility |
| PP | Protection profile |
| SFR | Security functional requirement |
| ST | Security target |
| TOE | Target of evaluation |

# 2. APPLICABLE BACKGROUND TO FPT_PHP REQUIREMENTS

EN 419221-5 is a Protection Profile (PP) conformant to Common Criteria version 3.1 revision 4, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security. The security assurance requirements of this Protection Profile are based on EAL4 augmented by AVA_VAN.5 “Advanced methodical vulnerability analysis”.

EN 419221-5 defines the attack surface to be considered for hardware attacks on the hardware security module (HSM):

- the HSM has to be deployed in a protected environment - this is formulated by the objective for the environment OE.ENV, which requires that the target of evaluation (TOE) shall operate in a protected environment that limits physical access to the TOE to authorised administrators;
- according to OE.ENV, the administrator shall install the TOE software and hardware environment (including client applications) in a secure state protecting against tampering attacks, emanation attacks and software changes;
- the Trusted Path between a local application and the TOE may be implemented by the secure environment (see FTP_TRP.1/Local, application note 29 of the PP) - the administrator installs the secure environment and thus can have plain access to the authentication data of the user, if he/she actively listens to the channel;
- according to paragraph 4.4.1.1 Authorisation of the PP, acting as an administrator is an authorisation to carry out management activities on the TOE, but not to use keys nor to be able to access their values.

Therefore, the physical access to the TOE during operation is limited to authorised administrators that fulfil security-relevant tasks during installation and operation. Nevertheless, the TOE has to protect against administrator access to or use of keys.

Since physical access is limited to authorised administrators, it is considered that the FPT_PHP requirements are fulfilled if the requirements of section 7.7.2 Physical security general requirements and section 7.7.3 Physical security requirements for each physical security embodiment in ISO/IEC 19790:2020 for security level 3 are met.

EN 419221-5 states the above-mentioned precisions in application notes for FPT_PHP.1 and FPT_PHP.3, and adds a CEM refinement for AVA_VAN.5 Advanced methodical vulnerability analysis. Therefore, no additional vulnerability analysis for the physical attacks is needed, and the standards provide direct guidance on testing, that has to be performed to gain the required assurance on the hardware protection of the TOE.

# 3. IMPACT ON TESTING AGAINST FPT_PHP REQUIREMENTS

## 3.1 GENERAL TESTING INTERPRETATIONS

For the evaluation of ICT products against EN 419221-5:

- the design assessment shall be performed to verify that;
  - the administrator cannot gain access to the plaintext user keys;
  - the FPT_PHP requirements are implemented;
- testing shall be executed against the requirements from ISO/IEC 19790:2020 based on the assurance claims made in FPT_PHP.1 and FPT_PHP.3 and shall demonstrate related expected results are met (the undermentioned section “Detailed testing interpretations” indicates which requirements are applicable for the different types of cryptographic modules);
- as OE.ENV ensures that only authorised administrators can reach access to the physical instance of the TOE, physical attacks by other persons shall be considered as non-applicable;
- the security measures according to ISO/IEC 19790:2020, section 7.7.2 and 7.7.3, security level 3 shall be considered as sufficient for authorised administrators.

## 3.2 DETAILED TESTING INTERPRETATIONS

ISO/IEC 19790:2020 states in “7.7.2 Physical security general requirements“ for security level 3 that requirements 07.01 – 07.28 have to be fulfilled.

Section “7.7.3 Physical security requirements for each physical security embodiment“ states that in addition to the general physical security requirements specified in 7.7.2 the following requirements have to be fulfilled for security level 3:

a) for single-chip cryptographic modules: requirements 07.34 – 07.38;

b) for multiple-chip embedded cryptographic modules: requirements 07.43 – 07.51;

c) for multiple-chip standalone cryptographic modules: requirements 07.60 – 07.65.

As stated above, an authorised administrator shall not have access to /nor use keys and shall not be able to access their values unless he/she is able to demonstrate he/she is the key owner. Hence all kinds of administrator accesses shall be taken into account by the ITSEF, including logical access via interfaces which are only accessible by administrators.
The interfaces shall be tested according the “Common Evaluation Manual (CEM)” which includes functional testing, vulnerability analysis and penetration testing.

## 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