Joint Interpretation Library

Guidance for Hardware assessment in EN 419221-5 (HSM PP)

Version 1.0
May 2021

This page is intentionally left blank

Table of contents

1 Summary

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

2 This document constitutes a guidance for the interpretation of the FPT_PHP requirements and their application notes in the evaluation and certification of products according to this PP.

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

2 Background of the FPT_PHP requirements

4 [EN 419221-5] is a Protection Profile conformant to Common Criteria version 3.1 revision 4. The security assurance requirements of this Protection Profile are EAL4 augmented by AVA_VAN.5 “Advanced methodical vulnerability analysis”.

5 The authors of [EN 419221-5] had the challenge to define a proper attack surface for the hardware attacks on the HSM:

- HSMs, which are intended for [EN 419221-5], have to be deployed in a protected environment. This is formulated by the objective for the environment OE.ENV, which requires that the TOE shall operate in a protected environment that limits physical access to the TOE to authorized administrators.
- According OE.ENV the administrator shall install 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). The administrator installs the secure environment and thus can have plain access to the authentication data of the user, if he would actively listen to the channel.
- According to 4.4.1.1 authorization to act as an administrator is an authorization to carry out management activities on the TOE, but not to *use* keys or to be able to access their values.

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

7 Since physical access is limited to authorized administrators, it was decided 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 19790:2012 for security level 3 are met.

8 [EN 419221-5] states the above-mentioned in application notes for FPT_PHP.1 and FPT_PHP.3 plus a CEM refinement for AVA_VAN.5 Advanced methodical vulnerability analysis. Therefore, this section in the standard does not require a vulnerability analysis for the physical attacks, but provides direct guidance on testing, that has to be performed to gain the required assurance on the hardware protection of the TOE.

3 Evaluation Assessment of the FPT_PHP requirements

9 In the Common Criteria evaluation against [EN 419221-5]:

- The design assessment will be performed to verify that
  - the administrator cannot gain access to the plaintext user keys,
  - the FPT_PHP requirements are implemented.
- Testing is executed against the requirements from ISO/IEC 19790:2012 based on the assurance claims made in FPT_PHP.1 and FPT_PHP.3 and must show the expected results. The undermentioned section "Regarding the Testing" names which requirements are applicable for the different types of cryptographic modules.
- As OE.ENV ensures that only authorized administrators can reach access to the physical instance of the TOE attacks by other persons are non-applicable. For authorized administrators the security measures according to ISO/IEC 19790:2012, section 7.7.2 and 7.7.3, security level 3 are sufficient.

3.1 Regarding the Testing

10 ISO/IEC 19790:2012 states in „7.7.2 Physical security general requirements" for security level 3 that the there listed requirements 07.01 – 07.28 have to be fulfilled.

11 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:

- For single-chip cryptographic modules:
  requirements 07.34 - 07.38
- For multiple-chip embedded cryptographic modules:
  requirements 07.43 - 07.51
- For multiple-chip standalone cryptographic modules:
  requirements 07.60 – 07.65

12 Please note: The above described testing refers to FPT_PHP requirements only. The physical protection shall prevent physical accesses of authorized administrators.

13 As stated above, an authorized administrator shall not have access to use keys or to be able to access their values unless the administrator is able to demonstrate authorization as key owner.

14 Hence all kinds of administrator accesses have to be taken into account by the ITSEF, including logical accesses via interfaces which are only accessible by administrators.

15 The interfaces have to be tested according the “Common Evaluation Manual (CEM)” which includes e.g. functional testing, vulnerability analysis and penetration testing.