Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative Protection Profile Module for Server Applications

Foreword

This is a Supporting Document, intended to complement the Common Criteria (CC) version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

Supporting Documents may be "Guidance Documents", that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or "Mandatory Technical Documents", whose application is mandatory for evaluations whose scope is covered by that of the Supporting Document. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

This Supporting Document has been developed by the iTC for Application Software iTC and is designed to be used to support the evaluations of TOEs against the cPP identified in Section 1.1, “Technology Area and Scope of Supporting Document”.

Acknowledgements

This Supporting Document was developed by the iTC for Application Software international Technical Community with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

Revision History

Table 1. Revision history

Version	Date	Description
1.0	2022-04-06	Initial Release
1.0e	2024-02-15	Incorporated feedback received following initial release.

General Purpose

See Section 1.1, “Technology Area and Scope of Supporting Document”.

Field of special use

This Supporting Document applies to the evaluation of TOEs claiming conformance with the collaborative PP-Module for Server Applications.

Table of Contents

1. Introduction

1.1. Technology Area and Scope of Supporting Document

This Supporting Document (SD) is mandatory for evaluations of products that claim conformance to any of the following cPP(s):

- collaborative PP-Module for Server Applications, Version 1.1, 2022-08-16

Although Evaluation Activities (EAs) are defined mainly for the evaluator to follow, the definitions in this SD aim to provide a common understanding for developers, evaluators and users as to what aspects of the TOE are tested in an evaluation against Collaborative Protection Profile for Application Software, and to what depth the testing is carried out. This common understanding in turn contributes to the goal of ensuring that evaluations against Collaborative Protection Profile for Application Software achieve comparable, transparent and repeatable results. In general, the definition of EAs will also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of SFRs, and may identify particular requirements for the content of Security Targets (STs) (especially the TOE Summary Specification (TSS)), AGD guidance, tests, and possibly required supplementary information (e.g. *any examples, such as for entropy analysis or cryptographic key architecture*).

1.2. Structure of the Document

EAs can be defined for both SFRs and SARs. These are defined in separate sections of this SD.

If any EA cannot be successfully completed in an evaluation then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an EA may be modified or deemed not applicable for a particular TOE, but this must be agreed with the Certification Body for the evaluation.

In general, if all EAs (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a 'pass'. To reach a 'fail' verdict when the EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

Similarly, at the more granular level of Assurance Components, if the Evaluation Activities for an Assurance Component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the Assurance Component is a 'pass'. To reach a 'fail' verdict for the Assurance Component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

2. Evaluation Activities for SFRs

2.1. Structure of EAs

All EAs for SFRs defined in this Section include the following items to keep consistency among EAs.

1. Objective of the EA

   Objective defines the goal of the EA. Assessment Strategy describes how the evaluator can achieve this goal in more detail and Pass/Fail criteria defines how the evaluator can determine whether the goal is achieved or not.

2. Dependency

   Where the EA depends on completion of another EA then the dependency and the other EA is also identified here.

3. Tool types required to perform the EA

   If performing the EA requires any tool types in order to complete the EA then these tool types are defined here.

4. Required input from the developer or other entities

   Additional detail is specified here regarding the required format and content of the inputs to the EA.

5. Assessment Strategy

   Assessment Strategy provides guidance and details on how to perform the EA. It includes, as appropriate to the content of the EA;

   a. How to assess the input from the developer or other entities for completeness with respect to the EA
   b. How to make use of any tool types required (potentially including guidance for the calibration or setup of the tools)
   c. Guidance on the steps for performing the EA

6. Pass/Fail criteria

   The evaluator uses these criteria to determine whether the EA has demonstrated that the TOE has met the relevant requirement or that it has failed to meet the relevant requirement.

7. Requirements for reporting

   Specific reporting requirements that support transparency and reproducibility of the Pass/Fail judgement are defined here.

2.2. Justification for EAs for SFRs

EAs in this SD provide specific or more detailed guidance to evaluate the *type of* system, however, it is the CEM work units based on which the evaluator shall perform evaluations.

This Section explains how EAs for SFRs are derived from the particular CEM work units identified in Assessment Strategy to show the consistency and compatibility between the CEM work units and EAs in this SD.

Assessment Strategy for ASE_TSS requires the evaluator to examine that the TSS provides sufficient design descriptions and its verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary information will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the cPP.

Assessment Strategy for AGD_OPE/ADV_FSP requires the evaluator to examine that the AGD guidance provides sufficient information for the administrators/users as it pertains to SFRs, its verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Assessment Strategy for ATE_IND requires the evaluator to conduct testing that the iTC has determined that those testing of the TOE in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that derive those EAs are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.3. Security Management (FMT)

2.3.1. Supported Configuration Mechanism (FMT_MEC_EXT)

2.3.1.1. FMT_MEC_EXT.1.1/Server

2.3.1.1.1. TSS

The evaluator shall review the TSS to identify where the application's configuration data is stored. The evaluator shall also verify that the TSS identifies who has read and write access to the configuration data.

2.3.1.1.2. Operational Guidance

No activities specified.

2.3.1.1.3. Test

The evaluator shall run the following tests:

- Test 1: The evaluator shall verify that the access rules for the configuration files align with the read and write access identified in the TSS.

- Test 2: The evaluator shall run the application while monitoring it with the following platform specific tools and make changes to its configuration. The evaluator shall verify that the tool logs show corresponding changes to the locations identified in the TSS for storage of configuration data. The following platform specific tools and procedures must be used:
  - Windows: SystInternal tool ProcMon
    - The evaluator shall run the application while monitoring it with the SysInternal tool ProcMon and make changes to its configuration. The evaluator shall verify that ProcMon logs show corresponding changes to the locations identified in the TSS for storage of configuration data.
  - Linux or macOS: strace (or equivalent utility)
    - The evaluator shall run the application while monitoring it with the utility strace. The evaluator shall make security-related changes to its configuration. The evaluator shall verify that strace logs corresponding changes to configuration files that reside in /etc (for system-specific configuration) or in the user's home directory (for user-specific configuration).

2.3.2. Specification of Management Functions (FMT_SMF)

2.3.2.1. FMT_SMF.1.1/Server

2.3.2.1.1. TSS

No activities specified.

2.3.2.1.2. Operational Guidance

The evaluator shall verify that every management function specified in the SFR is described in the operational guidance. If multiple management interfaces are supported, the guidance documentation must describe which interfaces may be used to perform the management functions.

2.3.2.1.3. Test

The evaluator shall perform the following test:

- Test 1: The evaluator shall test the application's ability to provide each management function by configuring the application and testing each function specified. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed. Each function should be tested on each management interface on which the functionality is supported.

2.4. Protection of the TSF (FPT)

2.4.1. Anti-Exploitation Capabilities (FPT_AEX_EXT)

2.4.1.1. FPT_AEX_EXT.2.1/Server

2.4.1.1.1. TSS

No activities specified.

2.4.1.1.2. Operational Guidance

No activities specified.

2.4.1.1.3. Test

The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests:

- Test 1: [conditional] If the application is being tested on Windows, the evaluator shall ensure that the application can run successfully with Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The following link describes how to enable Exploit Protection, https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection.
- Test 2: [conditional] If the application is being tested on Linux, the evaluator shall ensure that the application can successfully run on a system with SELinux (or equivalent platform vendor recommended security features) enabled and enforcing.
- Test 3: [conditional] If the application is being tested on macOS, the evaluator shall ensure that the application can successfully run on a system without disabling System Integrity Protection (SIP).

3. Evaluation Activities for Selection-Based Requirements

This PP-Module does not define selection-based requirements. Component participation control is addressed by the Agent module when a PP-Configuration includes Agent Applications. Protection of data transmitted between TOE components is addressed by FTP_DIT_EXT.1 in the base cPP. Certificate validation and certificate path processing requirements are addressed by the X.509 package selected through the base cPP, where applicable.

4. Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the App PP base to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The Collaborative Protection Profile for Application Software includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

5. References

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2022-11-002, CC:2022, Revision 1, November 2022.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2022-11-003, CC:2022, Revision 1, November 2022.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
- [ERR] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-02-001, Version 1.0, 1 February 2024
- [cPP] Collaborative Protection Profile for Application Software, Version 1.1, 2022-08-16