Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative Protection Profile Module for Agent 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 Agent 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 Agent 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, 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. Communication (FCO)

2.3.1. Component Registration Channel Definition (FCO_CPC_EXT.1/Agent)

2.3.1.1. FCO_CPC_EXT.1/Agent

2.3.1.1.1. TSS

The evaluator shall examine the TSS to confirm it:

- Describes the method by which a Security Administrator enables and disables communications between pairs of TOE components
- Describes the relevant details according to the type of channel in the main selection made in FCO_CPC_EXT.1.2/Agent:
  - First type: the TSS identifies the relevant SFR iteration, if present, that specifies the channel used.
  - Second type: the TSS describes details of the channel and the mechanisms that it uses.

2.3.1.1.2. Operational Guidance

The evaluator shall examine the guidance documentation to confirm that it contains instructions for enabling and disabling communications with any individual TOE components. The evaluator shall confirm that the method of disabling is such that all other TOE components can be prevented from communicating with the TOE component that is being removed from the TOE (preventing the remaining TOE components from either attempting to initiate communications to the disabled component, or from responding to communications from the disabled component).

The evaluator shall examine the guidance documentation to confirm that it includes recovery instructions should a connection be unintentionally broken during the registration process.

If the TOE uses a registration channel for registering components to the TOE (i.e. where the ST author selects a channel protected according to FTP_DIT_EXT.1 in FCO_CPC_EXT.1.2/Agent) then the evaluator shall examine the Preparative Procedures to confirm that they:

- describe the security characteristics of the registration channel (e.g. the protocol, keys and authentication data on which it is based).
- identify any dependencies between the configuration of the registration channel and the security of the subsequent intra-TOE communications (e.g. where AES-256 intra-TOE communications depend on transmitting 256 bit keys between TOE components and therefore rely on the registration channel being configured to use an equivalent key length).
- identify any aspects of the channel can be modified by the operational environment in order to improve the channel security and shall describe how this modification can be achieved (e.g. generating a new key pair, or replacing a default public key certificate).

As background for the examination of the registration channel description, it is noted that the requirements above are intended to ensure that administrators can make an accurate judgement of any risks that arise from the default registration process. Examples would be the use of self-signed certificates (i.e. certificates that are not chained to an external or local Certification Authority, manufacturer-issued certificates (where control over aspects such as revocation, or which devices are issued with recognised certificates, is outside the control of the operational environment), use of generic/non-unique keys (e.g. where the same key is present on more than one instance of a device), or well-known keys (i.e. where the confidentiality of the keys is not intended to be strongly protected – note that this does not imply there is a positive action or intention to publicise the keys).

2.3.1.1.3. Test

The evaluator shall carry out the following tests:

- Test 1.1: The evaluator shall confirm that an Agent application that is not currently a member of the TOE cannot communicate with any TOE component until the non-member entity is enabled by a Security Administrator for each of the non-equivalent TOE components with which it is required to communicate.
- Test 1.2: The evaluator shall confirm that after enablement, an Agent application can communicate only with the TOE component that it has been enabled for. This includes testing that the enabled communication is successful for the enabled pair, and that communication remains unsuccessful with any other TOE component for which communication has not been explicitly enabled.

Some TOEs may set up the registration channel before the enablement step is carried out, but in such a case the channel must not allow communications until after the enablement step has been completed.

The evaluator shall repeat Tests 1.1 and 1.2 for each different type of enablement process that can be used in the TOE.

- Test 2: The evaluator shall separately disable each TOE component in turn and ensure that the other TOE components cannot then communicate with the disabled component, whether by attempting to initiate communications with the disabled component or by responding to communication attempts from the disabled component.
- Test 3: The evaluator shall carry out the following tests according to those that apply to the values of the selection made in the ST for FCO_CPC_EXT.1.2/Agent.

    - If the ST uses the first type of communication channel in the selection in FCO_CPC_EXT.1.2/Agent then the evaluator tests the channel via the Evaluation Activities for FTP_DIT_EXT.1 in the base cPP.
    - If the ST uses the 'no channel' selection, then no test is required.
- Test 4 [conditional]: If *a channel protected according to FTP_DIT_EXT.1* is selected in FCO_CPC_EXT.1.2/Agent, the evaluator shall perform one of the following tests, according to the TOE characteristics identified in its TSS and operational guidance:
    - If the registration channel is not subsequently used for communication between TOE components, then the evaluator shall confirm that the registration channel can no longer be used after the registration process has completed, by attempting to use the channel to communicate with each of the endpoints after registration has completed.
    - If the registration channel is subsequently used for communication between TOE components then the evaluator shall confirm that any aspects identified in the operational guidance as necessary to meet the requirements for a steady-state inter-component channel (as in FTP_DIT_EXT.1) can indeed be carried out (e.g. there might be a requirement to replace the default key pair and/or public key certificate).

2.4. Protection of the TSF (FPT)

This PP-Module does not define FPT_ITT evaluation activities. Protection of data transmitted between TOE components is addressed by FTP_DIT_EXT.1 in the base cPP.

3. Evaluation Activities for Selection-Based Requirements

This PP-Module does not define selection-based requirements. 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

Appendix A: Rationales

A.1. SFR Dependencies Analysis

The dependencies between SFRs implemented by the TOE are addressed as shown in the base PP.