collaborative PP-Module for Agent Applications

Acknowledgements

This collaborative Protection Profile Module (PP-Module) was developed by the iTC for Application Software international Technical Community (iTC) also known as AppSW-iTC 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	2023-02-15	Incorporated feedback received following initial release.

Table of Contents

Preface

This module is part of a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is software applications. Under this cPP software applications can be categorized under the following broad categories:

1. Enterprise Agent Applications

This cPP-Module is to be used against which all of the above categories of software applications may be evaluated. In addition there are PP-Modules that may be applicable based on the category of application.

In addition to the above categories there are large number of applications (Desktop and Mobile) that fall under “Consumer-grade” category. While such applications could be evaluated under the Application Software cPP, it is not the intention of this iTC to specifically address this category. The iTC doesn’t believe the consumer grade app ecosystem would support the historical cost and timelines associated with a Common Criteria evaluation.

Objectives of Document

This document presents the Common Criteria (CC) collaborative Protection Profile Module (PP-Module) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for Enterprise Agent Applications. The Evaluation activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this PP-Module, are described in [SD].

Scope of Document

The scope of the PP-Module within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation. In particular, a PP-Module defines the IT security requirements of a generic type of TOE and specifies the functional security measures to be offered by that TOE to meet stated requirements [[CC1], Section B.14].

Intended Readership

The target audiences of this PP-Module are developers, CC consumers, system integrators, evaluators and schemes.

Although the PP-Module and SD may contain minor editorial errors, the PP-Module is recognized as living document and the iTC is dedicated to ongoing updates and revisions. Please report any issues to the AppSW-iTC.

Related Documents

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017.
- [SD] Supporting Document Mandatory Technical Document: Evaluation Activities for collaborative Protection Profile Module for Agent Applications, Version 1.0, February 23, 2022

For more see the Common Criteria Portal.

1. PP-Module Introduction

1.1. PP-Module Reference Identification

- PP-Module Reference: collaborative PP-Module for Agent Applications

- PP-Module Version: 1.0e
- PP-Module Date: 2023-02-15

1.2. TOE Overview

1.2.1. Compliant Targets of Evaluation

This is a Collaborative Protection Profile (cPP) Module whose Target of Evaluation (TOE) is Enterprise Agent Applications. This PP-Module is compatible with the cPP for Application Software and collaborative PP-Module for Server Applications.

For purposes of a PP-Configuration, an Agent Application is any separately deployed TOE application component that communicates with another TOE component under the control, coordination, policy, enrollment, or trust relationship established by the TOE. This may include endpoint agents, worker services, peer services, microservice payloads, subordinate application services, or other application components that are identified as TOE parts in the ST.

For containerized or microservices TOEs, the TOE consists of the application payload components identified in the ST. The container orchestration platform, container runtime, operating system, service mesh infrastructure, ingress infrastructure, cluster networking, and platform-provided secret or configuration stores are part of the operational environment unless explicitly included in the TOE boundary.

1.3. TOE Use Cases

All use cases of Enterprise Agent applications defined in the Collaborative Protection Profile for Application Software are applicable to this PP-Module.

1.4. Distributed and Microservices TOE Configurations

This PP-Module may be used in a PP-Configuration with the PP-Module for Server Applications to evaluate distributed application software. Distributed application software includes server-agent deployments, clustered server deployments, and microservices architectures composed of multiple application payload components.

The ST shall identify each Agent Application component, describe the role of each component, identify which claimed SFRs are implemented by each component, and describe all communications between Agent Application components and other TOE components. The ST shall also distinguish TOE components from operational environment components. If the TOE relies on operational environment components for execution, scheduling, networking, isolation, credential storage, configuration storage, time services, or protection of inter-component communications, the ST shall identify the dependency and the guidance shall describe the required environmental configuration.

2. CC Conformance Claims

As defined by the references [CC1], [CC2] and [CC3], this PP-Module:

- conforms to the requirements of Common Criteria v3.1, Revision 5,
- is Part 2 extended,
- does not claim conformance to any other security functional requirement packages.

In order to be conformant to this PP-Module, a ST shall demonstrate Exact Conformance. Exact Conformance, as a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the SFRs in Security Functional Requirements (these are the mandatory SFRs) of this PP-Module, and potentially SFRs from Consistency Rationale (these are selection-based SFRs) and Selection-Based Requirements (these are optional SFRs) of this PP-Module. While iteration is allowed, no additional requirements (from the CC parts 2 or 3, or definitions of extended components not already included in this PP-Module) are allowed to be included in the ST. Further, no SFRs in Security Functional Requirements of this PP-Module are allowed to be omitted.

2.1. Components allowed with this cPP in a PP-Configuration

The list of packages, PP-Modules and cPPs that may be used in conjunction with this Module can be found at: https://appswcpp.github.io/cPP/AppSW_cPP_allowed-with-list.pdf

3. Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1. Threats

3.1.1. T.UNTRUSTED_COMMUNICATION_CHANNELS_AGENT

Attackers may take advantage of poorly designed or non-secure protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the application itself. Attackers may attempt to target applications that do not use standardized secure tunneling protocols to protect the critical network traffic. This threat is of particular concern when an application uses protocols that have not been subject to extensive peer review. Additionally attackers may attempt to connect via untrusted entities and use that connectivity to perform various attacks.

SFR Rationale:

- FCO_CPC_EXT.1/Agent SFR ensures that only trusted entities connect with each other.

- FPT_ITT.1/Agent SFR ensures that the communication between trusted entities is secure using well known protocols.

3.2. Assumptions

All Assumptions of the Collaborative Protection Profile for Application Software apply also to this PP-Module.

3.3. Organizational Security Policies

There are no OSPs for applications.

4. Security Objectives

4.1. Security Objectives for the TOE

All Objectives of the Collaborative Protection Profile for Application Software apply also to this PP-Module.

4.2. Security Objectives for the Operational Environment

All objectives for the Operational Environment of the Collaborative Protection Profile for Application Software apply also to this PP-Module.

5. Security Functional Requirements

5.1. Conventions

The individual security functional requirements are specified in the sections below. The following conventions are used for the completion of operations:

- [*Italicized text within square brackets*] indicates an operation to be completed by the ST author.
- **Bold text** indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [text within square brackets] indicates the completion of a selection.
- Number in parentheses after SFR name, e.g. (1) indicates the completion of an iteration.
- '/Agent' has been added to every SFR in this module to distinguish SFRs added from Server modules.

Extended SFRs are identified by having a label “EXT” at the end of the SFR name.

5.2. Communication (FCO)

5.2.1. FCO_CPC_EXT.1/Agent

FCO_CPC_EXT.1.1/Agent The TSF shall require a Security Administrator to enable communications between any pair of TOE parts before such communication can take place.

FCO_CPC_EXT.1.2/Agent The TSF shall implement a registration process in which TOE parts establish and use a communications channel that uses [*selection:*

- *A channel that meets the secure channel requirements in FPT_ITT.1,*
- *No channel*

].

Application Note 1: An Agent can communicate with a Server, another Agent, or another separately deployed TOE component identified in the ST. In a microservices architecture, this may include communication between application payload services. This SFR can be iterated if the registration method varies depending on what TOE parts are communicating. "No channel" is selected if the registration is performed via out-of-band manual means.

FCO_CPC_EXT.1.3/Agent The TSF shall enable a Security Administrator to disable communications between any pair of TOE parts.

5.3. Protection of the TSF (FPT)

5.3.1. FPT_ITT.1/Agent

FPT_ITT.1.1/Agent The TSF shall protect TSF data from **disclosure and detect its modification** when it is transmitted between separate parts of the TOE **through the use of [*selection: SSH, TLS, DTLS, HTTPS*]**.

Application Note 2: The data passed in this trusted communication channel are encrypted as defined by the protocol chosen in the selection. The ST author should identify the channels and protocols used by each pair of communicating parts, iterating this SFR as appropriate.

If certificates are used for authentication in any of the protocols selected above, then FIA_X509_EXT.1/ITT/Agent is to be selected.

6. Security Assurance Requirements

This PP-Module does not define any additional assurance requirements above and beyond what is defined in the Collaborative Protection Profile for Application Software that it extends. Application of the SARs to the TOE boundary described by both the claimed base and this PP-Module is sufficient to demonstrate that the claimed SFRs have been implemented correctly by the TOE.

Appendix A: Selection-Based Requirements

A.1. Identification and Authentication (FIA)

A.1.1. FIA_X509_EXT.1/ITT/Agent Certificate Validation

FIA_X509_EXT.1.1/ITT/Agent The application shall [*selection: invoked platform-provided functionality, implement functionality*] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of two certificates.
- The certification path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*selection:*
  - *the Online Certificate Status Protocol (OCSP) as specified in RFC 6960,*
  - *Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3,*
  - *Certificate Revocation List (CRL) as specified in RFC 5759 Section 5,*
  - *an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066,*
  - *no revocation method*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

Application Note 3: This SFR should be chosen if in FPT_ITT.1/Agent protocols selected utilize X.509 certificates for peer authentication. In this case, the use of revocation list checking is optional as there are additional requirements surrounding the enabling and disabling of the ITT channel as defined in FCO_CPC_EXT.1/Agent. If revocation checking is not supported, the ST author should select no revocation method. However, if certificate revocation checking is supported, the ST author selects whether this is performed using OCSP or CRLs.

It is acceptable for the TOE to depend on the platform for certification checking (as defined in this SFR) however all the evaluation activities must be performed irrespective of whether the TOE performs the certificate checking or passes the responsibility to the platform.

The TSF shall be capable of supporting a minimum path length of two certificates. That is, it shall support a certificate hierarchy comprising of at least a self-signed root certificate and a TOE identity certificate.

If the TOE does not support functionality that uses any of the certificate types listed in the extendedKeyUsage rules in FIA_X509_EXT.1.1 then this is stated in the TSS and the relevant part of the SFR is considered trivially satisfied. However, if the TOE does support functionality that uses certificates of any of these types then the corresponding rule must of course be satisfied as in the SFR.

FIA_X509_EXT.1.2/ITT/Agent The application shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

Application Note 4: This requirement applies to certificates that are used and processed by the TSF and restricts the certificates that may be added as trusted CA certificates.

Appendix B: Optional Requirements

There are currently no Optional requirements. Following section may be applicable in later revisions.

Appendix C: Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module, including those used in Consistency Rationale and Selection-Based Requirements .

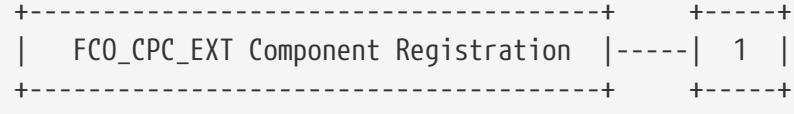
C.1. Communication Partner Control (FCO_CPC_EXT)

C.1.1. Family Behaviour

This is a new component within the FCO class used to define high-level constraints on the ways that partner IT entities communicate. For example, there may be constraints on when communication channels can be used, how they are established, and links to SFRs expressing lower-level security properties of the channels.

C.1.2. Component Levelling

Component leveling



FCO_CPC_EXT.1/Agent Component Registration Channel Definition, requires the TSF to support a registration channel for joining together server and agent TOE parts or other distributed application TOE components, and to ensure that the availability of this channel is under the control of an Administrator. It also requires statement of the type of channel used (allowing specification of

further lower-level security requirements by reference to other SFRs).

Management: FCO_CPC_EXT.1/Agent

The following actions could be considered for the management functions in FPT:

a. There are no management activities foreseen

Audit: FCO_CPC_EXT.1/Agent

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Enabling communications between a pair of TOE parts as in FCO_CPC_EXT.1.1/Agent (including identities of the endpoints).
b. Disabling communications between a pair of TOE parts as in FCO_CPC_EXT.1.3/Agent (including identity of the endpoint that is disabled).

FCO_CPC_EXT.1/Agent

Hierarchical to: No other components

Dependencies: No other components

FCO_CPC_EXT.1.1/Agent The TSF shall require a Security Administrator to enable communications between any pair of TOE parts before such communication can take place.

FCO_CPC_EXT.1.2/Agent The TSF shall implement a registration process in which TOE parts establish and use a communications channel that uses [*selection:*

- *A channel that meets the secure channel requirements in FPT_ITT.1,*
- *No channel*

].

FCO_CPC_EXT.1.3/Agent The TSF shall enable a Security Administrator to disable communications between any pair of TOE parts.

Appendix D: Consistency Rationale

D.1. Consistency of TOE Type

When this PP-Module is used to extend [cPP_APP_SW], the TOE type for the overall TOE is still a generic application. However, one of the functions of the device must be the ability for it to the capability to be managed by a server application. The TOE boundary is simply extended to include that functionality.

D.2. SFR Dependencies Analysis

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