PP-Configuration for Enterprise Server Applications and Agent/Application Component(s)

Table of Contents

Acknowledgements . . . 1
Revision History . . . 1
1. Introduction . . . 1
1.1. PP-Configuration Overview . . . 2
1.2. PP-Configuration Reference . . . 2
1.3. PP-Configuration Components . . . 2
1.4. Distributed and Microservices TOE Architectures . . . 2
2. Conformance Claims . . . 7
2.1. CC Statement . . . 7
2.2. CC Conformance Claims . . . 7
3. SAR Statement . . . 7
3.1. Related Documents . . . 8

Acknowledgements

This PP-Configuration 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	2024-02-15	Incorporated feedback received following initial release.

1. Introduction

1.1. PP-Configuration Overview

The purpose of a PP-Configuration is to combine Protection Profiles (PPs) and PP-Modules for various technology types into a single configuration that can be evaluated as a whole.

This PP-Configuration is for enterprise server applications and their agent or application component(s). It provides the enforceable PP-Configuration path for distributed application software, including server-agent deployments, clustered server deployments, and microservices architectures composed of multiple application payload components.

1.2. PP-Configuration Reference

This PP-Configuration is identified as follows:

- PP-Configuration for Enterprise Server Applications and Agent/Application Component(s), Version 1.0e, 2024-02-15
- As a shorthand reference, it can be identified as "CFG_APP-Server-Agent_V1.0e""

1.3. PP-Configuration Components

This PP-Configuration includes the following components:

Table 2. PP-Configuration Components

[base PP]	cPP_APP_SW_V1.1
[PP-Module 1]	MOD_Server_v1.1
[PP-Module 2]	MOD_Agent_v1.1

1.4. Distributed and Microservices TOE Architectures

For this PP-Configuration, a distributed TOE consists of multiple separately deployed application components that collectively provide the TOE security functionality. Each TOE component shall be identified in the ST and mapped to the base PP, Server Module, Agent Module, or a combination of those components, as applicable.

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.

The ST shall provide an SFR allocation rationale that identifies whether each claimed requirement is satisfied by all TOE components, by applicable TOE components that perform the relevant function, by at least one TOE component, by the TOE as a whole, or by an allowed operational environment dependency. The ST shall describe all inter-component TOE communications and identify the mechanisms used to authorize and protect those communications.

1.4.1. SFR Allocation for Distributed TOEs

For a distributed TOE, the SFRs are satisfied by the TOE as a whole; however, not every SFR is necessarily implemented by every TOE component. The ST author shall use the following allocation categories to identify how each SFR is satisfied by the distributed TOE.

All Components

Every TOE component shall independently satisfy the requirement.

Applicable Components

Every TOE component that performs the relevant function shall satisfy the requirement. The ST shall identify the components to which the requirement applies and justify why the requirement does not apply to other TOE components.

At Least One Component

At least one TOE component shall satisfy the requirement on behalf of the TOE. The ST shall identify the component or components that satisfy the requirement and describe how this satisfies the TOE-level claim.

TOE as a Whole

The requirement is satisfied by the collective behavior of the TOE components. The ST shall describe the TOE-level behavior and identify any component responsibilities necessary to satisfy the claim.

Operational Environment Dependency

The TOE relies on the operational environment for the function, where allowed by the base cPP or PP-Module. The ST shall identify the environmental dependency and the guidance shall describe the required environmental configuration.

The following table defines the expected allocation for the base cPP SFRs in a distributed TOE.

Table 3. Base cPP SFR Allocation for Distributed TOEs

SFR	Allocation	Distributed TOE guidance
FCS_CKM.1/AK	Applicable Components	Applies to each TOE component that invokes or implements asymmetric key generation.
FCS_CKM.1/SK	Applicable Components	Applies to each TOE component that generates symmetric keys.
FCS_CKM.2	Applicable Components	Applies to each TOE component that performs key establishment.
FCS_CKM_EXT.1	Applicable Components	Applies to each TOE component that invokes or implements key generation services.
FCS_COP.1/Hash	Applicable Components	Applies to each TOE component that performs hashing for a claimed function.
FCS_COP.1/KeyedHash	Applicable Components	Applies to each TOE component that performs keyed-hash functions for a claimed function.

SFR	Allocation	Distributed TOE guidance
FCS_COP.1/SigGen	Applicable Components	Applies to each TOE component that generates digital signatures.
FCS_COP.1/SigVer	Applicable Components	Applies to each TOE component that verifies digital signatures, including update verification if performed by that component.
FCS_COP.1/SKC	Applicable Components	Applies to each TOE component that performs encryption or decryption.
FCS_HTTPS_EXT.1	Applicable Components	Applies to each TOE component that implements HTTPS as a client, server, or server with mutual authentication.
FCS_HTTPS_EXT.2	Applicable Components	Applies to each TOE component that implements HTTPS with peer certificate authentication behavior covered by this requirement.
FCS_PBKDF_EXT.1	Applicable Components	Applies to each TOE component that performs password conditioning.
FCS_RBG.1	Applicable Components	Applies to each TOE component that implements RBG functionality.
FCS_RBG.2	Applicable Components	Applies to each TOE component that implements RBG functionality using external seeding.
FCS_RBG.3	Applicable Components	Applies to each TOE component that implements RBG functionality using a single internal noise source.
FCS_RBG.4	Applicable Components	Applies to each TOE component that implements RBG functionality using multiple internal noise sources.
FCS_RBG.5	Applicable Components	Applies to each TOE component that implements RBG functionality using combined noise sources.
FCS_RBG_EXT.1	Applicable Components	Applies to each TOE component that invokes platform-provided RBG services, implements RBG functionality, or claims no RBG functionality.
FCS_SNI_EXT.1	Applicable Components	Applies to each TOE component that creates or uses salts, nonces, or initialization vectors for claimed cryptographic functions.
FCS_STO_EXT.1	Applicable Components	Applies to each TOE component that persistently stores credentials.
FDP_DAR_EXT.1	Applicable Components	Applies to each TOE component that stores sensitive application data at rest.

SFR	Allocation	Distributed TOE guidance
FDP_DEC_EXT.1	All Components	Each TOE component shall identify and restrict its access to platform resources and sensitive information repositories as required by the base cPP.
FDP_NET_EXT.1	All Components	Each TOE component shall identify and restrict its inbound and outbound network communications.
FMT_CFG_EXT.1	All Components	Each TOE component shall satisfy secure-by-default and file-permission requirements for its installed binaries, data, and default credentials.
FMT_MEC_EXT.1	Applicable Components	Applies to each TOE component that stores or manages configuration options.
FMT_SMF.1	Applicable Components	Applies to each TOE component that provides security management functions. At least one component shall be identified if management functions are claimed for the TOE.
FPR_ANO_EXT.1	Applicable Components	Applies to each TOE component that transmits personally identifiable information.
FPT_AEX_EXT.1	All Components	Each TOE component shall satisfy the anti-exploitation requirements applicable to its platform and implementation type.
FPT_API_EXT.1	All Components	Each TOE component shall use only documented and supported platform APIs.
FPT_API_EXT.2	Applicable Components	Applies to each TOE component that parses IANA MIME media types covered by the objective requirement.
FPT_FLS.1	Applicable Components	Applies to each TOE component that must preserve a secure state for the selected failure conditions.
FPT_IDV_EXT.1	TOE as a Whole	The TOE shall identify software versions. The ST shall identify how each separately versioned TOE component is represented in the TOE version information.
FPT_LIB_EXT.1	All Components	Each TOE component shall identify its third-party libraries.
FPT_TST.1	Applicable Components	Applies to each TOE component that performs TSF self-tests or integrity verification covered by the requirement.

SFR	Allocation	Distributed TOE guidance
FPT_TUD_EXT.1	TOE as a Whole	The TOE shall provide trusted update support. The ST shall identify how each updateable TOE component is checked, delivered, installed, and versioned.
FPT_TUD_EXT.2	Applicable Components	Applies to each TOE component or update package that performs installation or update integrity functions covered by this selection-based requirement.
FTP_DIT_EXT.1	Applicable Components	Applies to each TOE component that transmits data or sensitive data to another trusted IT product or invokes platform-provided functionality for that protection. Inter-component TOE communications are addressed by the Server and Agent Module requirements in this PP-Configuration.

The following table defines the expected allocation for the Server and Agent PP-Module SFRs in a distributed TOE.

Table 4. Server and Agent Module SFR Allocation for Distributed TOEs

SFR	Allocation	Distributed TOE guidance
FMT_MEC_EXT.1/Server	Applicable Components	Applies to each Server Application component that stores or manages server configuration data.
FMT_SMF.1/Server	Applicable Components	Applies to each Server Application component that provides management functions. The ST shall identify which component or components manage inter-component communications, enrollment, or policy.
FPT_AEX_EXT.2/Server	All Server Components	Each Server Application component shall be compatible with security features provided by its platform vendor.
FCO_CPC_EXT.1/Server	Applicable Components	Applies to each Server Application component that enables, disables, registers, or authorizes communication with another TOE component.
FIA_X509_EXT.1/ITT/Server	Applicable Components	Applies to each Server Application component that validates X.509 certificates for inter-TOE-part communication.
FPT_ITT.1/Server	Applicable Components	Applies to each Server Application component that transmits TSF data between separate parts of the TOE.

SFR	Allocation	Distributed TOE guidance
FCO_CPC_EXT.1/Agent	Applicable Components	Applies to each Agent Application component that is enabled, disabled, registered, authorized, or otherwise controlled for communication with another TOE component.
FPT_ITT.1/Agent	Applicable Components	Applies to each Agent Application component that transmits TSF data between separate parts of the TOE.
FIA_X509_EXT.1/ITT/Agent	Applicable Components	Applies to each Agent Application component that validates X.509 certificates for inter-TOE-part communication.

If an operational environment component, such as a container orchestration platform, container runtime, service mesh infrastructure, ingress infrastructure, cluster networking, or platform-provided secret or configuration store, is relied upon to support a claimed SFR, the ST shall identify the dependency. The evaluator assesses the TOE's use of the dependency and the required configuration guidance, but the environmental component is not included in the TOE boundary unless explicitly claimed.

If a TOE container receives credentials, keys, tokens, certificates, or other secrets from an operational environment mechanism, such as a platform secret store, mounted secret volume, injected environment variable, or external secrets provider, the ST shall identify the mechanism, the TOE components that consume the secrets, the purpose of each secret, and whether the TOE persists, transforms, caches, or re-exports the secret. If the TOE persists or manages the secret after receipt, the applicable base cPP requirements, including FCS_STO_EXT.1, FDP_DAR_EXT.1, FMT_MEC_EXT.1, and related cryptographic requirements, apply to the TOE component performing that function.

2. Conformance Claims

2.1. CC Statement

To be conformant to this PP-Configuration, an ST must demonstrate Exact Conformance, as defined by the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs.

2.2. CC Conformance Claims

This PP-Configuration, and its components specified in section 1.3, are conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

3. SAR Statement

The set of SARs specified for this PP-Configuration are taken from, and identical to, those specified in the base PP.

3.1. Related Documents

Common Criteria[1]

Table 5. Common Criteria References

[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.
[addenda]	CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, May 2017.

[1] For details see http://www.commoncriteriaportal.org/