PP-Configuration for cPP_DBMS, DBMS in the Cloud Module, and DBMS Cryptographic Functions Module

Version 0.4, 2026-06-30

Table of Contents

Acknowledgements

This PP-Configuration was developed by the Database Management Systems international Technical Community (iTC), also known as DBMS-iTC, with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

Revision History

Table 1. Revision history

Version	Date	Description
0.4	2026-06-30	Initial public review draft. Defines the PP-Configuration for tenant-operated DBMS cloud deployments using the DBMS Base PP, DBMS in the Cloud Module, and DBMS Cryptographic Functions Module, including formal CCDB-018 consumption and the optional Enterprise Enhanced use case.

Chapter 1. Introduction

1.1. PP-Configuration Overview

This PP-Configuration combines the collaborative Protection Profile for Database Management Systems (Version 2.0), the collaborative PP-Module for DBMS in the Cloud, Version 0.4, and the collaborative PP-Module for DBMS Cryptographic Functions, Version 0.4.

The configuration is intended for DBMS products deployed by a customer or tenant on cloud infrastructure or platform services. The DBMS in the Cloud Module defines cloud deployment integration requirements, while the DBMS Cryptographic Functions Module defines the mandatory DBMS cryptographic requirements used by the cloud deployment.

1.2. PP-Configuration Reference

Table 2. PP-Configuration Identification

Attribute	Value
PP-Configuration Title	PP-Configuration for cPP_DBMS, DBMS in the Cloud Module, and DBMS Cryptographic Functions Module
PP-Configuration Short Name	PPC_DBMS_CLOUD_CRYPTO
PP-Configuration Version	0.4
PP-Configuration Publication Date	2026-06-30
Sponsor	Database Management Systems international Technical Community (DBMS-iTC)
CC Version	CC:2022

1.3. PP-Configuration Components

Table 3. PP-Configuration Components

Type	Component	Version / Date	Role in Configuration
Base PP	collaborative Protection Profile for Database Management Systems	Version 2.0, 27 April 2026	Defines the baseline DBMS TOE type, security problem definition, mandatory SFRs, SAR package, and exact conformance baseline.

Type	Component	Version / Date	Role in Configuration
PP-Module	collaborative PP-Module for DBMS Cryptographic Functions	Version 0.4, 2026-06-30	Provides mandatory DBMS cryptographic requirements for data-at-rest encryption, data-in-transit protection, and key management.
PP-Module	collaborative PP-Module for DBMS in the Cloud	Version 0.4, 2026-06-30	Adds cloud-specific requirements for tenant-operated DBMS deployments on cloud infrastructure or platform services.

1.4. Configuration Scope

This PP-Configuration applies to tenant-operated DBMS deployments in cloud environments. It is not intended for provider-operated Database-as-a-Service offerings where the cloud service provider operates and manages the DBMS on behalf of tenants.

The DBMS DBaaS Module is mutually exclusive with the DBMS in the Cloud Module. A TOE claiming the DBMS DBaaS Module shall use the DBaaS PP-Configuration rather than this PP-Configuration.

Chapter 2. Component Statements

2.1. Base PP Statement

The DBMS Base PP is the required Base PP for this PP-Configuration. All mandatory requirements of the Base PP apply.

2.2. DBMS Cryptographic Functions Module Statement

The DBMS Cryptographic Functions Module is mandatory in this PP-Configuration. The Security Target shall include all mandatory SFRs from the module and all selection-based SFRs triggered by completed selections.

The Crypto Module is authoritative for:

- DBMS data-at-rest encryption
- DBMS data-in-transit protection, including TLS and X.509 component claims where applicable
- DBMS cryptographic key management
- Catalogue-derived components consumed in the Crypto Module and applicable Functional Package components

2.3. Crypto Module Use Case Statement

The Security Target shall identify `[USE CASE 1] General-Purpose Cryptographic Deployment`, `[USE CASE 2] Enterprise Enhanced`, or both, as applicable. Inclusion of the Cloud Module does not automatically select Enterprise Enhanced. When selected, Enterprise Enhanced constrains only the applicable Catalogue operations according to the Crypto Module template; Cloud-specific `FDP_DIT_EXT.1` mapping and testing remain in the Cloud Module and SD.

2.4. DBMS in the Cloud Module Statement

The DBMS in the Cloud Module is mandatory in this PP-Configuration. The Security Target shall include all mandatory SFRs from the Cloud Module and all selection-based SFRs triggered by completed selections.

The Cloud Module is authoritative for cloud-specific integration and configuration requirements, including:

- Cloud identity integration
- Cloud audit integration and audit export
- Cloud configuration and secret handling while under TOE control
- Trusted update, deployment integrity, and cloud resilience signaling requirements
- Cloud-specific mapping of inherited `FDP_DIT_EXT.1` data-in-transit protection to cloud deployment channels

Chapter 3. Conformance Claims

3.1. CC Conformance

This PP-Configuration and its components claim conformance to Common Criteria for Information Technology Security Evaluation, CC:2022, as follows:

- CC Part 1 conformant
- CC Part 2 extended
- CC Part 3 conformant

3.2. PP-Configuration Conformance Statement

To be conformant to this PP-Configuration, a Security Target shall demonstrate Exact Conformance to this PP-Configuration and to each component listed in Section 1.3, “PP-Configuration Components”.

The Security Target shall include:

1. A statement that the claimed PP-Configuration includes the DBMS Base PP.
2. A statement that the claimed PP-Configuration includes the DBMS Cryptographic Functions Module.
3. A statement that the claimed PP-Configuration includes the DBMS in the Cloud Module.
4. All mandatory SFRs from the DBMS Base PP, DBMS Cryptographic Functions Module, and DBMS in the Cloud Module.
5. All selection-based SFRs triggered by completed selections in the claimed components.
6. Identification of the applicable Crypto Module use case or use cases and, when Enterprise Enhanced is selected, completion of all applicable operations according to its selection template.
7. The SAR package inherited from the DBMS Base PP.

While iteration is allowed, the Security Target shall not include additional requirements from CC Part 2, CC Part 3, or extended components not already included in the DBMS Base PP, the claimed DBMS PP-Modules, or another component explicitly permitted by this PP-Configuration.

Chapter 4. Security Assurance Requirements

The SAR package for this PP-Configuration is inherited from the DBMS Base PP: EAL2 as defined in CC:2022 Part 5, augmented by ALC_FLR.3 Systematic flaw remediation.

No additional SARs are introduced by this PP-Configuration.

Chapter 5. SFR Composition

Table 4. SFR Composition Summary

Source	SFR Treatment	Notes
DBMS Base PP	All mandatory, optional, and selection-based requirements apply as specified by the Base PP.	The Base PP provides the baseline DBMS requirements and conformance rules.
DBMS Cryptographic Functions Module	All mandatory requirements apply. Selection-based requirements apply when triggered by module selections.	The module provides `FDP_DAR_EXT.1`, `FDP_DIT_EXT.1`, key management requirements, consumed Catalogue-derived components, and the relationship to applicable Functional Packages.
DBMS in the Cloud Module	All mandatory requirements apply. Selection-based requirements apply when triggered by module selections.	The module defines cloud-specific requirements and maps inherited cryptographic protections to cloud deployment channels.

Chapter 6. Consistency Rationale

This PP-Configuration is consistent because each component has a distinct scope:

- The DBMS Base PP defines the baseline DBMS TOE type and assurance package.
- The DBMS Cryptographic Functions Module defines DBMS-specific cryptographic requirements and integration activities; Catalogue methods evaluate algorithms and Functional Package methods evaluate protocols and certificates.
- The DBMS in the Cloud Module defines cloud deployment integration requirements for tenant-operated cloud deployments.

The Cloud Module does not redefine the Crypto Module's data-at-rest or data-in-transit requirements. Instead, it identifies the cloud deployment channels and integration points to which the inherited Crypto Module requirements apply. This maintains clear ownership of cryptographic SFRs while making those protections mandatory for cloud deployments.

Chapter 7. Technical Decisions

Technical Decisions applicable to the DBMS Base PP, DBMS Cryptographic Functions Module, or DBMS in the Cloud Module apply according to the affected component document. This PP-Configuration does not introduce additional Technical Decisions.

Appendix A: Related Documents

- [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 requirements, CCMB-2022-11-002, CC:2022 Revision 1, November 2022.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022 Revision 1, November 2022.
- [CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022 Revision 1, November 2022.
- [CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022 Revision 1, November 2022.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2022-11-006, CEM:2022 Revision 1, November 2022.
- [cPP_DBMS] collaborative Protection Profile for Database Management Systems, Version 2.0, 27 April 2026.
- [cPP_DBMS_SD] Supporting Document Mandatory Technical Document Evaluation Activities for the collaborative Protection Profile for Database Management Systems, Version 2.0, 27 April 2026.
- [DBMS_MOD_CRYPTO] collaborative PP-Module for DBMS Cryptographic Functions, Version 0.4, 2026-06-30.
- [DBMS_MOD_CRYPTO_SD] Supporting Document - Evaluation Activities for DBMS Cryptographic Functions Module, Version 0.4, 2026-06-30.
- [DBMS_Cloud_MOD] collaborative PP-Module for DBMS in the Cloud, Version 0.4, 2026-06-30.
- [DBMS_Cloud_SD] Supporting Document - Evaluation Activities for DBMS in the Cloud Module, Version 0.4, 2026-06-30.

Appendix B: Acronyms

Table 5. Acronyms used in this PP-Configuration

Acronym	Meaning
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
DBMS	Database Management System
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality