PP-Configuration for cPP_DBMS 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 claiming the DBMS Cryptographic Functions Module with the DBMS Base PP, 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) with the collaborative PP-Module for DBMS Cryptographic Functions, Version 0.4.

The configuration is intended for DBMS products that claim DBMS-specific cryptographic support without also claiming a cloud deployment module. The DBMS Cryptographic Functions Module defines the TOE-enforced requirements for DBMS key management, data-at-rest encryption, and data-in-transit protection.

1.2. PP-Configuration Reference

Table 2. PP-Configuration Identification

Attribute	Value
PP-Configuration Title	PP-Configuration for cPP_DBMS and DBMS Cryptographic Functions Module
PP-Configuration Short Name	PPC_DBMS_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	Adds DBMS-specific cryptographic SFRs and consumes CCDB-018 components for key management and data-at-rest encryption; data-in-transit protocols and certificate behavior are supplied by applicable Functional Packages.

1.4. Configuration Scope

This PP-Configuration applies to DBMS TOEs that provide DBMS-specific cryptographic functions as part of the TOE Security Functionality. It does not include the DBMS in the Cloud Module or the DBMS DBaaS Module. A TOE claiming either cloud deployment module shall use the corresponding PP-Configuration for that module.

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.

The Base PP assumption `A.CONNECT` is displaced for the data-in-transit channels covered by the DBMS Cryptographic Functions Module. In this PP-Configuration, the mandatory Crypto Module requirement `FDP_DIT_EXT.1` provides TOE-enforced data-in-transit protection for data transmitted between the TOE and external entities.

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 module is responsible for:

- DBMS master key and data encryption key lifecycle requirements
- Data-at-rest encryption strategy
- Data-in-transit protection
- Applicable Catalogue-derived components consumed in the Crypto Module and applicable TLS/X.509 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. Enterprise Enhanced is optional in this PP-Configuration and constrains only the applicable Catalogue operations according to the Crypto Module's Enterprise Enhanced Use Case Selection Template. It does not create a separate PP-Configuration or independently assert FIPS 140-3 validation, NIAP approval, or complete-product CNSA 2.0 conformance.

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. All mandatory SFRs from the DBMS Base PP and the DBMS Cryptographic Functions Module.
4. All selection-based SFRs triggered by completed selections in the DBMS Base PP or the DBMS Cryptographic Functions Module.
5. 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.
6. 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 DBMS Cryptographic Functions Module, 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 mandatory `FDP_DIT_EXT.1` data-in-transit protection and mandatory DBMS data-at-rest cryptographic requirements.
Catalogue and Functional Package components	Catalogue-derived components are consumed and reproduced by the DBMS Cryptographic Functions Module; protocol and certificate components are supplied by the applicable Functional Packages.	The ST author shall include every Catalogue-derived component triggered by the Crypto Module selections and the applicable TLS/X.509 Functional Package components required by `FDP_DIT_EXT.1`.

Chapter 6. Consistency Rationale

This PP-Configuration is consistent because the DBMS Cryptographic Functions Module strengthens the DBMS Base PP without contradicting it. The Base PP relies on an operational-environment assumption for connectivity protection. The Crypto Module converts the relevant data-in-transit protection into a TOE-enforced SFR through `FDP_DIT_EXT.1`.

The Crypto Module does not alter the DBMS TOE type defined by the Base PP. It adds cryptographic security functions that are appropriate for DBMS TOEs and are evaluated in conjunction with the Base PP assurance activities and the module Supporting Document.

Chapter 7. Technical Decisions

Technical Decisions applicable to the DBMS Base PP or the DBMS Cryptographic Functions 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.

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