PP-Configuration for cPP_DBMS, DBMS DBaaS Module, and DBMS Cryptographic Functions Module

Version 0.5, 2026-07-20

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 provider-operated DBaaS deployments using the DBMS Base PP, DBMS DBaaS Module, and DBMS Cryptographic Functions Module, including formal CCDB-018 consumption and the optional Enterprise Enhanced use case.
0.4	2026-07-14	Component statements corrected: customer-controlled key models are defined by the DBaaS Module's FCS_CKM_DBAAS_EXT.1 and couple to the Crypto Module's Key Origin selections (previously misattributed to the Crypto Module); DBaaS authoritative-scope list updated for the Trusted Service Update design.
0.4	2026-07-18	Added the Evaluation Approach for the Composed TOE: the DBaaS Module SD's Managed-Service Evaluation Constraint, Evidence Vantages, and Evaluator Access Strategy govern evidence collection for all component activities under this PP-Configuration, including Base PP and Crypto Module SD activities that assume administrative access the managed-service model does not provide; laboratories directed to the Evidence Vantage Mapping and Test Environment Guidance for scoping.
0.4	2026-07-20	Aligned the composition with the Crypto Module's role-specific ML-KEM design. Customer-authorized KEM establishment is an optional DBaaS key model mapped to the "Established through Key Encapsulation" origin; the Crypto Module remains authoritative for TOE-boundary KeyGen, encapsulation or decapsulation, derivation, destruction, and transferred-key protection, while external KMS operations remain environmental allocations.

Version	Date	Description
0.5	2026-07-20	Updated the composition to the Version 0.5 DBaaS and Cryptographic Functions Modules and SDs, including the completed managed-service assurance model, normative audit coverage, and explicit Master Key protection selection.

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 Database-as-a-Service (DBaaS), Version 0.5, and the collaborative PP-Module for DBMS Cryptographic Functions, Version 0.5.

The configuration is intended for provider-operated managed database services where the cloud service provider operates and manages the DBMS on behalf of tenants. The DBMS DBaaS Module defines managed-service requirements for tenant isolation, resource governance, backup and restore, immutable audit behavior, and provider-administrator restrictions. The DBMS Cryptographic Functions Module defines the mandatory DBMS cryptographic requirements used by the DBaaS deployment.

1.2. Review Set Placement

This PP-Configuration is included in the full Version 0.5 module review release as the Crypto + DBaaS composition family. It is published for review alongside the Crypto + Cloud family and uses the same DBMS Cryptographic Functions Module as its mandatory cryptographic component.

1.3. PP-Configuration Reference

Table 2. PP-Configuration Identification

Attribute	Value
PP-Configuration Title	PP-Configuration for cPP_DBMS, DBMS DBaaS Module, and DBMS Cryptographic Functions Module
PP-Configuration Short Name	PPC_DBMS_DBAAS_CRYPTO
PP-Configuration Version	0.5
PP-Configuration Publication Date	2026-07-20
Sponsor	Database Management Systems international Technical Community (DBMS-iTC)
CC Version	CC:2022

1.4. 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.
PP-Module	collaborative PP-Module for DBMS Cryptographic Functions	Version 0.5, 2026-07-20	Provides mandatory DBMS cryptographic requirements for data-at-rest encryption, data-in-transit protection, and key management.
PP-Module	collaborative PP-Module for Database-as-a-Service (DBaaS)	Version 0.5, 2026-07-20	Adds managed-service requirements for provider-operated DBMS services.

1.5. Configuration Scope

This PP-Configuration applies to provider-operated managed database services. It is not intended for tenant-operated DBMS deployments on cloud infrastructure or platform services.

The DBMS DBaaS Module is mutually exclusive with the DBMS in the Cloud Module. A TOE claiming the DBMS in the Cloud Module shall use the Cloud 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, including protected tenant data and protected backups where applicable
- DBMS data-in-transit protection for tenant-facing, administrative, and programmatic interfaces
- DBMS cryptographic key management, including the Key Origin selections and trusted channels on which the DBaaS Module's customer-controlled key mechanisms rely; where ML-KEM is selected, this includes role-specific TOE operations, optional TOE KeyGen, KDF-based Master Key or KEK derivation, and destruction of secret intermediate values
- Catalogue-derived components consumed in the Crypto Module and applicable Functional Package components

The customer-controlled key models themselves (BYOK, external KMS integration, key-reference mechanisms, and optional customer-authorized ML-KEM establishment, with the provider-inaccessibility and revocation requirements) are defined by the DBaaS Module's `FCS_CKM_DBAAS_EXT.1`, which couples to the Crypto Module's Key Origin selections as described in that module. An ML-KEM claim does not imply that KMIP implements ML-KEM: the ST identifies each operation performed by the TOE and each operation allocated to an external KMS or other customer-controlled service. Protocol-level ML-KEM, including hybrid TLS, remains governed by the applicable Functional Package.

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 DBaaS Module does not automatically select Enterprise Enhanced. When selected, Enterprise Enhanced constrains only the applicable Catalogue operations according to the Crypto Module template; DBaaS-specific tenant, backup, update, and provider-operation requirements remain in the DBaaS Module and SD.

2.4. DBMS DBaaS Module Statement

The DBMS DBaaS Module is mandatory in this PP-Configuration. The Security Target shall include

all mandatory SFRs from the DBaaS Module and all selection-based SFRs triggered by completed selections.

The DBaaS Module is authoritative for managed-service controls, including:

- Tenant isolation and tenant-context binding
- Residual information protection for cross-tenant resource reuse
- Resource governance
- Tenant-scoped and immutable audit behavior
- Protected backup and restore path requirements
- Customer-controlled key models (FCS_CKM_DBAAS_EXT.1), coupled to the Crypto Module's Key Origin selections, including the optional KEM-established origin when the customer retains enforceable authorization control
- Trusted service update (declared deployment model, signature-verified service software, tenant version visibility)

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 1.4, “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 DBaaS Module.
4. All mandatory SFRs from the DBMS Base PP, DBMS Cryptographic Functions Module, and DBMS DBaaS 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. Evaluation Approach for the Composed TOE

A TOE conformant to this PP-Configuration is a provider-operated managed service. The Evaluation Activities of all three components — the Base PP SD, the Crypto Module SD, and the DBaaS Module SD — are executed against that service, and the Base PP and Crypto Module SDs were written for TOEs where the evaluator holds full administrative access. Evidence collection for every component's activities is therefore governed by the DBaaS Module SD [[DBMS_MOD_DBAAS_SD]]: its Managed-Service Evaluation Constraint, its Evidence Vantages (V1 tenant data plane, V2 tenant service control plane, V3 evaluator-controlled external services, V4 provider-internal operations), and its Evaluator Access Strategy apply to Base PP and Crypto Module activities as well as to the DBaaS Module's own.

A Base PP or Crypto Module activity exercisable from the tenant vantages (V1, V2) is performed there unchanged. Where such an activity assumes host-level, operating-system, or full-DBA access that the managed-service model does not provide to tenants, the evaluator applies the DBaaS Module SD's Evaluator Access Strategy and records each reliance on TSS review, operational guidance, scheme-accepted evidence, or provider-supported demonstration in the ETR.

The DBaaS Module SD's Evidence Vantage Mapping appendix assigns expected vantages to every DBaaS Module test activity and identifies the activities that require provider participation. Laboratories should use it, together with that SD's Test Environment Guidance, when scoping an evaluation against this PP-Configuration: the evaluation requires an evaluation tenancy with at least two tenant contexts, an evaluator-controlled external key management service and audit sink, and scheduled provider participation for the provider-internal (V4) activities.

Chapter 6. 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 DBaaS Module	All mandatory requirements apply. Selection-based requirements apply when triggered by module selections.	The module defines managed-service controls for provider-operated DBMS services and inherits cryptographic protections from the Crypto Module.

Chapter 7. 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 DBaaS Module defines managed-service requirements for provider-operated DBMS services.

The DBaaS Module does not redefine the Crypto Module's data-at-rest or data-in-transit requirements. Instead, it adds DBaaS-specific controls for tenant isolation, provider-administrator restrictions, protected backup and restore paths, and managed-service operations. This maintains clear ownership of cryptographic SFRs while making those protections mandatory for DBaaS deployments.

Chapter 8. Technical Decisions

Technical Decisions applicable to the DBMS Base PP, DBMS Cryptographic Functions Module, or DBMS DBaaS 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 0.5, 2026-07-20.
- [DBMS_MOD_CRYPTO_SD] Supporting Document - Evaluation Activities for DBMS Cryptographic Functions Module, Version 0.5, 2026-07-20.
- [DBMS_MOD_DBAAS] collaborative PP-Module for Database-as-a-Service (DBaaS), Version 0.5, 2026-07-20.
- [DBMS_MOD_DBAAS_SD] Supporting Document - Evaluation Activities for DBaaS Module, Version 0.5, 2026-07-20.

Appendix B: Acronyms

Table 5. Acronyms used in this PP-Configuration

Acronym	Meaning
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
DBaaS	Database-as-a-Service
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