collaborative PP-Module for DBMS Cryptographic Functions

26 June 2026

Version 0.3

Table of Contents

Acknowledgements

This collaborative Protection Profile Module (PP-Module) 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. The organizations that contributed to the development of this PP-Module include:

INDUSTRY

IBM

Microsoft

Oracle Corp.

COMMON CRITERIA TEST LABORATORIES

atsec information security

Intertek EWA-Canada and Intertek Acumen

TÜViT

Teron Labs

Combitech

GOVERNMENT AGENCIES

FMV/CSEC - Swedish Certification Body for IT Security

BSI - Bundesamt für Sicherheit in der Informationstechnik

JISEC - Japan IT Security Evaluation and Certification Scheme

Revision History

Table 1. Revision history

Version	Date	Description
0.1	2026-01-25	Initial Draft
0.2	2026-01-25	Revised to act as a Consumer of the CC Crypto Catalogue; removed redundant algorithm definitions.

Version	Date	Description
0.3	2026-06-26	Structural completeness update: expanded PP-Module structure, conformance claims, policies, objectives, rationale, SARs, dependency summaries, and appendices. Corrected CCDB-018 component references (FCS_CKM.6, FCS_COP.1/SKC, FCS_COP.1/AEAD, and FCS_CKM.1/SKG), updated the TLS reference to Functional Package for TLS v2.1, aligned Base PP references with cPP_DBMS Version 2.0, and adopted shared AsciiDoc PDF/HTML rendering assets.
0.4	2026-06-30	Added mandatory FDP_DIT_EXT.1 Data-in-Transit Protection, relocated from the DBMS Cloud Module so that this module is the single source of data-in-transit protection across all configurations. Reworked cryptographic requirements to consume components from CCDB-018 directly, added explicit Catalogue provenance and modification rules, and added the optional Enterprise Enhanced use case selection template for alignment with FIPS 140-3, NIAP, and CNSA 2.0 requirements applicable to this module. Identified the Crypto SD transitional mechanism for Certification Body-recognized algorithm validation evidence pending publication of the Catalogue Evaluation Methods.
0.4	2026-07-07	Package Conformance now requires the TLS FP v2.1 claim (and X.509 FP v1.0 where certificate authentication applies) rather than disclaiming functional package claims; Exact Conformance permits extended components defined in Functional Packages claimed per Package Conformance; Conformance Claim Rationale adds identification of claimed Functional Packages. SFR List application note on FDP_DIT_EXT.1 names the Cloud Module as the added-module configuration and references the DBMS DBaaS Module as planned on a later publication track.

Version	Date	Description
0.4	2026-07-08	Corrected APE to ACE for PP-Module evaluation under CC:2022. Replaced the Consistency Rationale appendix, which duplicated the main-body Security Rationale tables, with the ACE_MCO consistency demonstration: TOE type, security problem definition, security objectives, and SFRs versus the Base PP, plus a configuration-neutrality statement covering all allowed PP-Configurations. Reworded the data-in-transit consistency analysis and the FDP_DIT_EXT.1 application note: FDP_DIT_EXT.1 supplements, and does not replace, A.CONNECT; removed the claim that FDP_DIT_EXT.1 discharges the FPT_ITT.1 dependency of FPT_TRC.1 (the SFR is scoped to TOE-to-external-entity channels and does not address inter-TSF transfer).
0.4	2026-07-08	Restructured FDP_DIT_EXT.1.1 so TLS cannot be deselected: the element now requires the TLS Functional Package claim directly, with a selection governing only supplementary protocols ([selection: no other cryptographic protocol, [assignment: other protocol claimed from an applicable Functional Package]]). The application note states that a novel or proprietary data-in-transit mechanism does not substitute for the TLS claim, and that protocols implemented by the underlying operating system or kernel (for example, IPsec) are outside the TOE boundary in this module’s composition model. The extended component definition now carries the same operation structure as the instantiated SFR; ECD wording for FCS_CKM_EXT.1.2 and FDP_ITC_EXT.1.3 aligned to their instantiations ("claimed as"/"claimed from").

Version	Date	Description
0.4	2026-07-08	Added a third Key Origin to FCS_CKM_EXT.1.1, "Externally Managed": an external key management service (e.g., a KMIP-conformant key manager) remains the authoritative store and the TOE retrieves the Master Key for transient use or invokes its operations by reference, with no persistent plaintext Master Key storage in the TOE boundary. FDP_ITC_EXT.1 retitled "Trusted Channel for Key Import and External Key Management" and now triggered by either external Key Origin; the key-management message protocol (e.g., KMIP) is carried over the mutual TLS channel and is not itself evaluated. Threat T.KEY_IMPORT_INTERCEPTION, objective O.TRUSTED_KEY_IMPORT, conformance rules, Package Conformance, rationale mappings, trigger tables, and ECDs updated; added the KMIP bibliography entry and an explicit note that the import threat is vacuously countered for internally generated keys.
0.4	2026-07-08	Introduction chapters updated for the data-in-transit and external-key-management scope: TOE Type now names data-at-rest, data-in-transit, and Master Key management; TOE Scope gains the TLS-protected external communication channels bullet and extends the trusted-channel bullet to external key management; the Preface’s originated-requirements list gains Data-in-Transit Protection and generalizes the key import bullet; Keywords gain KMIP, Data-in-Transit, and TLS.
0.4	2026-07-08	Enterprise Enhanced template gains an FCS_CKM_EXT.1.2 row restricting stored-DEK protection to key wrapping (FCS_COP.1/KeyWrap) or authenticated encryption (FCS_COP.1/AEAD); the symmetric key encryption option remains available under the General-Purpose use case. The FCS_CKM_EXT.1 application note now states that the FCS_COP.1/SKC option provides confidentiality without modification-detection for wrapped key material and that compensating integrity mechanisms should be described in the TSS. A public-review question on retaining the SKC option in General-Purpose was added to the review page.

Version	Date	Description
0.4	2026-07-08	Bound the appendix-only mandatory statuses into the conformance machinery: Exact Conformance rule 1 now explicitly requires FCS_CKM.6 and at least one of FCS_COP.1/SKC or FCS_COP.1/AEAD. Rewrote FDP_DAR_EXT.1.2 (formerly an unfalsifiable "the TOE shall ensure … adheres to the Catalogue" statement) as a selection binding the FDP_DAR_EXT.1.1 encryption to the claimed FCS_COP.1/SKC and/or FCS_COP.1/AEAD components, with the ECD mirrored. SFR List type wording for FCS_CKM.6, FCS_COP.1/SKC, and FCS_COP.1/AEAD now describes, rather than legislates, the conformance requirement.
0.4	2026-07-08	Corrected the Enterprise Enhanced FCS_CKM.5 row against the Catalogue source: the SP 800-108 rows (KDF-CTR, KDF-FB, KDF-DPI) and the KDF-MAC-2S MAC step offer only AES-CMAC and HMAC-SHA-1/-256/-512 as PRFs, so the row now requires AES-256-CMAC or HMAC-SHA-512 for those rows and reaches SHA-384/SHA-512 only through the KDF-HASH and KDF-MAC-1S rows (the previous row text required HMAC-SHA-384 completions the Catalogue does not offer). Added a DBMS-iTC Application Note interpreting the reproduced FCS_RBG.1 dependency list: the seeding dependency is satisfied by FCS_RBG.2, FCS_RBG.3, or FCS_RBG.4 per the seeding architecture, and the primitive dependency applies per the selected DRBG type; the Catalogue text itself is unchanged. Editorial sweep: Exact Conformance cites CC:2022 Part 1 directly; Conventions iteration example corrected to a component of this module; deleted the P.CRYPTOGRAPHIC_STANDARDS configurability sentence that mapped to no management SFR; FCS_CKM_EXT.7 explicitly identified as not consumed; FCS_CKM.6 key-source dependency substitution justified in the dependency summary; FDP_ITC_EXT.1.2 certificate example moved out of element text; SD bibliography reference pinned to Version 0.4.

Version	Date	Description
0.4	2026-07-08	Added an application note to the FPT_TST.1/RBG and FPT_FLS.1/RBG iterations assigning their evaluation treatment to the Supporting Document: evaluation methods are expected from the Catalogue Evaluation Methods; until a scheme-recognized version is available, Certification Body-approved CMVP (FIPS 140-3) module-validation evidence may cover self-test execution and failure behavior, with the TOE-integration residue evaluated per the SD’s transitional coverage.

Preface

This PP-Module, the **DBMS Cryptographic Functions Module**, extends the collaborative Protection Profile for Database Management Systems (cPP_DBMS) to support secure cryptographic implementations.

This PP-Module **consumes the Common Criteria Cryptographic Catalogue** [[Crypto_Catalog]]. The DBMS-iTC does not originate, redefine, or replace the Catalogue SFRs, extended component definitions, dependencies, or algorithm-level Evaluation Activities reproduced in this document. Catalogue components are copied into this PP-Module so that they can be selected, completed, and evaluated as part of a conforming PP-Configuration. Each Catalogue-derived component is identified by its CCDB-018 identifier and source section, and every DBMS-specific modification is explicitly identified.

The DBMS-iTC originates only the database-specific requirements needed to apply those cryptographic components to a DBMS, including:

- **Key Hierarchy Management**: The management of Master Keys and Data Encryption Keys (DEKs).
- **Key Import and External Key Management**: The secure import of keys from external entities (BYOK) and integration with external key management services (e.g., KMIP-conformant key managers).
- **Encryption Strategy**: The scope of data-at-rest encryption (Storage-Scope vs. Granular).
- **Data-in-Transit Protection**: Mandatory protection of data transmitted between the TOE and external entities, using TLS and X.509 components claimed from the applicable Functional Packages.

This module must be used in conjunction with the cPP_DBMS. A conforming ST includes the Catalogue-derived components copied into this module when they are triggered by the TOE's implementation and completes their operations using the choices retained by this PP-Module.

Objectives of Document

This document expresses the security functional requirements for database-specific cryptographic operations and incorporates the standardized Catalogue components used to specify algorithm implementations.

Scope of Document

The scope of this PP-Module within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation, CC:2022. 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 may contain minor editorial errors, it is recognized as a living document and the iTC is dedicated to ongoing updates and revisions. Please report any issues to the DBMS-iTC.

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.
- [CCE] Common Criteria for Information Technology Security Evaluation, Errata and interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-002, Version 1.1, July 22, 2024.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2022-11-006, CEM:2022 Revision 1, November 2022.
- [SD] Supporting Document - Evaluation Activities for DBMS Cryptographic Functions Module, Version 0.4.
- [Crypto_Catalog] Specification of Functional Requirements for Cryptography (CCDB-018), Version 1.0, January 2025. Available at commoncriteria/crypto-catalog and commoncriteriaportal.org.
- [Crypto_Eval_Methods] Evaluation Methods for Cryptographic Security Functional Requirements, companion evaluation-methods document identified by CCDB-018. CCDB-018 states that this document will specify the Catalogue Evaluation Activities; use the version recognized by the responsible Certification Body when available.
- [TLS_FP] Functional Package for Transport Layer Security (TLS), Version 2.1, 2025-08-25. Available at commoncriteria.github.io/tls.
- [X509_FP] Functional Package for X.509 Certificates, Version 1.0. Available at commoncriteria.github.io/X509.
- [KMIP] OASIS Key Management Interoperability Protocol Specification, Version 2.1, OASIS Standard, 2020. Available at docs.oasis-open.org/kmip. Cited informatively; later versions are equally applicable.

- [FIPS_140_3] Security Requirements for Cryptographic Modules, FIPS PUB 140-3, March 2019. Available at nist.gov.
- [NIAP_APP_PP] Protection Profile for Application Software, Version 2.0, 16 June 2025. Available at niap-ccevs.org.
- [CNSA_2] Commercial National Security Algorithm Suite 2.0 Cybersecurity Advisory, PP-22-1338, Version 1.0, September 2022, and CNSA 2.0 FAQ, PP-24-4014, Version 2.1, December 2024. Available from nsa.gov and nsa.gov.
- [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_Cloud_MOD] collaborative PP-Module for DBMS in the Cloud, Version 0.4.

For more information, see the Common Criteria Portal.

Chapter 1. PP-Module Introduction

1.1. PP-Module Reference Identification

This section provides the formal identification of this PP-Module per ACE_INT requirements.

Table 2. PP-Module Identification

Attribute	Value
PP-Module Title	collaborative PP-Module for DBMS Cryptographic Functions
PP-Module Short Name	DBMS_MOD_CRYPTO
PP-Module Version	0.4
PP-Module Publication Date	2026-06-30
PP-Module Sponsor	Database Management Systems international Technical Community (DBMS-iTC)
CC Version	CC:2022
PP-Module Keywords	Database, DBMS, Cryptography, TDE, BYOK, KMIP, Key Management, Data-in-Transit, TLS, Crypto Catalogue

Chapter 2. PP-Module Base

This PP-Module requires the **collaborative Protection Profile for Database Management Systems (cPP_DBMS)** [[cPP_DBMS]] as its Base PP.

2.1. Allowed PP-Configurations

This PP-Module may be claimed in the following PP-Configurations:

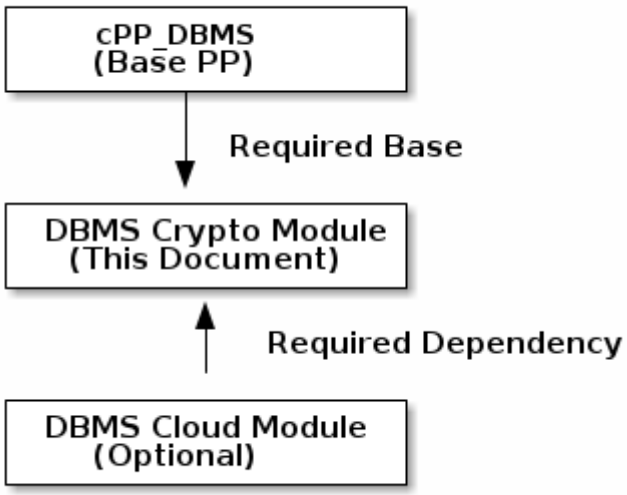
1. **cPP_DBMS + DBMS Cryptographic Module**

   This standalone configuration is used when a DBMS requires cryptographic protections (data-at-rest encryption, data-in-transit protection, key management, or key import) but is not deployed in a cloud environment.

2. **cPP_DBMS + DBMS Cloud Module + DBMS Cryptographic Module**

   This configuration is required when the DBMS Cloud Module [[DBMS_Cloud_MOD]] is claimed. The Cloud Module mandates the inclusion of this Crypto Module to provide Data-in-Transit protections using TLS, including HTTPS over TLS where applicable, and Data-at-Rest encryption protections. See the DBMS Cloud Module for full PP-Configuration requirements.

2.2. PP-Module Relationship Diagram



Application Note: When the DBMS Cloud Module is included in the PP-Configuration, this module is a mandatory dependency. When the DBMS Cloud Module is not included, this module may be claimed independently against the cPP_DBMS Base PP.

Chapter 3. TOE Overview

This PP-Module applies to the cryptographic functions of Database Management Systems (DBMS). It assumes the TOE implements cryptographic mechanisms for data protection.

3.1. TOE Type

The TOE type addressed by this PP-Module is: Database Management Systems implementing cryptographic protections for data-at-rest, data-in-transit, and Master Key management, including keys imported from or managed by external key management services.

3.2. TOE Scope

The TOE includes:

- Key management logic for data encryption keys (DEKs).
- Master key management functionality.
- Trusted channel interfaces for key import and external key management.
- TLS-protected communication channels between the TOE and external entities (client, management, audit export, key management, and other external service channels).

The TOE implements or invokes the cryptographic functions specified by the Catalogue-derived components included in this PP-Module. Standalone cryptographic libraries or HSM appliances that are not included in the TOE boundary are part of the operational environment; the ST shall identify the boundary and the mechanism by which the TOE invokes any environmental cryptographic service.

Chapter 4. TOE Use Cases

The use cases below follow the NIAP PP convention of identifying deployment-oriented requirement selections. Use cases do not create new SFRs. The ST shall identify every applicable use case and shall complete the Catalogue-derived SFR operations consistently with the corresponding selection template.

4.1. [USE CASE 1] General-Purpose Cryptographic Deployment

This use case applies to DBMS deployments that require cryptographic protection but are not required to use the Enterprise Enhanced selection template. The ST author may select any algorithm, mode, key size, construction method, and standard retained in the Catalogue-derived components of this PP-Module, subject to the component dependencies and acceptance by the applicable evaluation scheme.

4.2. [USE CASE 2] Enterprise Enhanced

This optional use case applies when a deployment requires the cryptographic selections applicable to this PP-Module to align with FIPS 140-3 [[FIPS_140_3]], current NIAP requirements represented by the Protection Profile for Application Software [[NIAP_APP_PP]], and CNSA 2.0 [[CNSA_2]]. The use case does not define new cryptographic SFRs or Evaluation Activities. It constrains operations in the consumed Catalogue components through Enterprise Enhanced Use Case Selection Template.

The Enterprise Enhanced use case addresses only cryptographic functions within the scope of this module, principally symmetric data protection, key derivation and protection, hashing, one-time values, and random bit generation. Protocol, certificate, asymmetric, and post-quantum requirements are supplied by the applicable Functional Packages or other Requirements Documents. Selection of this use case therefore demonstrates alignment of the in-scope operations; it does not by itself assert FIPS 140-3 validation, NIAP approval, CNSA 2.0 conformance for an entire product, or eligibility for any product list.

Chapter 5. CC Conformance Claims

This section describes the conformance claims for this PP-Module per ACE_CCL requirements defined in CC:2022. As a PP-Module, this document is evaluated under the ACE assurance class within the evaluation of a PP-Configuration that includes it.

5.1. Common Criteria Conformance

This PP-Module claims conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022, as follows:

- **CC Part 1 Conformance**: This PP-Module is consistent with CC:2022 Part 1 [[CC1]].
- **CC Part 2 Conformance**: This PP-Module is CC Part 2 extended, as it includes extended SFR components defined in Extended Component Definitions.
- **CC Part 3 Conformance**: This PP-Module is CC Part 3 conformant, as it does not define extended SAR components.

5.2. Package Conformance

A PP-Configuration including this PP-Module inherits the cPP_DBMS claim of conformance to the EAL2 assurance package defined in CC:2022 Part 5 [[CC5]], augmented by ALC_FLR.3 Systematic flaw remediation. This PP-Module does not introduce additional assurance package claims.

This PP-Module requires the following functional package claims:

- A Security Target claiming conformance to this PP-Module shall claim conformance to the Functional Package for Transport Layer Security (TLS), Version 2.1 [[TLS_FP]], including the TLS client or server components applicable to the TOE roles, to complete the channel requirements of `FDP_DIT_EXT.1` and, where "Imported from External Entity" or "Externally Managed" is selected in `FCS_CKM_EXT.1.1`, the mutual TLS channel required by `FDP_ITC_EXT.1`.
- A Security Target shall claim the applicable components of the Functional Package for X.509 Certificates, Version 1.0 [[X509_FP]], where certificate-based endpoint authentication is required by `FDP_DIT_EXT.1.2` or by the claimed TLS components.

Cryptographic components consumed from the Specification of Functional Requirements for Cryptography (CCDB-018) [[Crypto_Catalog]] are reproduced in Consumed Cryptographic Catalogue Components and do not constitute a separate package claim.

5.3. PP-Module Conformance Type

This PP-Module requires **Exact Conformance** from Security Targets claiming conformance.

5.3.1. Definition of Exact Conformance

Exact Conformance is defined in CC:2022 Part 1 [[CC1]]. A Security Target demonstrating Exact Conformance to this PP-Module must satisfy the following requirements:

1. **Mandatory SFRs**: The ST shall include all SFRs specified in Security Functional Requirements (Mandatory) of this PP-Module. The ST shall additionally include the Catalogue-derived components identified as Mandatory in the SFR List: FCS_CKM.6, and at least one of FCS_COP.1/SKC or FCS_COP.1/AEAD (as selected in FDP_DAR_EXT.1.2).
2. **Selection-Based SFRs**: The ST shall include SFRs from Security Functional Requirements (Selection-Based) when selections in mandatory SFRs trigger their inclusion. FCS_CKM.1/SKG is required when the TOE directly generates DEKs or internally generates MEKs. FDP_ITC_EXT.1 is required when "Imported from External Entity" or "Externally Managed" is selected in FCS_CKM_EXT.1.1.
3. **No Omissions**: No mandatory SFRs from Security Functional Requirements (Mandatory) may be omitted from the ST.
4. **Consumed Catalogue Components**: The ST shall include each Catalogue-derived component from Consumed Cryptographic Catalogue Components that is triggered by the TOE implementation and shall complete its operations using the choices retained by this PP-Module.
5. **Use Cases**: The ST shall identify the applicable use case or use cases. When Enterprise Enhanced is claimed, the ST shall satisfy Enterprise Enhanced Use Case Selection Template.
6. **No Additional Requirements**: While iteration is allowed, the ST shall not include additional requirements from CC Part 2 [[CC2]], CC Part 3 [[CC3]], or definitions of extended components not already included in this PP-Module, the Base PP (cPP_DBMS), another module in the claimed PP-Configuration, or a Functional Package claimed in accordance with Package Conformance.
7. **Iteration Permitted**: Iteration of SFRs is permitted to address multiple instances of a security requirement when necessary.
8. **Operations**: All assignments, selections, and refinements shall be completed in accordance with the SFR specifications in this PP-Module and the Base PP.

5.4. Conformance Claim Rationale

A Security Target or PP claiming conformance to this PP-Module shall include:

1. A statement identifying this PP-Module by title, version, and publication date.
2. A statement that the claimed PP-Configuration includes the required Base PP (cPP_DBMS).
3. A statement identifying the consumed Catalogue components included in the ST and the applicable use case or use cases.
4. A statement identifying the Functional Packages claimed in accordance with Package Conformance, by title and version.
5. A statement that the ST demonstrates Exact Conformance to this PP-Module.

Chapter 6. Security Problem Definition

6.1. Threats

This section describes the threats that the TOE is designed to address. Each threat identifies the threat agent, the adverse action, and the asset being protected, in accordance with CC:2022 requirements.

T.KEY_COMPROMISE

A malicious actor may obtain cryptographic keys (Master Keys or Data Encryption Keys) stored on the file system or in memory, enabling decryption of protected data. The threat agent may exploit insecure key storage, memory disclosure vulnerabilities, or unauthorized access to key management infrastructure. The assets at risk include Master Encryption Keys (MEKs), Data Encryption Keys (DEKs), and any data protected by those keys.

T.KEY_IMPORT_INTERCEPTION

A malicious actor may intercept or modify cryptographic keys or key-management traffic exchanged with an external entity (e.g., a Key Management System), compromising key material during one-time import or during ongoing external key-management operations. The threat agent may exploit insecure transport protocols, missing authentication of the key management endpoint, or man-in-the-middle positions on the network. The assets at risk include imported or externally managed Master Keys and the confidentiality and integrity of all data they subsequently protect.

T.WEAK_CRYPTO_IMPLEMENTATION

The TOE may incorrectly apply cryptographic algorithms or key management logic, resulting in data exposure. The threat agent may exploit non-standard algorithm implementations, weak key sizes, insecure modes of operation, or deviations from established standards to recover plaintext data or keys. The assets at risk include all data protected by the cryptographic functions of the TOE.

T.DATA_IN_TRANSIT_DISCLOSURE

A malicious actor may intercept, modify, or inject database data, credentials, or other sensitive data while it is transmitted between the TOE and external entities, including client-to-database connections, database-to-database connections, management and administrative channels, and connections to external services. The threat agent may exploit shared or untrusted networks, missing or weak transport protection, or a man-in-the-middle position. The assets at risk include the confidentiality and integrity of all data transmitted by the TOE to or from external entities.

6.2. Assumptions

This section describes the assumptions about the operational environment that must be satisfied for the TOE to provide its security functionality.

A.KEY_STORE_SECURITY

The operational environment provides secure storage for cryptographic key material (e.g.,

hardware security modules, secure enclaves, or encrypted filesystems) such that keys are protected from unauthorized physical or logical access. The environment ensures that:

- Key material at rest cannot be extracted from the storage medium without proper authorization;
- Access to key storage is protected by authentication and access control mechanisms independent of the TOE;
- The integrity of stored key material is protected against unauthorized modification.

6.3. Organizational Security Policies

This section defines the organizational security policies applicable to the cryptographic functions of the TOE.

P.CRYPTOGRAPHIC_STANDARDS

The organization shall require that the TOE implements cryptographic algorithms and key management practices in accordance with recognized standards. Specifically:

- Cryptographic algorithm selections shall comply with the requirements of the Common Criteria Cryptographic Catalogue [[Crypto_Catalog]];
- Key lengths and modes of operation shall meet the minimum requirements specified for the applicable assurance level;
- Deprecated or weak algorithms shall not be used for protecting sensitive data.

P.KEY_LIFECYCLE

The organization shall define and enforce a cryptographic key lifecycle policy that specifies:

- Procedures for key generation, including entropy requirements and approved generation methods;
- Key storage requirements, including protection of keys at rest;
- Key rotation schedules and procedures for re-encryption following rotation;
- Key destruction procedures to prevent unauthorized recovery of destroyed keys.

  The TOE must support these lifecycle operations through the key management functions defined in this PP-Module.

Chapter 7. Security Objectives

This section defines the security objectives that address the threats, assumptions, and organizational security policies identified in the Security Problem Definition.

7.1. Security Objectives for the TOE

O.KEY_HIERARCHY

The TOE shall enforce a key hierarchy where data encryption keys (DEKs) are generated or derived and protected by a Master Key (MEK), ensuring that DEKs are never stored in plaintext outside the TOE boundary.

O.MASTER_KEY_MANAGEMENT

The TOE shall provide functionality to generate or import Master Keys as selected in the ST and destroy Master Keys securely, supporting "Bring Your Own Key" (BYOK) scenarios where keys originate from external trusted sources.

O.TRUSTED_KEY_IMPORT

The TOE shall securely import cryptographic keys from, and exchange key-management communications with, external entities using trusted channels that provide confidentiality, integrity, and mutual authentication.

Application Note: This objective applies when "Imported from External Entity" or "Externally Managed" is selected in `FCS_CKM_EXT.1.1`. For a TOE that generates its Master Keys internally, no external key interface exists; the threat T.KEY_IMPORT_INTERCEPTION is vacuously countered, and this objective and FDP_ITC_EXT.1 apply together when either external origin is selected.

O.CATALOGUE_CONFORMANCE

The TOE shall implement cryptographic algorithms in accordance with the requirements defined in the Common Criteria Cryptographic Catalogue [[Crypto_Catalog]].

O.PROTECTED_TRANSIT

The TOE shall protect data transmitted between itself and external entities from unauthorized disclosure and modification using cryptographic protocols and certificate-authenticated endpoints specified by the Functional Package for TLS [[TLS_FP]] and the Functional Package for X.509 Certificates [[X509_FP]], as applicable.

7.2. Security Objectives for the Operational Environment

OE.KEY_STORE_PROTECTION

The operational environment shall provide secure storage for cryptographic key material. Storage shall protect keys from unauthorized physical and logical access through mechanisms such as hardware security modules (HSMs), trusted platform modules (TPMs), secure enclaves, or encrypted filesystems that prevent unauthorized extraction of stored keys. The environment shall ensure keys at rest cannot be extracted without proper authorization and that the integrity

of key material is maintained.

Chapter 8. Security Rationale

This section provides rationale showing how the defined security objectives address the identified threats and assumptions, and how the Security Functional Requirements (SFRs) satisfy the objectives. The rationale demonstrates completeness and consistency of the security problem definition, objectives, and requirements.

8.1. Threats to Objectives Mapping

The following table maps each threat to the security objectives that address it.

Threat	**Security Objectives Addressing the Threat**	**Rationale**
T.KEY_COMPROMISE	O.KEY_HIERARCHY O.MASTER_KEY_MANAGEMENT	Enforcing a key hierarchy (O.KEY_HIERARCHY) ensures that DEKs are always protected by the MEK and never stored in plaintext, limiting the impact of any single key compromise. Secure management of the MEK (O.MASTER_KEY_MANAGEMENT) prevents compromise of the root key from enabling bulk decryption.
T.KEY_IMPORT_INTERCEPTION	O.TRUSTED_KEY_IMPORT	When "Imported from External Entity" or "Externally Managed" is selected in `FCS_CKM_EXT.1.1`, establishing a trusted channel with confidentiality, integrity, and authentication controls (O.TRUSTED_KEY_IMPORT) prevents a malicious actor from intercepting or substituting key material during BYOK import or during ongoing external key-management exchanges.
T.WEAK_CRYPTO_IMPLEMENTATION	O.CATALOGUE_CONFORMANCE	Requiring the TOE to implement only algorithms and key sizes that appear in the Common Criteria Cryptographic Catalogue (O.CATALOGUE_CONFORMANCE) ensures that only proven, standards-compliant implementations are used, eliminating the risk of custom or weak algorithm usage.

Threat	Security Objectives Addressing the Threat	Rationale
T.DATA_IN_TRANSIT_DISCLOSURE	O.PROTECTED_TRANSIT	Requiring the TOE to protect all data transmitted to and from external entities using approved transport protocols with certificate-authenticated endpoints (O.PROTECTED_TRANSIT) provides confidentiality and integrity for data in transit and authenticates the communicating endpoints, preventing interception, modification, or injection on shared or untrusted networks.

8.2. Assumptions to Objectives Mapping

The following table maps each assumption to the operational environment objectives that uphold it.

Assumption	OE Objectives Upholding the Assumption	Rationale
A.KEY_STORE_SECURITY	OE.KEY_STORE_PROTECTION	The operational environment objective OE.KEY_STORE_PROTECTION directly requires the environment to provide secure physical and logical protection of key material, which is the exact property assumed in A.KEY_STORE_SECURITY. This includes hardware security modules (HSMs), secure enclaves, or encrypted filesystems that prevent unauthorized extraction of stored keys.

8.3. Objectives to SFRs Mapping

The following table maps each TOE security objective to the SFRs that satisfy it.

Security Objective for the TOE	SFRs Satisfying the Objective	Rationale
O.KEY_HIERARCHY	FCS_CKM.1/SKG (if DEKs are directly generated) FCS_CKM.5 or FCS_CKM_EXT.8 (if DEKs are derived) FDP_DAR_EXT.1 **Crypto Catalogue: FCS_COP.1/SKC and/or FCS_COP.1/AEAD**	FCS_CKM.1/SKG ensures directly generated DEKs are generated using the consumed random-bit-generation components when that path is used. When the TOE derives DEKs, the ST includes the applicable consumed derivation component (`FCS_CKM.5` or `FCS_CKM_EXT.8`) instead of `FCS_CKM.1/SKG` for the DEK path. FDP_DAR_EXT.1 enforces that user data encryption uses DEKs consistent with the hierarchy. The consumed `FCS_COP.1/SKC` and/or `FCS_COP.1/AEAD` components define the algorithms used to encrypt data with those DEKs.
O.MASTER_KEY_MANAGEMENT	FCS_CKM_EXT.1 **Crypto Catalogue: FCS_CKM.1/SKG and FCS_RBG.1 when MEKs are generated internally, FCS_CKM.6, and selected DEK protection operations**	FCS_CKM_EXT.1 manages the full MEK lifecycle including generation, import, DEK protection, and destruction. Internally generated MEKs require `FCS_CKM.1/SKG` and `FCS_RBG.1`; protected DEK storage requires the selected `FCS_COP.1/KeyWrap`, `FCS_COP.1/SKC`, or `FCS_COP.1/AEAD` claim; and `FCS_CKM.6` specifies the key destruction method to ensure MEKs cannot be recovered after destruction.
O.TRUSTED_KEY_IMPORT	FDP_ITC_EXT.1 (when an external Key Origin is selected) **TLS FP / Crypto Catalogue: mutual TLS channel components when an external Key Origin is selected**	FDP_ITC_EXT.1 defines the trusted channel requirements for key import and external key management, including confidentiality, integrity, and mutual authentication properties. The channel implementation is satisfied by the Functional Package for TLS v2.1 [[TLS_FP]] or the applicable TLS protocol component from the Crypto Catalogue [[Crypto_Catalog]].
O.CATALOGUE_CONFORMANCE	FCS_CKM.1/SKG (when direct symmetric key generation is claimed) FCS_CKM.5 or FCS_CKM_EXT.8 (when DEKs are derived) FDP_DAR_EXT.1 FDP_ITC_EXT.1 **Crypto Catalogue: All claimed components**	Each in-scope algorithm is specified by a Catalogue-derived component reproduced in this module. `FCS_CKM.1/SKG` requires the consumed RBG components when direct symmetric key generation is selected; derived DEKs require the applicable consumed key-derivation component; and FDP_DAR_EXT.1 requires a consumed symmetric or authenticated-encryption operation. FDP_ITC_EXT.1 requires a mutual TLS channel specified by the TLS Functional Package when key import is selected.

Security Objective for the TOE	SFRs Satisfying the Objective	Rationale
O.PROTECTED_TRANSIT	FDP_DIT_EXT.1 **TLS FP / X.509 FP / Crypto Catalogue: TLS and certificate-validation components**	FDP_DIT_EXT.1 requires the TOE to protect data in transit between itself and external entities. The channel implementation and endpoint authentication are satisfied by the Functional Package for TLS v2.1 [[TLS_FP]], the Functional Package for X.509 Certificates [[X509_FP]], or the applicable TLS and certificate-validation components from the Crypto Catalogue [[Crypto_Catalog]].

8.4. Consistency Summary

8.4.1. Threat Coverage

All threats defined in the Security Problem Definition are addressed by at least one security objective:

- T.KEY_COMPROMISE: Addressed by O.KEY_HIERARCHY, O.MASTER_KEY_MANAGEMENT
- T.KEY_IMPORT_INTERCEPTION: Addressed by O.TRUSTED_KEY_IMPORT when "Imported from External Entity" or "Externally Managed" is selected in FCS_CKM_EXT.1.1
- T.WEAK_CRYPTO_IMPLEMENTATION: Addressed by O.CATALOGUE_CONFORMANCE
- T.DATA_IN_TRANSIT_DISCLOSURE: Addressed by O.PROTECTED_TRANSIT

8.4.2. Assumption Coverage

All assumptions are upheld by operational environment objectives:

- A.KEY_STORE_SECURITY: Upheld by OE.KEY_STORE_PROTECTION

8.4.3. Policy Coverage

All organizational security policies are addressed by security objectives:

- P.CRYPTOGRAPHIC_STANDARDS: Addressed by O.CATALOGUE_CONFORMANCE, which requires all algorithms to comply with the Crypto Catalogue
- P.KEY_LIFECYCLE: Addressed by O.KEY_HIERARCHY (DEK generation or derivation), O.MASTER_KEY_MANAGEMENT (full MEK lifecycle), and O.TRUSTED_KEY_IMPORT when an external Key Origin is selected

8.4.4. Objective Coverage

All TOE security objectives are satisfied by SFRs:

- O.KEY_HIERARCHY: FCS_CKM.1/SKG when DEKs are directly generated, FCS_CKM.5 or FCS_CKM_EXT.8 when DEKs are derived, FDP_DAR_EXT.1
- O.MASTER_KEY_MANAGEMENT: FCS_CKM_EXT.1 and the consumed Catalogue components selected for internal MEK generation and DEK protection
- O.TRUSTED_KEY_IMPORT: FDP_ITC_EXT.1 when "Imported from External Entity" or "Externally Managed" is selected in FCS_CKM_EXT.1.1
- O.CATALOGUE_CONFORMANCE: Satisfied collectively by the Catalogue-derived components consumed in this PP-Module
- O.PROTECTED_TRANSIT: FDP_DIT_EXT.1 and the applicable TLS and X.509 Functional Package components

All OE objectives are either unconditional or have clear triggers linked to specific SFR selections.

Chapter 9. Security Functional Requirements

9.1. Conventions

The individual security functional requirements are specified in the sections below. The following conventions are used for SFR operations and module-specific refinements:

- **Refinement:** Additional or replacement text is shown in **bold**. Deleted text, when present, is shown as ~~**crossed out**~~.
- **Selection:** Selections are shown in square brackets using the CC operation designator, for example [selection: option one, option two].
- **Assignment:** Assignments are shown in square brackets using the CC operation designator, for example [assignment: *assignment value*].
- **Iteration:** A number or label in parentheses or after a slash following the SFR name indicates an iteration, for example FCS_CKM.1(1) or FCS_COP.1/SKC.

Extended SFRs are identified by having the label "EXT" in the SFR name.

Chapter 10. Security Functional Requirements (Mandatory)

10.1. FCS: Cryptographic Support (DBMS-Specific Requirements)

10.1.1. FCS_CKM_EXT.1 Cryptographic Key Management (Master Keys)

FCS_CKM_EXT.1.1 The TSF shall manage the lifecycle of the Master/Root Cryptographic Keys (MEKs) as follows:

- **Key Origin**: [selection: Generated Internally - The TSF shall generate the Master Key using the consumed FCS_CKM.1/SKG and FCS_RBG.1 components and store it securely within the TOE boundary; Imported from External Entity - The TSF shall import the Master Key from an external IT entity via the trusted channel defined in FDP_ITC_EXT.1, after which the TSF is the authoritative holder of the Master Key; Externally Managed - The TSF shall obtain use of the Master Key from an external key management service via the trusted channel defined in FDP_ITC_EXT.1, by retrieving the Master Key for transient use or by invoking Master Key operations by reference; the external service remains the authoritative store, and the TSF shall not persistently store plaintext Master Key material within the TOE boundary.]

FCS_CKM_EXT.1.2 The TSF shall protect the Master Key against disclosure and modification and shall protect stored DEKs under the Master Key using [selection: key wrapping claimed as FCS_COP.1/KeyWrap, symmetric key encryption claimed as FCS_COP.1/SKC, authenticated encryption claimed as FCS_COP.1/AEAD].

FCS_CKM_EXT.1.3 The TSF shall destroy Master Keys in accordance with the key destruction requirements specified in the Crypto Catalogue (FCS_CKM.6).

Application Note: This requirement models the DBMS-specific behavior of managing a root key (e.g., TDE Master Key). Three Key Origins are defined: internal generation; one-time import in which custody of the Master Key transfers to the TOE (e.g., BYOK); and external management, in which an external key management service — for example, a KMIP-conformant key manager [[KMIP]] — remains the authoritative store and the TOE retrieves the Master Key for transient use or invokes its operations by reference. When "Imported from External Entity" or "Externally Managed" is selected, FDP_ITC_EXT.1 must be included in the ST; KMIP or an equivalent key-management protocol is a message layer carried over that trusted channel and the protocol itself is not evaluated. The DEK protection selection in FCS_CKM_EXT.1.2 triggers the consumed FCS_COP.1/KeyWrap, FCS_COP.1/SKC, or FCS_COP.1/AEAD component when the TSF performs the DEK wrap or unwrap; where "Externally Managed" is selected and the external service performs those operations by reference, the ST identifies that allocation and claims the FCS_COP components only for TSF-implemented operations — the trusted channel, the no-plaintext-persistence property, and DEK handling within the TOE remain TSF obligations. The symmetric key encryption option (FCS_COP.1/SKC) provides confidentiality for stored DEKs but does not itself detect unauthorized modification of the wrapped key material; an ST selecting it should describe in the TSS any compensating integrity mechanisms (for example, keystore-container integrity protection). The

Enterprise Enhanced use case does not permit this option (see Enterprise Enhanced Use Case Selection Template). For the "Externally Managed" origin, FCS_CKM_EXT.1.3 applies to Master Key copies transiently held by the TSF; authoritative destruction of the Master Key is performed by the external service. If the selected operation has a Catalogue dependency on one-time values, the ST shall include FCS_OTV_EXT.1.

10.1.1.1. Dependencies

Dependency	Resolution
FCS_CKM.6 Cryptographic Key Destruction (Timing and Event)	Satisfied by the consumed FCS_CKM.6 component in FCS_CKM.6 Timing and Event of Cryptographic Key Destruction.
FCS_CKM.1/SKG and FCS_RBG.1 Symmetric Key Generation (conditional)	Satisfied by the consumed FCS_CKM.1/SKG and FCS_RBG.1 components when "Generated Internally" is selected in FCS_CKM_EXT.1.1 for MEK generation.
FCS_COP.1/KeyWrap, FCS_COP.1/SKC, or FCS_COP.1/AEAD DEK Protection Operation	Satisfied by the applicable consumed FCS_COP.1/KeyWrap, FCS_COP.1/SKC, or FCS_COP.1/AEAD component. FCS_OTV_EXT.1 is required when the selected operation has an IV, nonce, tweak, or other one-time-value dependency.
FDP_ITC_EXT.1 Trusted Channel for Key Import and External Key Management (conditional)	Satisfied by FDP_ITC_EXT.1 in this PP-Module. Required when "Imported from External Entity" or "Externally Managed" is selected in FCS_CKM_EXT.1.1.

10.2. FDP: User Data Protection

10.2.1. FDP_DAR_EXT.1 Data-at-Rest Encryption Strategy

FDP_DAR_EXT.1.1 The TSF shall enforce a Data-at-Rest Encryption strategy as follows:

- [selection: Storage-Scope Encryption - The TSF shall encrypt the persistent database storage objects identified in the ST and TSS using algorithms selected in the consumed Catalogue components, with only documented exclusions that do not contain plaintext user data or that are protected by an equivalent specified mechanism; Granular Data Encryption - The TSF shall encrypt specific data elements (e.g., columns, cells) using algorithms selected in the consumed Catalogue components.]

FDP_DAR_EXT.1.2 The TSF shall perform the encryption specified in FDP_DAR_EXT.1.1 using the cryptographic operations claimed in the included [selection: FCS_COP.1/SKC, FCS_COP.1/AEAD] components.

Application Note: The ST author must select the encryption strategy appropriate for the TOE. The FDP_DAR_EXT.1.2 selection binds the data-at-rest encryption to the consumed Catalogue components: at least one of FCS_COP.1/SKC or FCS_COP.1/AEAD must be selected and included, and the algorithms and modes evaluated are those claimed in the included components. For Storage-Scope Encryption, the ST and TSS must identify covered storage-object categories and any exclusions (for example, metadata, diagnostic files, or externally protected artifacts) with a rationale demonstrating that the exclusion does not contradict the requirement to protect database user data

at rest.

10.2.1.1. Dependencies

Dependency	Resolution
FCS_COP.1/SKC Cryptographic Operation (Symmetric-Key Cryptography) and/or FCS_COP.1/AEAD Authenticated Encryption with Associated Data	Satisfied by the consumed `FCS_COP.1/SKC` component for non-AEAD symmetric encryption modes and/or `FCS_COP.1/AEAD` when the data-at-rest encryption operation is an authenticated encryption mode (e.g., AES-GCM).
FCS_OTV_EXT.1 One-Time Values (conditional)	Satisfied by the consumed `FCS_OTV_EXT.1` component when the selected `FCS_COP.1/SKC`, `FCS_COP.1/AEAD`, or related mode requires IVs, nonces, tweaks, or other one-time values.
FCS_CKM_EXT.1 Cryptographic Key Management (Master Keys)	Satisfied by FCS_CKM_EXT.1 in this PP-Module, which manages the DEK protection hierarchy.

10.2.2. FDP_DIT_EXT.1 Data-in-Transit Protection

FDP_DIT_EXT.1.1 The TSF shall protect data in transit between the TOE and external entities from unauthorized disclosure and modification using TLS as claimed from the Functional Package for TLS v2.1 [[TLS_FP]] and [selection: **no other cryptographic protocol**, [assignment: *other cryptographic protocol claimed from an applicable Functional Package*]].

FDP_DIT_EXT.1.2 The TSF shall authenticate the endpoints of the protected channel using X.509 certificates claimed from the Functional Package for X.509 Certificates [[X509_FP]], where required by the selected protocol.

Application Note: This requirement is mandatory. It applies to all data transmitted between the TOE and external entities, including client-to-database connections, database-to-database connections, management and administrative channels, audit export channels, and connections to external services such as identity providers and key management services. The Base PP does not define cryptographic data-in-transit protection; it relies on the operational-environment assumption A.CONNECT. For any PP-Configuration that includes this module, this requirement supplements A.CONNECT with TOE-enforced protection for channels between the TOE and external entities; A.CONNECT is retained and continues to cover what the TOE does not enforce (see Consistency with the Base PP Data-in-Transit Treatment). TLS is mandatory for every conforming TOE: the element requires the TLS Functional Package claim directly, and the selection governs only whether an additional protocol supplements TLS. A novel or proprietary data-in-transit mechanism does not substitute for the TLS claim. Supplementary protocols are permitted only where claimed from an applicable Functional Package with scheme-acceptable Evaluation Activities and implemented within the TOE boundary; protocols implemented by the underlying operating system or kernel (for example, IPsec) are outside the TOE boundary in this module's composition model and cannot be used to satisfy this requirement, although they may be present in the operational environment as defense in depth. HTTPS is treated as HTTP over the claimed TLS channel and does not require a separate HTTPS component claim. CCDB-018 specifies cryptographic primitives and does not specify TLS or certificate validation components.

10.2.2.1. Dependencies

Dependency	Resolution
FCS_TLSC_EXT.1 / FCS_TLSS_EXT.1 TLS components (when TLS is selected)	Satisfied by the Functional Package for TLS v2.1 [[TLS_FP]]. The ST author claims the applicable TLS client or server component for the TOE role.
FIA_X509_EXT certificate-validation components (when certificate authentication is used)	Satisfied by the Functional Package for X.509 Certificates [[X509_FP]].
Protocol-specific cryptographic components (when another protocol is selected)	Satisfied by the applicable Functional Package identified in the ST.

Chapter 11. Security Functional Requirements (Selection-Based)

These SFRs apply only when triggered by selections in mandatory SFRs or when the TOE implements the corresponding functionality.

11.1. FCS: Cryptographic Support (Consumed Catalogue Components)

The Catalogue-derived selection-based cryptographic requirements are reproduced in Consumed Cryptographic Catalogue Components. `FCS_CKM.1/SKG` is included when the TOE directly generates DEKs or internally generates MEKs. `FCS_CKM.5` or `FCS_CKM_EXT.8` is included when the TOE derives DEKs. The supporting cryptographic operation, one-time-value, random-bit-generation, seeding, failure, and self-test components are included as triggered by those selections.

11.2. FDP: User Data Protection

11.2.1. FDP_ITC_EXT.1 Trusted Channel for Key Import and External Key Management

FDP_ITC_EXT.1.1 The TSF shall be capable of establishing a trusted channel between itself and an external key management entity for the purpose of importing cryptographic keys or communicating with an external key management service.

FDP_ITC_EXT.1.2 The TSF shall ensure the trusted channel provides:

- **Confidentiality**: Protection against disclosure.
- **Integrity**: Protection against modification.
- **Authentication**: Mutual Authentication - The TOE shall authenticate the external entity, and the external entity shall authenticate the TOE.

FDP_ITC_EXT.1.3 The trusted channel shall be implemented using mutual TLS claimed from the Functional Package for TLS v2.1 [[TLS_FP]].

Application Note: This SFR is required when "Imported from External Entity" or "Externally Managed" is selected in `FCS_CKM_EXT.1.1`. It covers both one-time key import (e.g., BYOK) and ongoing external key-management integration (e.g., a KMIP-conformant key manager [[KMIP]]); the key-management protocol messages are carried over the mutual TLS channel, and the protocol itself is not evaluated — the channel protection and the key-handling properties of `FCS_CKM_EXT.1` are. Mutual TLS is mandatory for both paths.

11.2.1.1. Dependencies

Dependency	Resolution
FCS_TLSC_EXT.1 / FCS_TLSS_EXT.1 mutual TLS components	Satisfied by Functional Package for TLS v2.1 [[TLS_FP]]. The ST author must claim the applicable TLS client or server component for the TOE role, including the selections and certificate-authentication support needed for mutual TLS.

11.3. FCS/FDP Class Dependencies Summary

Table 3. FCS/FDP Class Dependency Resolution

SFR	Dependencies	Resolution
FCS_CKM.1/SKG	FCS_RBG.1 (CCDB-018 Section 6.2)	Consumed Catalogue components when the TOE directly generates DEKs or internally generates MEKs. If DEKs are derived, the ST includes `FCS_CKM.5` or `FCS_CKM_EXT.8` for the derivation path.
FCS_CKM_EXT.1	FCS_CKM.6 (CCDB-018 Section 3.7); FCS_CKM.1/SKG and FCS_RBG.1 (when MEKs are generated internally); selected `FCS_COP.1/KeyWrap`, `FCS_COP.1/SKC`, or `FCS_COP.1/AEAD` for DEK protection; `FCS_OTV_EXT.1` when required; FDP_ITC_EXT.1 (when import selected)	Crypto Catalogue (FCS_CKM.6 and selected key-generation/protection claims); FDP_ITC_EXT.1 (this module, when import selected)
FDP_DAR_EXT.1	FCS_COP.1/SKC (CCDB-018 Section 4.10) and/or FCS_COP.1/AEAD (CCDB-018 Section 4.2) as applicable to the selected encryption mode; FCS_OTV_EXT.1 (when required by the selected mode); FCS_CKM_EXT.1	Consumed `FCS_COP.1/SKC` and/or `FCS_COP.1/AEAD`, plus consumed `FCS_OTV_EXT.1` when required; FCS_CKM_EXT.1 is defined by this module
FDP_ITC_EXT.1	FCS_TLSC_EXT.1 / FCS_TLSS_EXT.1 mutual TLS components	Functional Package for TLS v2.1 [[TLS_FP]]
FDP_DIT_EXT.1	FCS_TLSC_EXT.1 / FCS_TLSS_EXT.1 TLS components (when TLS selected); FIA_X509_EXT certificate-validation components (when certificate authentication used); protocol-specific components (when another protocol selected)	Functional Package for TLS v2.1 [[TLS_FP]] and Functional Package for X.509 Certificates [[X509_FP]], as applicable

Chapter 12. Security Assurance Requirements (SARs)

This PP-Module does not define additional Security Assurance Requirements beyond those already specified by the collaborative Protection Profile for Database Management Systems (cPP_DBMS) Version 2.0.

All SARs defined in the cPP_DBMS apply directly and fully to TOEs claiming conformance with this DBMS Cryptographic Functions Module.

12.1. SAR Inheritance

The following SAR families, as defined in the cPP_DBMS, are inherited unchanged:

- ADV: Development
- AGD: Guidance Documents
- ALC: Life-cycle Support
- ASE: Security Target Evaluation
- ATE: Tests
- AVA: Vulnerability Assessment

No additional or modified SARs are introduced by this PP-Module.

The applicable SAR set is inherited from cPP_DBMS Version 2.0: EAL2 as defined in CC:2022 Part 5 [[CC5]], augmented by ALC_FLR.3 Systematic flaw remediation.

Appendix A: Consumed Cryptographic Catalogue Components

This section reproduces the operative CCDB-018 component content used by this PP-Module. Unless a modification is identified in the provenance statement for a component, the requirement, dependencies, and retained selection rows preserve the substance of the **Specification of Functional Requirements for Cryptography**, Version 1.0 [[Crypto_Catalog]]; Catalogue Application Notes are carried forward with editorial condensation where needed for the AsciiDoc presentation. The DBMS-iTC is the consumer of this material and is not its originator.

A.1. Component Applicability

The Security Target shall include the following Catalogue-derived components when applicable to the TOE implementation:

1. **Symmetric or Authenticated Encryption**: To satisfy `FDP_DAR_EXT.1` and support DEK-based data encryption.

   Consumed components: `FCS_COP.1/SKC` for non-AEAD modes and/or `FCS_COP.1/AEAD` for authenticated encryption modes, as applicable to the selected operation. The ST shall include `FCS_COP.1/AEAD` when an authenticated encryption mode is used.

2. **Hashing**: When a selected KDF, RBG, signature-verification, or other consumed component depends on hashing.

   Consumed component: `FCS_COP.1/Hash` with the algorithm and standard selected from the retained Catalogue choices.

3. **Key Destruction**: To satisfy `FCS_CKM_EXT.1.3`.

   Consumed component: `FCS_CKM.6` (Timing and Event of Cryptographic Key Destruction, Section 3.7).

A.2. Conditional Component Inclusion

The Security Target **shall** include the following components when the indicated SFR selection is made:

Condition	Consumed Catalogue Component	Triggering SFR
DEKs are derived from existing keying material or other non-password derivation inputs	`FCS_CKM.5` Key Derivation, plus the supporting primitive claims required by the selected derivation function	FCS_CKM.1/SKG application note; FCS_CKM_EXT.1

Condition	Consumed Catalogue Component	Triggering SFR
DEKs are derived from a password or passphrase	FCS_CKM_EXT.8 Password-based Key Derivation, plus the supporting primitive claims required by the selected derivation function	FCS_CKM.1/SKG application note; FCS_CKM_EXT.1
"Generated Internally" selected for MEK origin in FCS_CKM_EXT.1.1	FCS_CKM.1/SKG and FCS_RBG.1 for MEK generation	FCS_CKM_EXT.1
TOE directly generates DEKs	FCS_CKM.1/SKG and FCS_RBG.1 for DEK generation	FCS_CKM.1/SKG
Key wrapping selected for DEK protection in FCS_CKM_EXT.1.2	FCS_COP.1/KeyWrap, plus FCS_OTV_EXT.1 when required by the selected Catalogue operation	FCS_CKM_EXT.1
Symmetric key encryption or authenticated encryption selected for DEK protection in FCS_CKM_EXT.1.2	FCS_COP.1/SKC or FCS_COP.1/AEAD, plus FCS_OTV_EXT.1 when required by the selected mode	FCS_CKM_EXT.1
Any claimed data encryption, key protection, or key wrapping operation has a Catalogue dependency on IVs, nonces, tweaks, or other one-time values	FCS_OTV_EXT.1 One-Time Values	FDP_DAR_EXT.1; FCS_CKM_EXT.1
TOE verifies signatures for an in-scope DBMS function such as autonomous or provider-managed update verification	FCS_COP.1/SigVer plus FCS_COP.1/Hash or FCS_COP.1/XOF, as applicable	Triggering update or integrity-verification requirement in the claimed PP-Configuration

Condition	Consumed Catalogue Component	Triggering SFR
"Imported from External Entity" or "Externally Managed" selected in FCS_CKM_EXT.1.1	Mutual TLS client or server components from Functional Package for TLS v2.1 [[TLS_FP]], as applicable to the TOE role	FDP_ITC_EXT.1
Certificate-based mutual TLS authentication requires signature generation or verification support not otherwise covered by the selected TLS component	Applicable asymmetric algorithm components as required by the TLS Functional Package selections	FDP_ITC_EXT.1

A.3. Catalogue-Derived Key Management Components

Catalogue Guidance Notes are not carried forward, consistent with CCDB-018 Section 2.2. The component text and Application Notes below are Catalogue material. DBMS-specific triggering conditions appear only in Component Applicability and Conditional Component Inclusion.

A.3.1. FCS_CKM.1/SKG Cryptographic Key Generation - Symmetric Key

Source and modification: CCDB-018 Section 3.3. The RSK row is copied without substantive modification. DBMS-specific uses of generated keys are specified separately in `FCS_CKM_EXT.1` and `FDP_DAR_EXT.1`.

Hierarchical to: No other components.

Dependencies: [`FCS_CKM.2`, `FCS_CKM.5`, `FCS_CKM_EXT.7`, or `FCS_COP.1`]; `FCS_CKM.6`; [`FCS_RBG.1` or `FCS_RNG.1`].

FCS_CKM.1.1/SKG The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: cryptographic key generation algorithm] and specified cryptographic key sizes [selection: cryptographic key sizes] that meet the following: [selection: list of standards].

Table 4. Allowed completion of FCS_CKM.1/SKG

Identifier	Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	List of Standards
RSK	Direct Generation from a Random Bit Generator as specified in `FCS_RBG.1`	[selection: 128, 192, 256, 512] bits	NIST SP 800-133 Revision 2, Section 6.1

Application Note: Include this component when the TOE creates symmetric keys directly from the output of an RBG without further conditioning. Use FCS_CKM.5 for keys derived from other keying material and FCS_CKM_EXT.8 for keys derived from passwords; both are consumed in this PP-Module. FCS_CKM_EXT.7 (keys derived from material contributed by multiple parties) is not consumed in this PP-Module — multi-party key derivation is outside its scope, and references to it in reproduced Catalogue dependency lists are retained only as Catalogue context.

A.3.2. FCS_CKM.5 Cryptographic Key Derivation

Source and modification: CCDB-018 Section 3.6. All Catalogue rows are retained. The component is included only when the TOE derives an in-scope DBMS key from non-password input.

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or FCS_COP.1]; FCS_CKM.6; [FCS_COP.1/CMAC, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_COP.1/SKC, or FCS_COP.1/AEAD].

FCS_CKM.5.1 The TSF shall derive cryptographic keys [selection: key type] from [selection: input parameters] in accordance with a specified cryptographic key derivation algorithm [selection: key derivation algorithm] and specified cryptographic key sizes [selection: key sizes] that meet the following: [selection: list of standards].

Table 5. Allowed completions of FCS_CKM.5

Key Type	Input Parameters	Key Derivation Algorithm	Key Sizes	List of Standards
KDF-CTR	[selection: direct generation from an RBG as specified in FCS_RBG.1, concatenated keys]	KPF2 - KDF in Counter Mode using [selection: AES-128-CMAC, AES-192-CMAC, AES-256-CMAC, Camellia-128-CMAC, Camellia-192-CMAC, Camellia-256-CMAC, CMAC-HIGHT-128, CMAC-LEA-128, CMAC-LEA-256, CMAC-SEED-128, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] as the PRF	[selection: 128, 192, 256, 512] bits	[selection: ISO/IEC 11770-6:2016, 7.3.2; NIST SP 800-108 Revision 1 Update 1, 4.1]
KDF-FB	[selection: direct generation from an RBG as specified in FCS_RBG.1, concatenated keys]	KPF3 - KDF in Feedback Mode using [selection: AES-128-CMAC, AES-192-CMAC, AES-256-CMAC, Camellia-128-CMAC, Camellia-192-CMAC, Camellia-256-CMAC, CMAC-HIGHT-128, CMAC-LEA-128, CMAC-LEA-256, CMAC-SEED-128, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] as the PRF	[selection: 128, 192, 256, 512] bits	[selection: ISO/IEC 11770-6:2016, 7.3.3; NIST SP 800-108 Revision 1 Update 1, 4.2]

Key Type	Input Parameters	Key Derivation Algorithm	Key Sizes	List of Standards
KDF-DPI	[selection: direct generation from an RBG as specified in FCS_RBG.1, concatenated keys]	KPF4 - KDF in Double-Pipeline Iteration Mode using [selection: AES-128-CMAC, AES-192-CMAC, AES-256-CMAC, Camellia-128-CMAC, Camellia-192-CMAC, Camellia-256-CMAC, CMAC-HIGHT-128, CMAC-LEA-128, CMAC-LEA-256, CMAC-SEED-128, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] as the PRF	[selection: 128, 192, 256, 512] bits	[selection: ISO/IEC 11770-6:2016, 7.3.4; NIST SP 800-108 Revision 1 Update 1, 4.3]
KDF-XOR	More than one intermediary key	Exclusive OR (XOR)	[selection: 128, 192, 256, 512] bits	N/A
KDF-ENC	Two keys	Encrypting using an algorithm specified in [selection: FCS_COP.1/SKC, FCS_COP.1/AEAD]	[selection: 128, 192, 256, 512] bits	N/A
KDF-HASH	Shared secret	Hash function from FCS_COP.1/Hash	[selection: 128, 192, 256, 512] bits	NIST SP 800-56C Revision 2, Section 4.1, Option 1
KDF-MAC-1S	Shared secret, salt, output length, fixed information	Keyed hash function from FCS_COP.1/KeyedHash	[selection: 128, 192, 256, 512] bits	NIST SP 800-56C Revision 2, Section 4.1, Options 2 and 3
KDF-MAC-2S	Shared secret, salt, IV, output length, fixed information	MAC step using [selection: AES-128-CMAC, AES-192-CMAC, AES-256-CMAC, Camellia-128-CMAC, Camellia-192-CMAC, Camellia-256-CMAC, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] and KDF step using [selection: KDF-CTR, KDF-FB, KDF-DPI] with a selected PRF	[selection: 128, 192, 256, 512] bits	NIST SP 800-56C Revision 2, Section 5

Key Type	Input Parameters	Key Derivation Algorithm	Key Sizes	List of Standards
KDF-KMAC	Key, context string, output length, label	[selection: KMAC128, KMAC256]	[selection: 128, 192, 256, 512] bits	NIST SP 800-108 Revision 1 Update 1, Section 4.4

Application Note: In KDF-MAC-2S, if a CMAC is selected in the MAC step, select AES-128-CMAC or Camellia-128-CMAC in the KDF step and select 128 as the output key size. If HMAC is selected in the MAC step, select the same HMAC in the KDF. The respective FCS_COP.1 component must be included for each primitive selected in the key derivation algorithm.

A.3.3. FCS_CKM.6 Timing and Event of Cryptographic Key Destruction

Source and modification: CCDB-018 Section 3.7. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM_EXT.3, FCS_CKM.5, FCS_CKM_EXT.7, or FCS_CKM_EXT.8].

FCS_CKM.6.1 The TSF shall destroy [assignment: list of cryptographic keys, including keying material] when [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [selection:

1. for volatile memory: [selection: a single overwrite consisting of [selection: a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of a key, [assignment: a value that does not contain any CSP]], removal of power to the memory, removal of all references to the key directly followed by a request for garbage collection];
2. for non-volatile memory that employs a wear-leveling algorithm: [selection: a single overwrite consisting of [selection: zeroes, ones, a pseudo-random pattern, a new value of a key of the same size, [assignment: a value that does not contain any CSP]], block erase];
3. for non-volatile memory that does not employ a wear-leveling algorithm: [selection: a [selection: single, [assignment: ST-author-defined multi-pass]] overwrite consisting of [selection: zeroes, ones, a pseudo-random pattern, a new value of a key of the same size, [assignment: a value that does not contain any CSP]] followed by read-verify and repeated up to [assignment: number of attempts] times on failure, block erase]

] that meets the following: [no standard].

Application Note: The first assignment in FCS_CKM.6.1 lists all keys and keying material subject to destruction, including intermediate keys, encryption keys, seeds, authentication secrets, passwords, PINs, and other secret values used to derive keys. The requirement does not apply to public components of asymmetric key pairs or keys permitted to remain stored. Block erase applies only to flash memory. A value selected for overwrite shall not itself contain a CSP.

A.3.4. FCS_CKM_EXT.8 Password-Based Key Derivation

Source and modification: CCDB-018 Section 3.9. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2, FCS_COP.1, or FCS_CKM_EXT.7]; FCS_CKM.6; FCS_OTV_EXT.1.

FCS_CKM_EXT.8.1 The TSF shall perform password-based key derivation functions in accordance with a specified cryptographic algorithm [HMAC-[selection: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512]], with iteration count of [assignment: number of iterations] using a randomly generated salt of length [assignment: equal to or greater than 128] bits and output cryptographic key sizes [selection: 128, 192, 256, 512] bits that meet the following standard: [NIST SP 800-132, Section 5.3, PBKDF2].

Application Note: NIST recommends a minimum iteration count of 1000 and prefers the largest number feasible given performance constraints. The randomly generated portion of the salt should be at least 128 bits and shall be derived from random bit generation; therefore FCS_OTV_EXT.1 is included.

A.4. Catalogue-Derived Cryptographic Operation Components

A.4.1. FCS_COP.1/AEAD Authenticated Encryption with Associated Data

Source and modification: CCDB-018 Section 4.2. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.5, FCS_CKM_EXT.7, or FCS_CKM_EXT.8]; FCS_CKM.6; FCS_OTV_EXT.1.

FCS_COP.1.1/AEAD The TSF shall perform [authenticated encryption with associated data] in accordance with a specified cryptographic algorithm [selection: cryptographic algorithm] and cryptographic key sizes [selection: cryptographic key sizes] that meet the following: [selection: list of standards].

Table 6. Allowed completions of FCS_COP.1/AEAD

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
AES-CCM	AES in CCM mode with a non-repeating nonce of at least 64 bits	[selection: 128, 192, 256] bits	[selection: ISO/IEC 18033-3:2010, FIPS PUB 197] and [selection: ISO/IEC 19772:2020, NIST SP 800-38C]

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
AES-GCM	AES in GCM mode with non-repeating IVs using [selection: deterministic, RBG-based] IV construction and a tag length of [selection: 96, 104, 112, 120, 128] bits	[selection: 128, 192, 256] bits	[selection: ISO/IEC 18033-3:2010, FIPS PUB 197] and [selection: ISO/IEC 19772:2020, NIST SP 800-38D]
CAM-CCM	Camellia in CCM mode with a non-repeating nonce of at least 64 bits	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 19772:2020, NIST SP 800-38C]
CAM-GCM	Camellia in GCM mode with non-repeating IVs using [selection: deterministic, RBG-based] IV construction and a tag length of [selection: 96, 104, 112, 120, 128] bits	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 19772:2020, NIST SP 800-38D]
SEED-CCM	SEED in CCM mode with an unpredictable, non-repeating nonce of at least 64 bits	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 19772:2020, NIST SP 800-38C]
SEED-GCM	SEED in GCM mode with non-repeating IVs using [selection: deterministic, RBG-based] IV construction and a tag length of [selection: 96, 104, 112, 120, 128] bits	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 19772:2020, NIST SP 800-38D]
LEA-CCM	LEA in CCM mode with an unpredictable, non-repeating nonce of at least 64 bits	[selection: 128, 192, 256] bits	ISO/IEC 29192-2:2019 and [selection: ISO/IEC 19772:2020, NIST SP 800-38C]
LEA-GCM	LEA in GCM mode with non-repeating IVs using [selection: deterministic, RBG-based] IV construction and a tag length of [selection: 96, 104, 112, 120, 128] bits	[selection: 128, 192, 256] bits	ISO/IEC 29192-2:2019 and [selection: ISO/IEC 19772:2020, NIST SP 800-38D]

Application Note: If the selected cryptographic algorithm requires an IV or nonce, `FCS_OTV_EXT.1` is included.

A.4.2. FCS_COP.1/CMAC Cryptographic Operation - CMAC

Source and modification: CCDB-018 Section 4.3. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.5, FCS_CKM_EXT.7, or FCS_CKM_EXT.8]; FCS_CKM.6.

FCS_COP.1.1/CMAC The TSF shall perform [CMAC] in accordance with a specified cryptographic algorithm [selection: cryptographic algorithm] and cryptographic key sizes [selection: cryptographic key sizes] that meet the following: [selection: list of standards].

Table 7. Allowed completions of FCS_COP.1/CMAC

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
AES-CMAC	AES using CMAC mode	[selection: 128, 192, 256] bits	[selection: ISO/IEC 18033-3:2010, FIPS PUB 197] and [selection: ISO/IEC 9797-1:2011, NIST SP 800-38B]
CAM-CMAC	Camellia using CMAC mode	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 9797-1:2011, NIST SP 800-38B]

A.4.3. FCS_COP.1/Hash Cryptographic Operation - Hashing

Source and modification: CCDB-018 Section 4.4. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_COP.1.1/Hash The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [selection: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512] that meets the following: [selection: ISO/IEC 10118-3:2018, FIPS PUB 180-4, FIPS PUB 202].

Application Note: The hash selection should be consistent with the strength of the operation it supports. SHA-1 shall not be used where collision resistance is required; its retained uses are limited to the applications permitted by the Catalogue and the applicable scheme.

A.4.4. FCS_COP.1/KeyedHash Cryptographic Operation - Keyed Hash

Source and modification: CCDB-018 Section 4.5. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.5, FCS_CKM_EXT.7, or FCS_CKM_EXT.8]; FCS_CKM.6; [FCS_COP.1/Hash or FCS_COP.1/XOF].

FCS_COP.1.1/KeyedHash The TSF shall perform [keyed hash message authentication] in accordance with a specified cryptographic algorithm [selection: keyed hash algorithm] and cryptographic key sizes [selection: cryptographic key size] that meet the following: [selection: list of standards].

Table 8. Allowed completions of FCS_COP.1/KeyedHash

Keyed Hash Algorithm	Cryptographic Key Sizes	List of Standards
HMAC-SHA-1	[selection: (ISO/FIPS) 160, (FIPS) 128] bits	[selection: ISO/IEC 9797-2:2021, FIPS PUB 198-1]
HMAC-SHA-224	[selection: (ISO/FIPS) 224, (FIPS) 192, 128] bits	[selection: ISO/IEC 9797-2:2021, FIPS PUB 198-1]
HMAC-SHA-256	[selection: (ISO/FIPS) 256, (FIPS) 192, 128] bits	[selection: ISO/IEC 9797-2:2021, FIPS PUB 198-1]
HMAC-SHA-384	[selection: (ISO/FIPS) 384, (FIPS) 256, 192, 128] bits	[selection: ISO/IEC 9797-2:2021, FIPS PUB 198-1]
HMAC-SHA-512	[selection: (ISO/FIPS) 512, (FIPS) 384, 256, 192, 128] bits	[selection: ISO/IEC 9797-2:2021, FIPS PUB 198-1]
KMAC128	128 bits	[selection: ISO/IEC 9797-2:2021, NIST SP 800-185]
KMAC256	256 bits	[selection: ISO/IEC 9797-2:2021, NIST SP 800-185]
KMACXOF128	[assignment: integer 256 ⇐ Lk < 22040]	[selection: ISO/IEC 9797-2:2021, NIST SP 800-185]
KMACXOF256	[assignment: integer 256 ⇐ Lk < 22040]	[selection: ISO/IEC 9797-2:2021, NIST SP 800-185]

Application Note: If KMACXOF128 or KMACXOF256 is selected, FCS_COP.1/XOF is included. The key-size choices shall be consistent with the selected ISO or FIPS standard.

A.4.5. FCS_COP.1/SigVer Cryptographic Operation - Signature Verification

Source and modification: CCDB-018 Section 4.8. All Catalogue rows are retained. In this PP-Module the component is included when the TOE verifies signatures for an in-scope DBMS function such as autonomous or provider-managed update verification. Protocol-specific signature verification remains governed by the applicable Functional Package.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.5, or no other component]; [FCS_COP.1/Hash or FCS_COP.1/XOF].

FCS_COP.1.1/SigVer The TSF shall perform [digital signature verification] in accordance with a specified cryptographic algorithm [selection: cryptographic algorithm] and cryptographic algorithm parameters [selection: cryptographic algorithm parameters] that meet the following: [selection: list of standards].

Table 9. Allowed completions of FCS_COP.1/SigVer

Identifier	Cryptographic Algorithm	Algorithm Parameters	List of Standards
RSA-PKCS	RSASSA-PKCS1-v1_5	Modulus [selection: 2048, 3072, 4096] bits; [selection: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512]	RFC 8017 and FIPS PUB 186-5
RSA-PSS	RSASSA-PSS	Modulus [selection: 2048, 3072, 4096] bits; [selection: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256]	RFC 8017 and FIPS PUB 186-5
DSA	DSA	Domain parameters (L,N) = [selection: (2048,224), (2048,256), (3072,256)]	FIPS PUB 186-4, signature verification only
ECDSA	ECDSA	Curve [selection: P-256, brainpoolP256r1, P-384, brainpoolP384r1, P-521, brainpoolP512r1] with selected SHA/SHA3/SHAKE hash	[selection: ISO/IEC 14888-3:2018, FIPS PUB 186-5] and selected curve standard
KCDSA	KCDSA	[selection: SHA-224, SHA-256, SHA-384, SHA-512]	ISO/IEC 14888-3:2018
EC-KCDSA	EC-KCDSA	Curve [selection: P-224, P-256, B-233, B-283, K-233, K-283] with selected SHA-2 hash	ISO/IEC 14888-3:2018 and NIST SP 800-186
EdDSA	Edwards-Curve Digital Signature Algorithm	[selection: Edwards25519, Edwards448]	FIPS PUB 186-5 and RFC 8032
LMS	Leighton-Micali Signature	Private key size and SHA-256/SHAKE256 parameters, Winternitz parameter, and tree height selected as specified by the Catalogue	RFC 8554 and NIST SP 800-208
HSS	Hierarchical Signature System using LMS	LMS parameter set and number of levels selected as specified by the Catalogue	RFC 8554 and NIST SP 800-208
XMSS	eXtended Merkle Signature Scheme	Private key size, SHA-256/SHAKE256 parameters, and tree height selected as specified by the Catalogue	RFC 8391 and NIST SP 800-208

Identifier	Cryptographic Algorithm	Algorithm Parameters	List of Standards
XMSSMT	Multi-tree XMSS	XMSS parameter set, total tree height, and number of levels selected as specified by the Catalogue	RFC 8391 and NIST SP 800-208

Application Note: When a public verification key is integrity protected within the TOE, the ST may select no key-import, generation, or derivation dependency. The selected hash or XOF component remains included. DSA is retained only for verification of legacy signatures as permitted by the Catalogue.

A.4.6. FCS_COP.1/KeyWrap Cryptographic Operation - Key Wrapping

Source and modification: CCDB-018 Section 4.9. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.5, FCS_CKM_EXT.7, or FCS_CKM_EXT.8]; FCS_CKM.6; FCS_COP.1/SKC.

FCS_COP.1.1/KeyWrap The TSF shall perform [key wrapping] in accordance with a specified cryptographic algorithm [selection: cryptographic algorithm] and cryptographic key sizes [selection: cryptographic key sizes] that meet the following: [selection: list of standards].

Table 10. Allowed completions of FCS_COP.1/KeyWrap

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
KW	[selection: AES, Camellia, SEED, LEA] in KW mode	[selection: 128; AES/Camellia/LEA 192; AES/Camellia/LEA 256] bits	[selection: ISO/IEC 19772:2020, Clause 6; NIST SP 800-38F, Section 6.2]
KWP	[selection: AES, Camellia, SEED, LEA] in KWP mode	[selection: 128; AES/Camellia/LEA 192; AES/Camellia/LEA 256] bits	NIST SP 800-38F, Section 6.3
CCM	[selection: AES, Camellia, LEA, SEED] in CCM mode with a non-repeating nonce of at least 64 bits	[selection: 128; AES/Camellia/LEA 192; AES/Camellia/LEA 256] bits	[selection: ISO/IEC 19772:2020, Clause 7; NIST SP 800-38C]

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
GCM	[selection: AES, Camellia, LEA, SEED] in GCM mode with a 96-bit non-repeating IV using deterministic construction and a tag length of [selection: 96, 104, 112, 120, 128] bits	[selection: 128; AES/Camellia/LEA 192; AES/Camellia/LEA 256] bits	[selection: ISO/IEC 19772:2020, Clause 10; NIST SP 800-38D]

Application Note: The key used to protect transported keying material should provide at least the security strength of the protected key. SEED supports 128-bit keys only.

A.4.7. FCS_COP.1/SKC Cryptographic Operation - Symmetric-Key Cryptography

Source and modification: CCDB-018 Section 4.10. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.5, FCS_CKM_EXT.7, or FCS_CKM_EXT.8]; FCS_CKM.6; FCS_OTV_EXT.1.

FCS_COP.1.1/SKC The TSF shall perform [symmetric-key encryption/decryption] in accordance with a specified cryptographic algorithm [selection: cryptographic algorithm] and cryptographic key sizes [selection: cryptographic key sizes] that meet the following: [selection: list of standards].

Table 11. Allowed completions of FCS_COP.1/SKC

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
AES-CBC	AES in CBC mode with non-repeating and unpredictable IVs	[selection: 128, 192, 256] bits	[selection: ISO/IEC 18033-3:2010, FIPS PUB 197] and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
XTS-AES	AES in XTS mode with unique consecutive non-negative integer tweak values	[selection: 256, 512] bits	[selection: ISO/IEC 18033-3:2010, FIPS PUB 197] and [selection: IEEE Std. 1619-2018, NIST SP 800-38E]
AES-CTR	AES in CTR mode with a non-repeating initial counter and no repeated counter values under the same key	[selection: 128, 192, 256] bits	[selection: ISO/IEC 18033-3:2010, FIPS PUB 197] and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
CAM-CBC	Camellia in CBC mode with non-repeating and unpredictable IVs	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
CAM-CFB	Camellia in CFB mode with non-repeating and unpredictable IVs	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
CAM-OFB	Camellia in OFB mode with unique IVs	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
XTS-CAM	Camellia in XTS mode with unique consecutive non-negative integer tweak values	[selection: 256, 512] bits	ISO/IEC 18033-3:2010 and [selection: IEEE Std. 1619-2018, NIST SP 800-38E]
CAM-CTR	Camellia in CTR mode with a non-repeating initial counter and no repeated counter values under the same key	[selection: 128, 192, 256] bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
SEED-CBC	SEED in CBC mode with non-repeating and unpredictable IVs	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
SEED-CFB	SEED in CFB mode with non-repeating and unpredictable IVs	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
SEED-OFB	SEED in OFB mode with unique IVs	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
SEED-CTR	SEED in CTR mode with a unique incremental counter	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
HIGHT-CBC	HIGHT in CBC mode with non-repeating and unpredictable IVs	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
HIGHT-CFB	HIGHT in CFB mode with non-repeating and unpredictable IVs	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
HIGHT-OFB	HIGHT in OFB mode with unique IVs	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
HIGHT-CTR	HIGHT in CTR mode with a unique incremental counter	128 bits	ISO/IEC 18033-3:2010 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
LEA-CBC	LEA in CBC mode with non-repeating and unpredictable IVs	[selection: 128, 192, 256] bits	ISO/IEC 29192-2:2019 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]

Identifier	Cryptographic Algorithm	Key Sizes	List of Standards
LEA-CFB	LEA in CFB mode with non-repeating and unpredictable IVs	[selection: 128, 192, 256] bits	ISO/IEC 29192-2:2019 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
LEA-OFB	LEA in OFB mode with unique IVs	[selection: 128, 192, 256] bits	ISO/IEC 29192-2:2019 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]
LEA-CTR	LEA in CTR mode with a unique incremental counter	[selection: 128, 192, 256] bits	ISO/IEC 29192-2:2019 and [selection: ISO/IEC 10116:2017, NIST SP 800-38A]

Application Note: If the selected cryptographic algorithm requires an IV, counter, or tweak value, FCS_OTV_EXT.1 is included.

A.4.8. FCS_COP.1/XOF Extendable-Output Function

Source and modification: CCDB-018 Section 4.11. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, or FCS_CKM.5].

FCS_COP.1.1/XOF The TSF shall perform [extendable-output function] in accordance with a specified cryptographic algorithm [selection: cryptographic algorithm] and parameters [selection: parameters] that meet the following: [selection: list of standards].

Table 12. Allowed completions of FCS_COP.1/XOF

Algorithm	Parameters	List of Standards
cSHAKE	Output length d = [selection: 128, 256] bits and [selection: SHAKEd, KECCAK[2d]]	NIST SP 800-185 and FIPS PUB 202
KMACXOF	Output length d = [selection: 128, 256] bits	NIST SP 800-185
SHAKE	Output length d = [selection: 128, 256] bits	FIPS PUB 202

A.5. Catalogue-Derived One-Time Value and Random Bit Generation Components

A.5.1. FCS_OTV_EXT.1 One-Time Value

Source and modification: CCDB-018 Section 5.2. All Catalogue rows are retained.

Hierarchical to: No other components.

Dependencies: FCS_RBG.1; [FCS_COP.1/KeyedHash, FCS_COP.1/SKC, FCS_CKM.5, FCS_CKM_EXT.8, FCS_COP.1/CMAC, FCS_COP.1/KeyWrap, FCS_COP.1/AEAD, or FCS_COP.1/KeyEncap].

FCS_OTV_EXT.1.1 The TSF shall perform cryptographic one-time value generation for [selection: algorithm or mode] using the output of a [selection: random bit generator as defined in FCS_RBG.1, deterministic OTV construction, [assignment: OTV construction method]] and sizes of length that meet the following: [selection: list of standards].

Table 13. Allowed completions of FCS_OTV_EXT.1

Algorithm or Mode	List of Standards	Catalogue Guidance Retained for the ST Author
HMAC	FIPS PUB 198-1; NIST SP 800-56C Revision 2	Salts may be secret or known, randomly generated or zero, as permitted by the selected use and standard.
KMAC	NIST SP 800-185; NIST SP 800-56C Revision 2	Salts and secret IVs are selected as required by the use and standard.
KDF	NIST SP 800-108 Revision 1; NIST SP 800-135 Revision 1; ISO/IEC 11770-6:2016	Salts and IVs are generated as directed for the selected primitive.
PBKDF	NIST SP 800-132	Salts are generated and used as directed by the PBKDF standard.
CTR	NIST SP 800-38A	The initial counter shall not repeat, and counter values shall not repeat under the same secret key.
CBC	NIST SP 800-38A, Appendix C	IVs shall be unpredictable where required and shall not repeat where reuse would disclose common plaintext prefixes.
OFB	NIST SP 800-38A	IVs shall not repeat and shall not be generated by invoking the cipher on another IV.
CFB	NIST SP 800-38A	IVs should not repeat.
XTS	NIST SP 800-38E; IEEE Std. 1619-2018	Tweak values shall be consecutive non-negative integers beginning at an arbitrary non-negative integer.
CMAC	NIST SP 800-38B	The IV is all zeroes.
KW, KWP	NIST SP 800-38F	Use any nonce required by the selected construction and use case.
CCM	NIST SP 800-38C	Nonces shall not repeat.
GCM	NIST SP 800-38D	For RBG-based IV construction, invocations shall remain within the limits of Section 8.3 for a given secret key.
RSA-OAEP	NIST SP 800-56B Revision 2	The padding mask shall be randomly generated.

A.5.2. FCS_RBG.1 Random Bit Generation

Source and modification: CCDB-018 Section 6.2. All Catalogue rows are retained. The `never` reseeding choice remains available in the general-purpose use case but is not permitted by the Enterprise Enhanced template.

Hierarchical to: No other components.

Dependencies: [`FCS_RBG.2` or `FCS_RBG.3`]; `FCS_COP.1/Hash`; `FCS_COP.1/SKC`; `FPT_FLS.1/RBG`; `FPT_TST.1/RBG`.

DBMS-iTC Application Note: The dependency list above reproduces the Catalogue text. The DBMS-iTC interprets it as follows, without modifying the underlying components: the seeding dependency is satisfied by `FCS_RBG.2`, `FCS_RBG.3`, or `FCS_RBG.4` according to the TOE's seeding architecture (the Catalogue's disjunction predates the internal-seeding-multiple-sources component, which equally satisfies the dependency's purpose); and the primitive dependency applies per the selected DRBG type — `FCS_COP.1/Hash` for Hash_DRBG and HMAC_DRBG, `FCS_COP.1/SKC` for CTR_DRBG.

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [selection: DRBG algorithm] in accordance with [selection: list of standards] after initialization.

Table 14. Allowed completions of FCS_RBG.1.1

Identifier	RBG Algorithm	List of Standards
HASH_DRBG	Hash_DRBG with [selection: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512]	[selection: ISO/IEC 18031:2011, NIST SP 800-90A Revision 1]
HMAC_DRBG	HMAC_DRBG with [selection: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512]	[selection: ISO/IEC 18031:2011, NIST SP 800-90A Revision 1]
CTR_DRBG	CTR_DRBG with [selection: AES-128, AES-192, AES-256, Camellia-128, Camellia-192, Camellia-256, SEED-128, HIGHT-128, LEA-128, LEA-192, LEA-256]	[selection: ISO/IEC 18031:2011, NIST SP 800-90A Revision 1]

FCS_RBG.1.2 The TSF shall use a [selection: TSF entropy source [assignment: name of entropy source], TSF interface for obtaining entropy] for initialization and reseeding.

FCS_RBG.1.3 The TSF shall update the DRBG state by [selection: reseeding, uninstantiating and re-instantiating] using a [selection: TSF entropy source [assignment: name of entropy source], TSF interface for obtaining entropy [assignment: name of interface]] in the following situations: [selection: never, on demand, on the condition [assignment: condition], after [assignment: time]] in accordance with [assignment: list of standards].

Application Note: If reseeding is selected but is not feasible when required, the TSF uninstantiates the DRBG rather than producing output of insufficient quality. The ST identifies the applicable reseed interval, uninstantiation procedure, and any exposed reseed interface.

A.5.3. FCS_RBG.2 Random Bit Generation - External Seeding

Source and modification: CCDB-018 Section 6.3. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: FCS_RBG.1.

FCS_RBG.2.1 The TSF shall be able to accept a minimum input of [assignment: minimum input length greater than zero] from a TSF interface for the purpose of obtaining entropy.

Application Note: The input shall be sufficient to satisfy the entropy requirements of the selected DRBG. The ST describes protection of the integrity and confidentiality of entropy received from an external source.

A.5.4. FCS_RBG.3 Random Bit Generation - Internal Seeding, Single Source

Source and modification: CCDB-018 Section 6.4. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: FCS_RBG.1; FCS_RBG.5.

FCS_RBG.3.1 The TSF shall be able to seed the DRBG using a [selection: TSF software-based entropy source, TSF hardware-based entropy source] [assignment: name of entropy source] with [assignment: number of bits] bits of min-entropy.

A.5.5. FCS_RBG.4 Random Bit Generation - Internal Seeding, Multiple Sources

Source and modification: CCDB-018 Section 6.5. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: FCS_RBG.1; FCS_RBG.5.

FCS_RBG.4.1 The TSF shall be able to seed the DRBG using [selection: [assignment: number] TSF software-based entropy source(s), [assignment: number] TSF hardware-based entropy source(s)].

A.5.6. FCS_RBG.5 Random Bit Generation - Combining Entropy Sources

Source and modification: CCDB-018 Section 6.6. Copied without substantive modification.

Hierarchical to: No other components.

Dependencies: FCS_RBG.1; [FCS_RBG.2, FCS_RBG.3, or FCS_RBG.4].

FCS_RBG.5.1 The TSF shall [selection: hash, concatenate and hash, XOR, input into a linear feedback shift register, [assignment: combining operation]] [selection: output from TSF entropy source(s), input from TSF interface(s) for obtaining entropy] resulting in a minimum of [assignment: number of bits] bits of min-entropy to create the entropy input into the derivation

function as defined in [selection: ISO/IEC 18031:2011, NIST SP 800-90A Revision 1].

A.6. CC Part 2 Components Required by Catalogue Dependencies

The following iterations are copied from CC:2022 Part 2 and completed only for the FCS_RBG.1 dependency. They are not DBMS-iTC-originated cryptographic requirements.

A.6.1. FPT_FLS.1/RBG Failure with Preservation of Secure State

FPT_FLS.1.1/RBG The TSF shall preserve a secure state when the following types of failures occur: [DRBG self-test failure].

A.6.2. FPT_TST.1/RBG TSF Self-Testing

FPT_TST.1.1/RBG The TSF shall run a suite of self-tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, under [assignment: conditions under which self-test shall occur]] to demonstrate the correct operation of [the DRBG and its supporting cryptographic primitives].

FPT_TST.1.2/RBG The TSF shall provide authorized users the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data].

FPT_TST.1.3/RBG The TSF shall provide authorized users the capability to verify the integrity of [selection: [assignment: parts of the TSF], the TSF].

Application Note: The evaluation treatment of these two iterations is defined in the Supporting Document [[SD]]. Their evaluation methods are expected from the Catalogue Evaluation Methods; until a scheme-recognized version is available, Certification Body-approved CMVP (FIPS 140-3) module-validation evidence may cover self-test execution and failure behavior, with the TOE-integration residue evaluated per the SD's transitional coverage.

A.7. Enterprise Enhanced Use Case Selection Template

An ST claiming [USE CASE 2] Enterprise Enhanced shall satisfy every applicable row below. The template constrains operations in components already consumed from CCDB-018 and, for FCS_CKM_EXT.1.2, the DEK protection selection of this module; it does not add or replace a Catalogue component. A TOE that does not satisfy this template may still conform under [USE CASE 1] General-Purpose Cryptographic Deployment.

Table 15. Enterprise Enhanced cryptographic selection template

Component	Required Enterprise Enhanced Completion	Alignment Basis
FCS_CKM.1/SKG	Select RSK direct generation under NIST SP 800-133 Revision 2. Select 256-bit keys, or 512 bits only when the value comprises two AES-256 keys for XTS.	NIAP symmetric-key generation convention; AES-256 strength required by CNSA 2.0.

Component	Required Enterprise Enhanced Completion	Alignment Basis
FCS_CKM.5	Select a NIST SP 800-108 or NIST SP 800-56C derivation row with a FIPS-approved primitive at CNSA 2.0 strength: for the KDF-CTR, KDF-FB, KDF-DPI, and KDF-MAC-2S rows, select AES-256-CMAC or HMAC-SHA-512 as the PRF (HMAC-SHA-384 is not an available PRF selection in those Catalogue rows); for the KDF-HASH and KDF-MAC-1S rows, use the SHA-384 or SHA-512 primitives claimed through the constrained FCS_COP.1/Hash or FCS_COP.1/KeyedHash rows. Select a 256- or 512-bit output as required by the consuming operation. Do not select KDF-XOR or KDF-ENC.	NIST-approved derivation methods and primitives suitable for a FIPS Approved mode; CNSA 2.0 symmetric/hash strength.
FCS_CKM_EXT.8	Select HMAC-SHA-384 or HMAC-SHA-512, a randomly generated salt of at least 128 bits, an implementation-appropriate iteration count justified in the TSS, and a 256- or 512-bit output.	NIST SP 800-132 and the Catalogue component; NIAP password-conditioning convention.
FCS_CKM.6	List every in-scope MEK, DEK, intermediate key, and secret derivation value. Select destruction methods consistent with the cryptographic module security policy and ensure the TSF enters or preserves a secure state when destruction fails.	FIPS 140-3 sensitive security parameter management and NIAP key-destruction treatment.
FCS_CKM_EXT.1.2	Select key wrapping claimed as FCS_COP.1/KeyWrap or authenticated encryption claimed as FCS_COP.1/AEAD for the protection of stored DEKs. The symmetric key encryption option (FCS_COP.1/SKC) is not permitted under this use case.	NIST SP 800-38F key wrapping and NIST SP 800-57 confidentiality-and-integrity protection of stored keys; CNSA 2.0 AES-256 strength via the constrained KeyWrap and AEAD rows.
FCS_COP.1/AEAD	Select AES-GCM or AES-CCM with a 256-bit key. For GCM, select a 128-bit tag and an IV construction permitted by NIST SP 800-38D.	NIAP AES mode selections and key size; CNSA 2.0 AES-256.
FCS_COP.1/CMAC	When required, select AES-CMAC with a 256-bit key and NIST SP 800-38B.	FIPS-approved primitive and CNSA 2.0 AES-256 strength.

Component	Required Enterprise Enhanced Completion	Alignment Basis
FCS_COP.1/Hash	Select SHA-384 and/or SHA-512 under FIPS PUB 180-4. Select other hashes only when an applicable Functional Package expressly requires them for a separate protocol function; those selections do not satisfy this use-case row.	CNSA 2.0 SHA-384/SHA-512 and NIAP hash convention.
FCS_COP.1/KeyedHash	When required, select HMAC-SHA-384 and/or HMAC-SHA-512 under FIPS PUB 198-1 with a key size consistent with the selected security strength.	NIAP HMAC convention and CNSA 2.0 hash strength.
FCS_COP.1/SigVer	When the TOE verifies signatures on DBMS software or firmware updates, select LMS, HSS, XMSS, and/or XMSSMT with parameters permitted by NIST SP 800-208 and the applicable CNSA 2.0 transition policy. Do not use a legacy DSA, RSA, ECDSA, KCDSA, or EdDSA row to satisfy this use-case entry.	CNSA 2.0 software/firmware signature verification choices available in CCDB-018 Version 1.0 and current NIAP transition treatment.
FCS_COP.1/KeyWrap	Select AES in KW, KWP, CCM, or GCM mode with a 256-bit key. When GCM is selected, use a 128-bit tag and the deterministic 96-bit IV construction required by the Catalogue row.	FIPS-approved AES key-protection modes and CNSA 2.0 AES-256.

Table 16. Enterprise Enhanced cryptographic selection template (continued)

Component	Required Enterprise Enhanced Completion	Alignment Basis
FCS_COP.1/SKC	Select AES-CBC or AES-CTR with a 256-bit key, or XTS-AES with a 512-bit combined key comprising two AES-256 keys. Other Catalogue algorithms remain available only under the general-purpose use case.	Current NIAP application PP AES mode set and CNSA 2.0 AES-256.
FCS_OTV_EXT.1	Select the NIST construction and standard associated with every selected AES, HMAC, KDF, PBKDF, or key-wrap operation. IVs, nonces, counters, tweaks, and salts shall meet the non-repetition, unpredictability, and size rules of the selected standard.	Catalogue and NIAP one-time-value treatment for FIPS-approved operations.
FCS_RBG.1	Select Hash_DRBG or HMAC_DRBG with SHA-384 or SHA-512, or CTR_DRBG with AES-256, under NIST SP 800-90A Revision 1. The never state-update choice is not permitted.	Current NIAP DRBG families; FIPS-approved primitives; CNSA 2.0 symmetric/hash strength.
FCS_RBG.2 through FCS_RBG.5	Include the component or components matching the selected entropy path. Provide at least 256 bits of min-entropy or external input sufficient to instantiate the selected DRBG at 256-bit security strength.	NIST SP 800-90 series and FIPS 140-3 entropy/DRBG expectations.
FPT_FLS.1/RBG and FPT_TST.1/RBG	Include both components whenever FCS_RBG.1 is included. Select self-tests and failure behavior that prevent cryptographic service after a DRBG self-test failure.	CCDB-018 dependencies and current NIAP DRBG self-test convention.

Application Note: FIPS 140-3 specifies requirements for cryptographic modules rather than a standalone algorithm-selection list. This template restricts Catalogue operations to functions suitable for the stated alignment target, but the ST shall make any cryptographic-module validation claim separately and shall identify the validated module, certificate, boundary, approved mode, and version when such a claim is made. CNSA 2.0 public-key, digital-signature, key-establishment, and post-quantum selections are outside the DBMS data-protection scope of this module and are addressed by applicable Functional Packages or other Requirements Documents.

Evaluation Note: The evaluator verifies triggered Catalogue components, completed operations, and any Enterprise Enhanced claim. Use [[Crypto_Eval_Methods]] when recognized. Until then, the Crypto SD allows Certification Body-recognized CAVP, CMVP, or equivalent evidence for covered algorithm correctness, requires an approved method for gaps, and retains all DBMS integration activities.

Appendix B: Optional Requirements

There are no Optional Requirements for this PP-Module.

Appendix C: Extended Component Definitions

This appendix contains the formal definitions for the extended requirements used in this PP-Module, in accordance with the conventions of CC:2022 Part 2 [[CC2]].

(Note: formatting conventions for selections and assignments in this appendix follow those in CC:2022 Part 2 [[CC2]].)

C.1. FCS: Cryptographic Support

C.1.1. FCS_CKM_EXT: Cryptographic Key Management

C.1.1.1. Family Behaviour

Cryptographic keys must be managed throughout their lifecycle. This family defines requirements for key generation, distribution, access, derivation, agreement, password-based derivation, and destruction. The DBMS-iTC adds `FCS_CKM_EXT.1` to address the DBMS-specific lifecycle of Master/Root Cryptographic Keys (MEKs) used to protect Data Encryption Keys (DEKs). `FCS_CKM_EXT.8` and its ECD material are consumed from CCDB-018 Annex A and are not originated by the DBMS-iTC.

C.1.1.2. Component levelling

- `FCS_CKM_EXT.1` Cryptographic Key Management (Master Keys), originated by the DBMS-iTC, requires the TSF to manage the full lifecycle of the MEK, including generation or import, protection, and destruction.
- `FCS_CKM_EXT.8` Password-Based Key Derivation, consumed from CCDB-018, requires keys to be derived from low-entropy password input using specified cryptographic primitives.

C.1.1.3. Management: FCS_CKM_EXT.8

There are no management activities foreseen by the Catalogue ECD.

C.1.1.4. Audit: FCS_CKM_EXT.8

The following actions should be auditable if FAU_GEN Security audit data generation is included: success and failure of the activity at the minimal level, and object attributes and values excluding sensitive information at the basic level.

C.1.1.5. FCS_CKM_EXT.8 Password-Based Key Derivation

Source: CCDB-018 Annex A.2.3. This ECD component is copied without substantive modification.

Hierarchical to: No other components.

Dependencies: [`FCS_CKM.2`, `FCS_COP.1`, or `FCS_CKM_EXT.7`]; `FCS_CKM.6`; `FCS_OTV_EXT.1`.

FCS_CKM_EXT.8.1 The TSF shall perform password-based key derivation functions in accordance

with a specified cryptographic algorithm [HMAC-[selection: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512]], with iteration count of [assignment: number of iterations] using a randomly generated salt of length [assignment: equal to or greater than 128] bits and output cryptographic key sizes [selection: 128, 192, 256, 512] bits that meet the following standard: [NIST SP 800-132, Section 5.3, PBKDF2].

C.1.1.6. Management: FCS_CKM_EXT.1

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

a) Selection of Master Key origin (internal generation vs. external import). b) Initiation of Master Key rotation. c) Initiation of Master Key destruction. d) Configuration of secure key storage settings.

C.1.1.7. Audit: FCS_CKM_EXT.1

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

a) Basic: Generation of a Master Key. b) Basic: Import of a Master Key from an external entity. c) Basic: Destruction of a Master Key. d) Detailed: Key rotation operations.

C.1.1.8. FCS_CKM_EXT.1 Cryptographic Key Management (Master Keys)

Hierarchical to: No other components.

Dependencies: `FCS_CKM.6` Timing and Event of Cryptographic Key Destruction (CCDB-018 Section 3.7); `FCS_CKM.1/SKG` and `FCS_RBG.1` when MEKs are generated internally; `FCS_COP.1/KeyWrap`, `FCS_COP.1/SKC`, or `FCS_COP.1/AEAD` for DEK protection as selected; `FCS_OTV_EXT.1` when required by the selected operation; `FDP_ITC_EXT.1` Trusted Channel for Key Import and External Key Management (this module, conditional when an external Key Origin is selected).

FCS_CKM_EXT.1.1 The TSF shall manage the lifecycle of the Master/Root Cryptographic Keys (MEKs) as follows:

- **Key Origin**: [selection: Generated Internally - The TSF shall generate the Master Key using the consumed `FCS_CKM.1/SKG` and `FCS_RBG.1` components and store it securely within the TOE boundary; Imported from External Entity - The TSF shall import the Master Key from an external IT entity via the trusted channel defined in FDP_ITC_EXT.1, after which the TSF is the authoritative holder of the Master Key; Externally Managed - The TSF shall obtain use of the Master Key from an external key management service via the trusted channel defined in FDP_ITC_EXT.1, by retrieving the Master Key for transient use or by invoking Master Key operations by reference; the external service remains the authoritative store, and the TSF shall not persistently store plaintext Master Key material within the TOE boundary.]

FCS_CKM_EXT.1.2 The TSF shall protect the Master Key against disclosure and modification and shall protect stored DEKs under the Master Key using [selection: key wrapping claimed as `FCS_COP.1/KeyWrap`, symmetric key encryption claimed as `FCS_COP.1/SKC`, authenticated encryption claimed as `FCS_COP.1/AEAD`].

FCS_CKM_EXT.1.3 The TSF shall destroy Master Keys in accordance with the key destruction

requirements specified in the Crypto Catalogue (FCS_CKM.6).

C.1.2. FCS_OTV_EXT: One-Time Value Generation

C.1.2.1. Family Behaviour

Cryptographic operations often require one-time values such as nonces, IVs, salts, and initial counters. These values are often non-secret.

C.1.2.2. Component levelling

FCS_OTV_EXT.1 One-Time Value Generation requires that one-time values be generated using the selected random or deterministic construction. This family and component are consumed from CCDB-018 Annex A and are not originated by the DBMS-iTC.

C.1.2.3. Management: FCS_OTV_EXT.1

There are no management activities foreseen by the Catalogue ECD.

C.1.2.4. Audit: FCS_OTV_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included: success and failure of the activity at the minimal level, and object attributes and values excluding sensitive information at the basic level.

C.1.2.5. FCS_OTV_EXT.1 One-Time Value Generation

Source: CCDB-018 Annex A.3.1. This ECD component is copied without substantive modification.

Hierarchical to: No other components.

Dependencies: FCS_RBG.1; [FCS_COP.1/KeyedHash, FCS_COP.1/SKC, FCS_CKM.5, FCS_CKM_EXT.8, FCS_COP.1/CMAC, FCS_COP.1/KeyWrap, FCS_COP.1/AEAD, or FCS_COP.1/KeyEncap].

FCS_OTV_EXT.1.1 The TSF shall perform cryptographic one-time value generation for [selection: algorithm or mode] using the output of a [selection: random bit generator as defined in FCS_RBG.1, deterministic OTV construction, [assignment: OTV construction method]] and sizes of length that meet the following: [selection: list of standards].

C.2. FDP: User Data Protection

C.2.1. FDP_DAR_EXT: Data-at-Rest Encryption Strategy

C.2.1.1. Family Behaviour

This family defines requirements for the TSF to enforce a data-at-rest encryption strategy for persistent database storage. This family is distinct from generic storage protection requirements in that it explicitly addresses the scope of encryption (Storage-Scope vs. Granular), documented exclusions, and the relationship to the key hierarchy managed by FCS_CKM_EXT.1. This allows the ST author to precisely characterize how broadly encryption is applied within the DBMS, which is a

key differentiator between different DBMS product architectures (e.g., Transparent Data Encryption vs. column-level encryption).

C.2.1.2. Component levelling

FDP_DAR_EXT.1 Data-at-Rest Encryption Strategy requires the TSF to define and enforce the scope and method of encryption applied to persistent database data.

C.2.1.3. Management: FDP_DAR_EXT.1

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

a) Selection of encryption strategy (Storage-Scope vs. Granular). b) Configuration of which data elements are subject to Granular Encryption (when selected). c) Configuration of encryption algorithm settings and documented storage-object exclusions (in conjunction with Crypto Catalogue selections).

C.2.1.4. Audit: FDP_DAR_EXT.1

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

a) Basic: Enabling or disabling data-at-rest encryption. b) Basic: Changes to the encryption scope or strategy. c) Detailed: Encryption or decryption failures.

C.2.1.5. FDP_DAR_EXT.1 Data-at-Rest Encryption Strategy

Hierarchical to: No other components.

Dependencies: `FCS_COP.1/SKC` Cryptographic Operation - Symmetric-Key Cryptography (CCDB-018 Section 4.10); `FCS_COP.1/AEAD` Cryptographic Operation - Authenticated Encryption with Associated Data (CCDB-018 Section 4.2, when an authenticated encryption mode is used); `FCS_OTV_EXT.1` One-Time Values (when required by the selected mode); `FCS_CKM_EXT.1` Cryptographic Key Management (Master Keys) (this module).

FDP_DAR_EXT.1.1 The TSF shall enforce a Data-at-Rest Encryption strategy as follows:

- [selection: Storage-Scope Encryption - The TSF shall encrypt the persistent database storage objects identified in the ST and TSS using algorithms selected in the consumed Catalogue components, with only documented exclusions that do not contain plaintext user data or that are protected by an equivalent specified mechanism; Granular Data Encryption - The TSF shall encrypt specific data elements (e.g., columns, cells) using algorithms selected in the consumed Catalogue components.]

FDP_DAR_EXT.1.2 The TSF shall perform the encryption specified in FDP_DAR_EXT.1.1 using the cryptographic operations claimed in the included [selection: FCS_COP.1/SKC, FCS_COP.1/AEAD] components.

C.2.2. FDP_ITC_EXT: Trusted Channel for Key Import and External Key Management

C.2.2.1. Family Behaviour

This family defines requirements for the TSF to establish a mutually authenticated TLS trusted channel to an external key management entity, for the purpose of securely importing cryptographic key material or communicating with an external key management service that remains the authoritative store for the Master Key (e.g., a KMIP-conformant key manager). It complements FCS_CKM_EXT.1 by defining the communication channel properties required when the "Imported from External Entity" or "Externally Managed" selection is made. It is distinct from the general trusted channel families (FTP_ITC, FTP_TRP) in that it is scoped to key management operations and explicitly defines mutual authentication requirements in that context.

C.2.2.2. Component levelling

FDP_ITC_EXT.1 Trusted Channel for Key Import and External Key Management requires the TSF to establish a trusted channel that provides confidentiality, integrity, and authentication for key import and external key-management operations.

C.2.2.3. Management: FDP_ITC_EXT.1

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

a) Configuration of trusted external key management entity endpoints. b) Management of certificates or credentials used for channel authentication. c) Management of the TOE certificate or credentials used for mutual TLS authentication.

C.2.2.4. Audit: FDP_ITC_EXT.1

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

a) Basic: Establishment of a trusted channel to an external key management entity. b) Basic: Successful or failed key import operations. c) Basic: Authentication failures on the trusted channel. d) Detailed: Certificate validation results during channel establishment.

C.2.2.5. FDP_ITC_EXT.1 Trusted Channel for Key Import and External Key Management

Hierarchical to: No other components.

Dependencies: `FCS_TLSC_EXT.1` and/or `FCS_TLSS_EXT.1` from the Functional Package for TLS v2.1 [[TLS_FP]], as required by the TOE role. These components must be included in the ST and configured to support mutual TLS for the key import channel.

FDP_ITC_EXT.1.1 The TSF shall be capable of establishing a trusted channel between itself and an external key management entity for the purpose of importing cryptographic keys.

FDP_ITC_EXT.1.2 The TSF shall ensure the trusted channel provides:

- **Confidentiality**: Protection against disclosure.

- **Integrity**: Protection against modification.
- **Authentication**: Mutual Authentication - The TOE shall authenticate the external entity, and the external entity shall authenticate the TOE.

FDP_ITC_EXT.1.3 The trusted channel shall be implemented using mutual TLS claimed from the Functional Package for TLS v2.1 [[TLS_FP]].

C.2.3. FDP_DIT_EXT: Data-in-Transit Protection

C.2.3.1. Family Behaviour

This family defines requirements for the TSF to protect data transmitted between the TOE and external entities from unauthorized disclosure and modification. It complements the data-at-rest and key-management families by extending cryptographic protection to data in transit, and it is distinct from FDP_ITC_EXT in that it addresses general protected communications rather than the key-import channel specifically.

C.2.3.2. Component levelling

FDP_DIT_EXT.1 Data-in-Transit Protection requires the TSF to protect data transmitted between the TOE and external entities and to authenticate the channel endpoints.

C.2.3.3. Management: FDP_DIT_EXT.1

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

a) Configuration of data-in-transit protocol settings. b) Management of certificates and trust anchors used for channel authentication.

C.2.3.4. Audit: FDP_DIT_EXT.1

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

a) Basic: Establishment or failure of a protected channel. b) Basic: Enabling or disabling data-in-transit protection. c) Detailed: Certificate validation results during channel establishment.

C.2.3.5. FDP_DIT_EXT.1 Data-in-Transit Protection

Hierarchical to: No other components.

Dependencies: `FCS_TLSC_EXT.1` and/or `FCS_TLSS_EXT.1` from the Functional Package for TLS v2.1 [[TLS_FP]] when TLS is selected; `FIA_X509_EXT` certificate-validation components from the Functional Package for X.509 Certificates [[X509_FP]] when certificate authentication is used; applicable protocol-specific components from another Functional Package when another protocol is selected.

FDP_DIT_EXT.1.1 The TSF shall protect data in transit between the TOE and external entities from unauthorized disclosure and modification using TLS as claimed from the Functional Package for TLS and [selection: no other cryptographic protocol, [assignment: other cryptographic protocol

claimed from an applicable Functional Package]].

FDP_DIT_EXT.1.2 The TSF shall authenticate the endpoints of the protected channel using X.509 certificates specified by the Functional Package for X.509 Certificates, where required by the selected protocol.

Appendix D: Consistency Rationale

This appendix demonstrates, per the ACE_MCO requirements of CC:2022, that this PP-Module is consistent with its Base PP, the collaborative Protection Profile for Database Management Systems (cPP_DBMS) Version 2.0, 27 April 2026 [[cPP_DBMS]]. The complete threat, objective, and SFR mappings for this module are stated once, in Security Rationale, and are not repeated here.

D.1. Consistency of TOE Type

The Base PP defines a Database Management System TOE. This PP-Module adds cryptographic functionality — key hierarchy and Master Key lifecycle management, data-at-rest encryption, and data-in-transit protection — to that same TOE type. It does not redefine what the TOE is, and all Base PP SFRs continue to apply to it.

D.2. Consistency of Security Problem Definition

The Base PP defines no cryptographic SFRs and leaves cryptographic protection concerns to the operational environment. This module's threats (T.KEY_COMPROMISE, T.KEY_IMPORT_INTERCEPTION, T.WEAK_CRYPTO_IMPLEMENTATION, T.DATA_IN_TRANSIT_DISCLOSURE) address exactly that cryptographic attack surface; none contradicts a Base PP threat. A.KEY_STORE_SECURITY adds an operational environment property — protection of key material stored outside the TOE execution boundary — that no Base PP assumption addresses, and neither removes nor weakens any Base PP assumption. The organizational security policies (P.CRYPTOGRAPHIC_STANDARDS, P.KEY_LIFECYCLE) are additive and have no Base PP counterpart with which to conflict.

D.3. Consistency of Security Objectives

The module's TOE objectives (O.KEY_HIERARCHY, O.MASTER_KEY_MANAGEMENT, O.TRUSTED_KEY_IMPORT, O.CATALOGUE_CONFORMANCE, O.PROTECTED_TRANSIT) are additive: each addresses a cryptographic threat or policy the Base PP does not cover, and none redefines, weakens, or replaces a Base PP objective. OE.KEY_STORE_PROTECTION assigns to the environment only the persistent protection of stored key material outside the TOE execution boundary — a responsibility the Base PP never assigned to the TOE; the TOE protects keys while in use within its boundary (FCS_CKM_EXT.1).

D.4. Consistency of Security Functional Requirements

The Base PP claims no FCS components, so the FCS components of this module — both module-defined and consumed from the Cryptographic Catalogue [[Crypto_Catalog]] — cannot conflict with any Base PP completion. The module's FDP components (FDP_DAR_EXT.1, FDP_DIT_EXT.1, FDP_ITC_EXT.1) are extended components with no Base PP counterpart; they do not modify the Base PP's access-control or residual-information FDP components. Where module SFRs depend on Base PP functionality (management and audit), the dependency is satisfied without altering any Base PP completion. Data-in-transit treatment is analyzed separately in Consistency with the Base PP Data-in-Transit Treatment.

D.5. Consistency Across PP-Configurations

This module's consistency argument is identical in every allowed PP-Configuration — claimed with the Base PP alone or together with the DBMS Cloud Module (and, on a later publication track, planned modules such as the DBMS DBaaS Module). Modules claimed alongside this module reference and scope its requirements; they do not modify them. No additional per-configuration consistency analysis therefore arises from this module.

D.6. Consistency with the Base PP Data-in-Transit Treatment

The Base PP (cPP_DBMS) does not define cryptographic SFRs. It addresses the protection of transmitted data through the operational-environment assumption A.CONNECT, which also discharges the FPT_ITT.1 dependency of FPT_TRC.1 for distributed TOEs. For any PP-Configuration that includes this PP-Module, FDP_DIT_EXT.1 is mandatory and provides TOE-enforced protection for data transmitted between the TOE and external entities, using TLS and X.509 components from the applicable Functional Packages.

FDP_DIT_EXT.1 supplements A.CONNECT; it does not replace it. The assumption is retained in full in the PP-Configuration and remains the basis for the aspects the TOE does not enforce — in particular the protection of transfers between separate parts of a distributed TOE, the leg of A.CONNECT that discharges the FPT_ITT.1 dependency of FPT_TRC.1. FDP_DIT_EXT.1 is scoped to channels between the TOE and external entities and does not address inter-TSF transfer. No Base PP assumption is removed or weakened. The module therefore strengthens, and does not contradict, the Base PP.

Appendix E: SFR List

This table is provided as a reference of all SFRs included in this PP-Module.

The Type column has the following definitions:

Mandatory

The requirement must be included in the ST.

Selection-Based

The requirement must be included in the ST when selections in other SFRs trigger its inclusion, or when the TOE implements the specified functionality.

Optional

The requirement may be included in the ST at the ST author's discretion.

Table 17. Security Functional Requirements

Requirement Class	Requirement Component	Type
Cryptographic Support (FCS)		

	Signature Verification	Selection-Based
	FCS_COP.1/KeyWrap Cryptographic Operation - Key Wrapping	Selection-Based
Requirement Class	**Requirement Component**	**Type**
	FCS_COP.1/SKC Symmetric-Key Cryptography	Selection-Based; at least one of this component or FCS_COP.1/AEAD shall be included, per the Exact Conformance statement and the FDP_DAR_EXT.1.2 selection
	FCS_COP.1/XOF Extendable-Output Function	Selection-Based
	FCS_OTV_EXT.1 One-Time Value	Selection-Based
	FCS_RBG.1 Random Bit Generation	Selection-Based
	FCS_RBG.2 Random Bit Generation - External Seeding	Selection-Based
	FCS_RBG.3 Random Bit Generation - Internal Seeding, Single Source	Selection-Based
	FCS_RBG.4 Random Bit Generation - Internal Seeding, Multiple Sources	Selection-Based
	FCS_RBG.5 Random Bit Generation - Combining Entropy Sources	Selection-Based
Protection of the TSF (FPT)	FPT_FLS.1/RBG Failure with Preservation of Secure State	Selection-Based
	FPT_TST.1/RBG TSF Self-Testing	Selection-Based
User Data Protection (FDP)	FDP_DAR_EXT.1 Data-at-Rest Encryption Strategy	Mandatory
	FDP_DIT_EXT.1 Data-in-Transit Protection	Mandatory
	FDP_ITC_EXT.1 Trusted Channel for Key Import and External Key Management	Selection-Based

Application Note on FDP_DIT_EXT.1: The Data-in-Transit Protection requirement (FDP_DIT_EXT.1) is mandatory and is defined in this module. It applies to every PP-Configuration that includes this module, including the standalone cPP_DBMS + DBMS Cryptographic Module configuration and the configuration that adds the DBMS Cloud Module. Modules claimed alongside this module reference, and do not redefine, FDP_DIT_EXT.1; they identify the deployment-specific channels (for example, cloud IAM, audit export, or tenant-facing connections) to which it applies. Planned modules on a later publication track, such as the DBMS DBaaS Module, are expected to follow the same pattern. The ST author includes the applicable TLS and X.509 components from the Functional Package for TLS v2.1 [[TLS_FP]] and the Functional Package for X.509 Certificates [[X509_FP]].

E.1. SFR Dependency Summary

Table 18. SFR Dependencies

SFR	Dependencies	Resolution
FCS_CKM.1/SKG	FCS_CKM.6; FCS_RBG.1 or FCS_RNG.1; and a key distribution, derivation, agreement, or cryptographic operation component	Resolved by the consumed FCS_CKM.6, FCS_RBG.1, and applicable FCS_COP.1 components. This component is not included for a derived-only DEK path.
FCS_CKM.5 / FCS_CKM_EXT.8	FCS_CKM.6; applicable FCS_COP.1 primitive; FCS_OTV_EXT.1 for password-based derivation	Resolved by the consumed key-destruction, primitive, and one-time-value components selected for the derivation path.
FCS_CKM.6	A component that creates, imports, accesses, derives, or agrees the keys being destroyed	Resolved by FCS_CKM_EXT.1, FCS_CKM.1/SKG, FCS_CKM.5, or FCS_CKM_EXT.8, as applicable. For imported or externally managed Master Keys, FCS_CKM_EXT.1 together with FDP_ITC_EXT.1 provides the key-sourcing function that the Catalogue's FDP_ITC.1 /FDP_ITC.2 alternatives would otherwise provide; this substitution is justified because those components are the DBMS-specific instantiations of the same dependency purpose.
FCS_COP.1/AEAD, FCS_COP.1/CMAC, FCS_COP.1/KeyedHash, FCS_COP.1/KeyWrap, FCS_COP.1/SKC	Applicable key generation, derivation, import, or agreement component; FCS_CKM.6; FCS_OTV_EXT.1 where specified	Resolved by the consumed components selected for the TOE's key origin, lifecycle, and operation.
FCS_COP.1/Hash / FCS_COP.1/XOF	No dependency for Hash; key source dependency for XOF	Hash has no dependency. XOF is included only with its applicable consumed key source component.
FCS_COP.1/SigVer	Optional key source dependency; FCS_COP.1/Hash or FCS_COP.1/XOF	A protected public verification key may satisfy the no-key-source choice. The consumed Hash or XOF component is included for the selected signature scheme.
FCS_OTV_EXT.1	FCS_RBG.1 and the cryptographic operation using the one-time value	Resolved by the consumed RBG and operation components selected in the ST.

SFR	Dependencies	Resolution
FCS_RBG.1	FCS_RBG.2, FCS_RBG.3, or FCS_RBG.4 per the seeding architecture (see the DBMS-iTC Application Note at FCS_RBG.1); FCS_COP.1/Hash or FCS_COP.1/SKC per the selected DRBG type; FPT_FLS.1/RBG; FPT_TST.1/RBG	Resolved by the consumed seeding and primitive components and the CC Part 2 RBG failure/self-test iterations included in this module.
FCS_RBG.2 through FCS_RBG.5	FCS_RBG.1 and the applicable source/combining component	Resolved according to the entropy path selected in FCS_RBG.1.2.
FCS_CKM_EXT.1	FCS_CKM.6 Timing and Event of Key Destruction FCS_CKM.1/SKG and FCS_RBG.1 (when MEKs are generated internally) selected FCS_COP.1/KeyWrap, FCS_COP.1/SKC, or FCS_COP.1/AEAD for DEK protection FCS_OTV_EXT.1 when required FDP_ITC_EXT.1 (when import selected)	Catalogue-derived components consumed in this module; FDP_ITC_EXT.1 is the DBMS-specific conditional component.
FDP_DAR_EXT.1	FCS_COP.1/SKC and/or FCS_COP.1/AEAD FCS_OTV_EXT.1 when required FCS_CKM_EXT.1	Catalogue-derived components consumed in this module; FCS_CKM_EXT.1 is the DBMS-specific mandatory component.
FDP_ITC_EXT.1	FCS_TLSC_EXT.1 and/or FCS_TLSS_EXT.1 mutual TLS components	Functional Package for TLS v2.1 [[TLS_FP]]
FDP_DIT_EXT.1	FCS_TLSC_EXT.1 and/or FCS_TLSS_EXT.1 TLS components (when TLS selected) FIA_X509_EXT certificate-validation components (when certificate authentication used) protocol-specific components (when another protocol selected)	Functional Package for TLS v2.1 [[TLS_FP]] and Functional Package for X.509 Certificates [[X509_FP]], as applicable

Appendix F: Global Dependency Resolution Summary

This section provides a comprehensive view of all SFR dependencies and their resolutions for this PP-Module.

F.1. Dependency Resolution by Type

Table 19. Dependencies Satisfied by Module SFRs

Dependent SFR	Required Dependency	Satisfying SFR
FCS_CKM_EXT.1 (when import selected)	FDP_ITC_EXT.1	FDP_ITC_EXT.1 (this module, selection-based when import is selected)
FDP_DAR_EXT.1	FCS_CKM_EXT.1	FCS_CKM_EXT.1 (this module)

Table 20. Dependencies Satisfied by Catalogue-Derived Components Included in This Module

Dependent SFR	Required Dependency	Satisfying Component
FCS_CKM.1/SKG	FCS_RBG.1	Consumed `FCS_RBG.1` and its selected seeding, primitive, failure, and self-test dependencies
FCS_CKM_EXT.1	FCS_CKM.6; FCS_CKM.1/SKG and FCS_RBG.1 when MEKs are generated internally; selected DEK protection operation	Consumed `FCS_CKM.6`; consumed `FCS_CKM.1/SKG` and `FCS_RBG.1` when MEKs are generated internally; selected consumed `FCS_COP.1/KeyWrap`, `FCS_COP.1/SKC`, or `FCS_COP.1/AEAD`
FDP_DAR_EXT.1	FCS_COP.1/SKC and/or FCS_COP.1/AEAD as applicable to the selected encryption mode; FCS_OTV_EXT.1 when required	Consumed `FCS_COP.1/SKC` and/or `FCS_COP.1/AEAD`; consumed `FCS_OTV_EXT.1` for required IVs, nonces, tweaks, or other one-time values
DEK derivation path (when DEKs are derived)	FCS_CKM.5 or FCS_CKM_EXT.8	Consumed CCDB-018 key derivation component selected according to the derivation input type

Table 21. Dependencies Satisfied by Functional Packages (Conditional)

Dependent SFR	Required Dependency	Resolution
FDP_ITC_EXT.1 (when import is selected)	FCS_TLSC_EXT.1, FCS_TLSS_EXT.1	Functional Package for TLS v2.1 [[TLS_FP]]

Dependent SFR	Required Dependency	Resolution
FDP_DIT_EXT.1 (mandatory)	FCS_TLSC_EXT.1 / FCS_TLSS_EXT.1 (when TLS selected); FIA_X509_EXT certificate-validation components (when certificate authentication used)	Functional Package for TLS v2.1 [[TLS_FP]] and Functional Package for X.509 Certificates [[X509_FP]], as applicable

F.2. Catalogue Consumption Rationale

This PP-Module deliberately does not originate SFRs for specific cryptographic algorithm implementations. It consumes and reproduces the applicable components from the Common Criteria Cryptographic Catalogue [[Crypto_Catalog]], then adds only the DBMS-specific applicability and integration requirements needed for the TOE type.

1. **Separation of Concerns:** The Catalogue is maintained through the Common Criteria cryptographic standards process. Retaining its component identifiers, operations, dependencies, ECDs, and evaluation methods prevents this PP-Module from presenting Catalogue material as DBMS-iTC-originated content.
2. **Flexibility:** The general-purpose use case retains the Catalogue's international choices. The Enterprise Enhanced use case narrows only the applicable operations needed for its stated alignment target.
3. **Reusability:** Catalogue components can be shared across multiple PP-Modules and PP-Configurations, promoting consistency across the DBMS iTC's document family and reducing the total evaluation burden.
4. **Evaluation Ownership:** Algorithm-level Evaluation Activities remain those associated with the Catalogue components. Pending publication of the Catalogue Evaluation Methods, the DBMS Crypto SD defines an evidence-reuse mechanism for Certification Body-recognized CAVP, CMVP, or equivalent validation results without originating replacement algorithm tests. The SD continues to define the DBMS-specific integration activities. FIPS 140-3 validation and algorithm validation claims remain separate claims supported by their own evidence.

Appendix G: Glossary

For the purpose of this PP-Module, the following terms and definitions apply. Terms defined in CC:2022 Part 1 [[CC1]] are included where they have particular relevance to this PP-Module.

BYOK (Bring Your Own Key)

A key management model in which the customer or tenant supplies their own cryptographic master key to the TOE, rather than allowing the TOE or the cloud provider to generate it. The customer retains control over the master key lifecycle, including generation, rotation, and destruction. BYOK is enabled in this module by FCS_CKM_EXT.1 (import selection) and FDP_ITC_EXT.1 (trusted channel).

Crypto Catalogue

The Common Criteria Cryptographic Catalogue, a repository of standardized SFR components for cryptographic algorithm implementations maintained by the Common Criteria community. This module invokes Catalogue components rather than defining algorithm-specific SFRs directly, ensuring alignment with current standards.

Data Encryption Key (DEK)

A cryptographic key used to encrypt and decrypt user data at rest. DEKs are generated by the TOE (via `FCS_CKM.1/SKG`) or derived using the applicable Catalogue derivation component (`FCS_CKM.5` or `FCS_CKM_EXT.8`) and are protected by the Master Encryption Key (MEK). DEKs should not be stored in plaintext outside the TOE boundary.

Storage-Scope Encryption

An encryption strategy in which the persistent database storage objects identified in the ST and TSS are encrypted, subject only to documented exclusions that do not contain plaintext user data or that are protected by an equivalent claimed mechanism. This strategy provides broad storage protection while allowing the ST to accurately describe DBMS-specific storage artifacts.

Granular Data Encryption

An encryption strategy in which specific data elements (e.g., individual columns, rows, or cells) are selectively encrypted by the DBMS based on data classification, policy, or sensitivity. This allows finer-grained access control but requires more complex key management.

Key Management System (KMS)

An external system or service that generates, stores, and manages cryptographic keys on behalf of the TOE. In BYOK scenarios, the KMS holds the master key and provides it to the TOE via a trusted channel (FDP_ITC_EXT.1). Examples include hardware security modules (HSMs), cloud-native KMS services (e.g., AWS KMS, Azure Key Vault), and on-premises key management appliances.

Master Encryption Key (MEK)

The root cryptographic key in the DBMS key hierarchy. The MEK protects (wraps) Data Encryption Keys (DEKs). Compromise of the MEK could enable decryption of all data protected by the DEKs it wraps. MEK lifecycle management is governed by FCS_CKM_EXT.1.

TDE (Transparent Data Encryption)

A database encryption feature that automatically encrypts data before it is written to storage and decrypts it when read, transparently to the application. TDE typically implements a key hierarchy with a master key protecting DEKs. This module's FDP_DAR_EXT.1 and FCS_CKM_EXT.1 address the security requirements for TDE implementations.

Appendix H: Acronyms

Table 22. Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
BYOK	Bring Your Own Key
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
cPP	collaborative Protection Profile
DBMS	Database Management System
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
iTC	international Technical Community
KEK	Key Encryption Key
KMS	Key Management System
MEK	Master Encryption Key
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OSP	Organizational Security Policy
PP	Protection Profile
RBG	Random Bit Generator
RSA	Rivest–Shamir–Adleman (asymmetric algorithm)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPD	Security Problem Definition
ST	Security Target
TDE	Transparent Data Encryption
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functionality

Acronym	Meaning
XTS	XEX-based Tweaked CodeBook mode with ciphertext Stealing