Technical Decision TD_DBMS_B_001: Update to Role Definitions and Security Attribute Management for Consistency

Issue

Several Security Functional Requirements (SFRs) in the DBMS cPP, specifically FMT_MSA.1.1, FMT_REV.1.1(2), and FMT_SMR.1.1, contained inconsistencies regarding which roles may manage or revoke security attributes of users and objects.

Prior wording did not align the authority of “users with sufficient privileges” (per the Discretionary Access Control policy) with the defined roles in FMT_SMR.1, nor clearly distinguish between **users** and **objects**.

This resulted in ambiguity for ST authors and evaluators.

Resolution

To resolve these inconsistencies and clarify role definitions and associated authority, the following updates apply to **Section 6.4.1 (FMT_MSA)**, **Section 6.4.3 (FMT_REV)**, **Section 6.4.5 (FMT_SMR)**, and **Section 6.2.1 (FDP_ACC)** of the DBMS cPP v1.3.

Updates to Section 6.4.5 (FMT_SMR – Security Roles)

Replace existing text with:

FMT_SMR.1.1

The TSF shall maintain the roles *[authorized administrator, authorized users, and [assignment: additional authorized identified roles]]*.

Application Note: The new “authorized users” role defined in FMT_SMR.1.1 is referenced in FMT_REV.1.1(2) and FMT_MSA.1.1(2) (Objects).

Updates to Section 6.4.1 (FMT_MSA – Management of Security Attributes)

Revise component text to distinguish user and object contexts as follows.

FMT_MSA.1.1(1) – Users

The TSF shall enforce the [**Discretionary Access Control policy**] to restrict the ability to **[manage]**

the security attributes associated with [**users**] to [**authorized administrator**]s.

FMT_MSA.1.1(2) – Objects

The TSF shall enforce the [**Discretionary Access Control policy**] to restrict the ability to [**manage**] the security attributes associated with [**objects**] to [**authorized administrators, authorized users]**.

Updates to Section 6.4.3 (FMT_REV – Revocation)

Clarify roles permitted to revoke object attributes:

FMT_REV.1.1(2)

The TSF shall restrict the ability to revoke [assignment: list of security attributes] associated with the[**objects**] under the control of the TSF to the [**authorized administrator, authorized users**].

FMT_REV.1.2(2)

The TSF shall enforce the rules [assignment: specification of revocation rules].

Updates to Section 6.2.1 (FDP_ACC – Access Control Policy)

Clarify scope and remove invalid refinements:

FDP_ACC.1.1

The TSF shall enforce the [Discretionary Access Control policy] on all subjects, all DBMS-controlled objects, and all operations among them.

Supporting Guidance

- The term *authorized users* is explicitly added as a role in FMT_SMR.1.1 to harmonize references across management and revocation SFRs.
- *Authorized users* replaces phrases such as “database users with sufficient privileges as allowed by the Discretionary Access Control policy.”
- Management of user-associated attributes is restricted to administrators only; management of object-associated attributes may be performed by administrators and authorized users.
- FDP_ACC.1.1 is clarified to apply comprehensively to all subjects and objects under DBMS control.

Rationale

These updates remove ambiguities and establish consistent role-based authority for security attribute management and revocation.

They align FMT_SMR, FMT_MSA, and FMT_REV with Common Criteria Part 2 principles for evaluability, least privilege, and separation of duties.

Impact

- All evaluations performed against the DBMS cPP v1.3 shall apply these clarifications.
- Security Targets must define “authorized users” as a role where applicable and update documentation and guidance accordingly.
- Evaluators shall confirm that rights to manage and revoke security attributes of users and objects are enforced per these revised role definitions.

Effective immediately. Cite this Technical Decision when applying Sections 6.2.1, 6.4.1, 6.4.3, and 6.4.5 of the DBMS cPP v1.3.