Chapter 1 Introduction

This section identifies the PP-Module as well as the Base PP and provides a Module overview for potential users.

1.1 PP Module Reference

Title: MILS Platform Protection Profile Storage Module
Sponsor: certMILS Consortium
CC Version: 3.1 (Revision 5)
Assurance Level: see the Base PP.
Version: draft
Keywords: Base-PP, PP-module, Operating System, Separation Kernel, MILS

1.2 Base PP Identification

Base MILS Platform Protection Profile, Version: 1.0

1.3 PP Module Overview

This PP module supplements the Base PP by specifying additional functions which are services provided by an SK to control the integrity of the persistent data storage.

The user data stored within the TOE persistent storage is monitored so that when an unauthorized modification takes place, it is detected and an action is performed in order to maintain original consistency and integrity.

Chapter 2 Consistency Rationale

This section states the correspondence between the PP-Module and its Base PP.

2.1 TOE type consistency

The TOE type for which both the Base PP and this PP Module are designed is “a special kind of operating system, namely an SK.”

An SK is a special kind of operating system that allows to effectively separate different containers called “partitions” from each other. Applications themselves are hosted in those partitions. They can also be entire operating systems. The SK is installed and runs on a hardware platform (e.g. embedded systems, desktop class hardware).

This PP Module supplements the Base PP by specifying additional functions which are services provided by an SK to control the integrity of the persistent data storage.

2.2 Security Problem Definition consistency

2.2.1 Assets

The section 3.1 of the Base PP describes the assets to be protected:

- Memory
- CPU time

This PP Module adds the following asset:

- Data Integrity

The new asset is independent and compatible with the assets defined in the Base PP as it does not interfere with the protection of the **Memory** or **CPU time**. It adds protection to the data stored within the TOE boundary instead.

2.2.2 Threats

The section 3.2 of the Base PP describes the threats contemplated:

- T.DISCLOSURE
- T.MODIFICATION
- T.DEPLETION

This PP Module does not contemplate additional threats.

The threat T.MODIFICATION is applicable to the integrity of the data stored within the TOE boundary.

2.2.3 Organizational Security Policies

Neither the Base PP nor this PP Module define organizational security policies.

2.2.4 Assumptions

This PP Module does not define additional assumptions. The assumptions defined in section 3.4 of the Base PP are applicable with no changes.

2.3 Security Objectives consistency

The section 4.1 of the Base PP describes the security objectives to be implemented:

- OT.CONFIDENTIALITY
- OT.INTEGRITY
- OT.AVAILABILITY

This PP Module adds the following security objective for the TOE:

- OT.DATA_INTEGRITY

This security objective extends/concretes OT.INTEGRITY specifically for data stored within the TOE boundary.

2.4 Security Functional Requirements consistency

In addition to the set of SFRs included in section 6.1 of the Base PP, this PP Module defines:

- FDP_SDI.2 Stored Data Integrity Monitoring and Action – This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific functionality for maintaining the integrity of the data stored within the TOE boundary. It has no dependencies with any of the SFRs included in the Base PP.

Chapter 3 Conformance claim

This protection profile module claims conformance to

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001 [1]
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components.Version 3.1, Revision 5. April 2017. CCMB-2017-04-002 [2]
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components.Version 3.1, Revision 5. April 2017. CCMB-2017-04-003 [3]

as follows

- Part 2 conformant.

The “Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017. CCMB-2017-04-004, [4]” has to be taken into account.

This protection profile module is associated with the Base MILS Platform Protection Profile Version 1.0.

3.1 Conformance Rationale

Since a PP module cannot claim conformance to any protection profile, this section is not applicable.

3.2 Conformance Statement

This Protection Profile Module requires strict conformance of any ST or PP claiming conformance to this PP Module.

Note: claiming conformance to this PP Module also requires claiming conformance to the Base MILS Platform Protection Profile.

Chapter 4 Security Problem Definition

This section describes the security aspects of the environment in which the TOE claiming conformance with the PP Module will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment.
- Organizational security policies with which the TOE must comply.
- Assumptions about the secure usage of the TOE.

4.1 Assets

Asset Name	Description	Security Properties to be Preserved
Data Integrity (AS.DATAINT)	The integrity of the data stored within the TOE boundary.	Integrity

Table 1: Assets

4.2 Threats

Assets are defined in Table 0 in Section 4.1. The attackers are the defined in the Base PP.

This PP Module does not define additional threats. The threat T.MODIFICATION is applicable against the asset AS.DATAINT.

4.3 Organizational Security Policies

This module defines no organizational security policies.

4.4 Assumptions

The assumptions are the same as in the base PP.

Chapter 5 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see previous section). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment.

This section presents the solution to the security problem in terms of objectives for the TOE and its operational environment.

5.1 Security Objectives for the TOE

OT.DATA_INTEGRITY

The TSF shall be able to detect unauthorized modifications of persistent data stored within the TOE boundary and perform actions when an integrity error is detected.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are the same as for the base TOE.

5.3 Security Objectives Rationale

	OT.DATA_INTEGRITY
T.MODIFICATION (Base PP)	X

Table 2: Security Objectives Rationale

T.MODIFICATION (Base PP)

If the security objective OT.DATA_INTEGRITY has been reached, the threat T.MODIFICATION is countered for data stored within the TOE boundary.

Chapter 6 Extended Components Definition

This module does not define any extended component.

Chapter 7 Security Requirements

This section defines the Security Functional requirements (SFRs) in relationship with the set of TOE security objectives in the PP-Module and with the security functional requirements of the Base-PP. This PP Module does not introduce specific assurance requirements. The assurance requirements are defined by the Base MILS Platform Protection Profile.

7.1 Security Functional Requirements

7.1.1 FDP_SDI.2 Stored Data Integrity Monitoring and Action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: action to be taken].

7.2 Security Requirements Rationale

	OT.DATA_INTEGRITY
FDP_SDI.2	X

Table 3: SFR Rationale

OT.DATA_INTEGRITY

FDP_SDI.2 specifies the persistent data storage monitoring for integrity check and actions.

7.3 Security Functional Requirements Dependencies Analysis

The following dependencies are defined for the SFRs used in this PP Module:

SFR	Dependencies	Satisfied?
FDP_SDI.2	none	yes

Table 4: SFR Dependencies Rationale

Chapter 8 Application Notes

Persistent data storage integrity check in a MILS system helps protecting user data against unauthorized modifications and thus the reliability of the data stored increase the reliability of the MILS system itself.

An active and efficient stored data integrity check must take place to make this capability be effective, which must in turn be accompanied by a set of actions for avoiding potential attacks to be successful. Then, the actions must guarantee that the integrity will be maintained even when an attack is detected.

Chapter 9 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
PP	Protection Profile
HW	Hardware
SW	Software
OS	Operating System
SK	Separation Kernel
SFR	Security Functional Requirement
SAR	Security Assurance Requirement

Chapter 10 Bibliography

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

[4] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1, Revision 5. April 2017. CCMB-2017-04-004