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 Security Audit 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 audit services provided by an SK to record events to be audited as defined by the SSP.

The information registered for the audit events generated includes, among other, the date and time when the event happened. For being able of including date/time in the audit records, the TOE will be able to provide reliable timestamps for the audit generation routine.

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).

The PP module extends the Base PP by specifying security objectives covering functions relative to audit data generation.

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 does not add any asset.

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.

2.2.3 Organizational Security Policies

This PP Module defines the following organizational security policy:

- P.AUDIT

This OSP extends the security problem definition of the Base PP by adding audit functionality to be covered. Such extension of the SPD is independent and compatible to the original SPD of the Base PP.

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.AUDIT

This security objective adds security functionality to the TOE regarding the audit data generation which is compatible to the rest of security objectives for the TOE defined in the Base PP.

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:

- FAU_GEN.1 Audit Data Generation – This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific functionality for audit data generation. It has no dependencies with any of the SFRs included in the Base PP.
- FPT_STM.1 Reliable Time Stamps – This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific functionality for providing reliable time stamps to the audit data generation functionality. 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 Threats

This PP module has no threats.

4.2 Organizational Security Policies

P.AUDIT

The TOE shall be able to record all events to be audited as defined by the SSP. Thereby, the TOE enforces each possible SSP, i.e. a set of SSPs, concrete configuration parameters with their allowed values shall be exactly described in the TOE User Manuals. For providing reliable timestamps for the audit security functionality, the system integrator shall select timer facilities in the TOE operational environment according to the SIP.

4.3 Assumptions

This PP module has no assumptions.

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.AUDIT

The TOE shall be able to record all events to be audited as defined by the SSP. Thereby, the TOE enforces each possible SSP, i.e. a set of SSPs, concrete configuration parameters with their allowed values shall be exactly described in the TOE User Manuals.

5.2 Security Objectives for the Operational Environment

This PP module has no security objectives for the operational environment.

5.3 Security Objectives Rationale

	OT.AUDIT
P.AUDIT	X

Table 1: Security Objectives Rationale

P.AUDIT

P.AUDIT is directly satisfied by OT.AUDIT.

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 Audit generation

7.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
c) [assignment: other specifically defined auditable events].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

7.1.2 Protection of the TSF

7.1.2.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

7.2 Security Requirements Rationale

	OT.AUDIT
FAU_GEN.1	X
FPT_STM.1	X

Table 2: SFR Rationale

OT.AUDIT

FAU_GEN.1 satisfies OT.AUDIT by generating audit records.

FPT_STM.1 satisfies OT.AUDIT by providing reliable timestamps to the audit records generated.

7.3 Security Functional Requirements Dependencies Analysis

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

SFR	Dependencies	Satisfied?
FAU_GEN.1	FPT_STM.1	yes
FPT_STM.1	none	yes

Table 3: SFR Dependencies Rationale

Chapter 8 Application Notes

Audit records generation in a MILS system helps the traceability of actions, error detection, and eventually attacks identification.

The audit functionality shall be implemented in a manner that it is not possible to avoid audit records generation. The start and stop of the audit records generation must be also recorded to allow audit reviewers identify periods of audit data generation. The startup and shutdown of the audit data generation must be performed according to the startup and shutdown of the entire system.

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