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 Information Flow Control 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 module defines the minimum functionality for controlling the flow of information between partitions that a TOE compliant with the Base MILS Platform Protection Profile has to provide.

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 information flow controlled by the TSF. Such an information flow control policy can be optionally provided by an SK that is compliant to the certMILS base PP.

2.2 Security Problem Definition Consistency

2.2.1 Assets

The base PP describes the assets to be protected:

- Memory (AS.MEM)
- CPU time (AS.TIME)

This PP module does not add any asset.

2.2.2 Threats

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.INFORMATION_FLOW

This OSP extends the security problem definition of the base PP by adding control flow functionality. 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 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. CONTROL_INFORMATION_FLOW

This security objective adds security functionality to the TOE regarding control information flow 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 the base PP, this PP module defines:

- FDP_IFC.1 Subset Information Flow Control – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality for information flow control. It has no dependencies with any of the SFRs included in the base PP.
- FDP_IFF.1 Simple Security Attributes – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality for information flow control. It has no dependencies with any of the SFRs included in the base PP.
- FMT_MSA.1 Management of Security Attributes – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality for management of the security attributes of the information flow control. It has no dependencies with any of the SFRs included in the base PP.
- FMT_MSA.3 Static Attribute Initialisation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality for initialisation of the attributes associated to the information flow control. It has no dependencies with any of the SFRs included in the base PP.
- FMT_SMF.1 Specification of Management Functions – This SFR adds management functionality to the FMT_SMF.1 SFR included in the base PP. ST authors may either iterate this SFR or extend the base PP FMT_SMF.1 by adding specific management functionality for information flow control attributes.

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

There are no specific threats countered by this PP module. A Security Target claiming compliance with this PP module may define the rules controlling information flow to counter specific threats. Those then need to be specified in the Security Target.

4.2 Organizational Security Policies

This PP module addresses the following organizational security policy.

P.INFORMATION_FLOW

The flow of information between partitions needs to be controlled by a set of defined rules partly based (at least partly) on security attributes of partitions.

4.3 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.CONTROL_INFORMATION_FLOW

A TOE compliant with this PP module enforces a set of rules used to control the setup of communication links between partitions.

5.2 Security Objectives for the Operational Environment

In case the security attributes of partitions used within the enforcement of the information flow policy are defined as part of the system build/configuration process, the following security objective for the operational environment holds.

OE.SECURE_INITIALIZATION

The definition of the security attributes of partitions as part of the system build/configuration process is done correctly and completely.

5.3 Security Objectives Rationale

Controlling the flow of information between partitions is done by checking a set of rules before setting up a communication link between partitions. This PP module does not specify what those rules are. They need to be defined in a Security Target that claims compliance to this PP module. Those rules may for example enforce that information coming in from some external network connection (and handled by a network handler partition) is passed through some 'filtering' partitions before it can be transmitted to 'regular' partitions. This example already shows a security attribute that would be part of the rules regulating the information flow: an attribute 'partition type' that at least distinguishes between a 'network connection partition', a 'filtering partition', and a 'regular partition'.

There are many other scenarios where the flow of information between partitions needs to be controlled. The classical label based information flow control is just one example. This information flow control can be implemented by labelling the partitions and controlling that a communication link from one partition to another one can only be set up when the sending partition has a 'lower' classification label than the receiving partition.

Therefore OT.CONTROL_INFORMATION_FLOW addresses the organizational security policy P.INFORMATION_FLOW.

Note: OE.SECURE_INITIALIZATION is addressed by the assumptions made in the base Protection Profile.

Chapter 6 Extended Components Definition

This PP module does not define extended components.

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 Information Flow Control

7.1.1.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on **communication links that are established between partitions**.

7.1.1.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: **partitions and** [assignment: the security attributes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **for establishing a communication link** [assignment: the security attribute-based relationship that must hold between *partitions*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, ~~based on security attributes,~~ that explicitly authorise information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, ~~based on security attributes,~~ that explicitly deny information flows].

Application Note: the rules that define when a communication link is allowed to be established may be based on security attributes of the partitions involved, but also on other TSF data like the assignment of resources to a partition.

7.1.2 Management

7.1.2.1 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

Application Note: In some cases the security attributes used for the information flow control policy will be assigned when the partition is defined by a TOE-external system build/configuration process and not dynamically created during execution of the TSF. In this case the selection in FMT_MSA.1.1 will be set to ‘define’ and the second assignment in FMT_MSA.1.1 will be set to ‘the system build/configuration process’

7.1.2.2 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [selection [assignment: the authorised identified roles], nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: In some cases the security attributes used for the information flow control policy will be assigned when the partition is defined by a TOE-external system build/configuration process and not dynamically created during execution of the TSF. In this case the selection in FMT_MSA.3.1 will be set to 'externally defined' and the selection in FMT_MSA.3.2 will be set to 'nobody'.

7.1.2.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **managing the security attributes of partitions**.

Application Note: In case the security attributes are static and assigned as part of the system build/configuration process, this should be mentioned in the Security Target.

7.2 Security Requirements Rationale

	OT.CONTROL_INFORMATION_FLOW
FDP_IFC.1	X
FDP_IFF.1	X
FMT_MSA.1	X
FMT_MSA.3	X
FMT_SMF.1	X

The purpose of this PP module is the specification of a security attribute based information flow control policy between partitions. This PP module neither specifies what those security attributes are nor does it define the rules of the policy. This allows this PP module to be the basis for many different information flow control policies including a ‘classical’ label based policy like the one defined in the Bell-LaPadula model.

FDP_IFF.1, in conjunctions with FDP_IFC.1, have been selected to allow the specification of an arbitrary security attribute based information flow policy. In the case where a Security Target wants to define a hierarchical label-based policy, selecting FDP_IFC.2 instead of FDP_IFC.1 is allowed.

FDP_IFC.1 has a dependency on FMT_MSA.3 which requires the security attributes of the partitions to be defined upon partition start-up. This can either be done by the TSF in the case where partitions can be created during operation or it can be done externally as part of the system build/configuration process. In the case where those security attributes can be managed during system operation, the rules this management has to follow are specified in FMT_MSA.1.

7.3 Security Functional Requirements Dependencies Analysis

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

SFR	**Dependencies**	**Satisfied?**
FDP_IFF.1	FDP_IFC.1	Yes
FDP_IFC.1	FDP_IFF.1 FMT_MSA.3	yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	yes no yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes no
FMT_SMF.1	none	yes

The dependencies of FMT_MSA.1 and FMT_MSA.3 on FMT_SMR.1 are not satisfied since the specification and management of the security attributes used in the rules of the information flow control policy may be either static, i. e. the security attributes are assigned as part of the system build/configuration process or the security attributes may be assigned automatically as defined by the rules of the policy when a new partition is created dynamically.

Chapter 8 Application Notes

Information flow between partitions in a MILS system is defined by the communication links between partitions. This PP module requires that such communication links can be created dynamically during the execution of the TOE. This PP module requires that such a creation of a new communication link is controlled by some policy which is based on security attributes of the sending and receiving partition. The rules may also include other TSF data like the assignment of specific resources to a partition or the state of the TSF (e. g. if the TOE is in some maintenance mode).

Communication links may be unidirectional or bidirectional. For example, modelling a label based information flow control policy requires the possibility to define unidirectional communication links.

There are many examples where an information flow policy enforced by an SK can be used. Those include:

- Modelling a workflow where information has to be passed via a defined path over different partitions.
- Enforcing a policy where information coming from a network needs to pass through different filters (e.g. firewall based filters, content filtering) before it is delivered to a partition. Each filter function may be implemented in a separate partition.
- Defining ‘clusters’ of partitions that are allowed to share information while they are not allowed to communicate with other clusters. This may be useful when partitions have different levels of trust assigned to them.

All those policies require the definition of security attributes that can be assigned to partitions as well as rules, based on those security attributes, that define the allowed information flow. Whenever a communication link between partitions is established (during start-up of the TOE or, if implemented, dynamically during execution, the TSF verifies that those rules are not violated.

Chapter 9 List of Abbreviations

Abbreviation	Translation
API	Application Programming Interface
MILS	Multiple Independent Levels of Safety / Security
PP	Protection Profile
SSP	System Security Policy
TOE	Target of Evaluation
TSF	TOE Security Functionality

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