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 HAL 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

A *hardware abstraction layer* (HAL) contains a set of drivers for specific hardware components and is supplied and approved by the integrator. In operational use, the product based on the SK always contains exactly one HAL. A HAL is in the same security domain as the SK. A HAL typically provides access to (or abstracts) hardware components such as e.g. timers or other types of interrupt handling. A HAL is protected from non-privileged applications by access control and resource management enforced by the SK.

The HAL ensures that the SK can execute with a given hardware. A HAL is invoked right after the bootloader, it sets up interrupt vectors and memory layout. At run-time provides HAL services, e.g. to trigger the hardware to restart the MILS platform. At run-time a HAL also does initial interrupt handling (including timer interrupts). This initial interrupt handling then invokes other parts of the TSF for further processing. Such further processing can be, for time interrupts, feeding the interrupt to a platform-independent scheduler implemented in the OS, or in other cases even a handler within a partition the interrupt is associated with.

Note: In embedded systems in general, also the term BSP (board support package) is used frequently for support of a specific platform. In a product based on an SK, BSP functionality can be split into:

- supporting functionality directly interacts with hardware which the SK needs to boot and which has to reside within the SK's address space (e.g. interrupt handling, initial setup of address layout) - allocated to the HAL
- functionality which can be implemented in a non-privileged or a privileged partition (e.g. a network card driver),
- and additional functionality which uses well-defined extension API(s) provided by the SK, and which resides in SK extension(s).

This module can be used to ensure that the HAL is certified so that the system integrator can rely on the properties of the HAL to be compliant to the SSP of the TOE.
The (important) task of correct board initialization is not treated in the security problem definition of this module, but it has to be ascertained by the TOE security architecture.

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 PP by specifying security objectives that the HAL provides (setup of memory, interrupts) and implements HAL services that allow the SK to enforce the SSP and ensures that the implementations of interrupt handling and HAL services do not bypass the SK’s SSP.

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.HAL_SERVICE
- P.HAL_INTERRUPT

These OSP extends the security problem definition of the Base PP by adding HAL services. 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 the following change:

- A.TRUSTED_PARTITIONS: This assumptions is modified as the system integrator does not have to analyze the HAL for compliance with the SK.

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.HAL_INTERRUPT
- OT.HAL_SERVICE

This security objective adds security functionality to the TOE regarding the HAL support 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:

- FMT_MOF.1/SERVICE Management of Security Functions Behaviour – This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific HAL services. It has no dependencies with any of the SFRs included in the Base PP.
- FMT_MOF.1/INTERRUPT Management of Security Functions Behaviour – This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific functionality for interrupt handling. 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 HAL support.

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 module defines no threats.

4.2 Organizational Security Policies

This module addresses the following organizational security policy.

P.HAL_SERVICE

The PP Module provides basic HAL functions a compliant TOE may use internally and must provide as services to partitions authorized by the administrative user to use those services. Providing the services of this PP Module to all partitions is also allowed.

P.HAL_INTERRUPT

The PP Module does interrupt handling (including timer interrupts).

4.3 Assumptions

The assumptions are the same as in the base PP minus A.TRUSTED_PARTITIONS for the HAL.

Application Note:

This means that the HAL has been evaluated, i.e. the system integrator does not have to analyze the HAL for compliance with the SK.

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.HAL_INTERRUPT

The initial interrupt handling is controlled by the HAL.

OT.HAL_SERVICE

HAL services are set up and their use is controlled by the HAL.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are the same as in the base PP minus OE.TRUSTED_PARTITIONS for the HAL.

5.3 Security Objectives Rationale

	OT.HAL_INTERRUPT	OT.HAL_SERVICE
P.HAL_INTERRUPT	X	
P.HAL_SERVICE		X

Table 1: Security Objectives Rationale

P.HAL_INTERRUPT

This policy is implemented by OT.HAL_INTERRUPT.

P.HAL_SERVICE

This policy is implemented by OT.HAL_SERVICE.

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 FMT_MOF.1/SERVICE Management of Security Functions Behaviour

FMT_MOF.1.1/SERVICE: The TSF shall restrict the ability to ***use*** the functions [assignment: list of ***HAL* services**] to [assignment: the authorised identified ***entities***].

7.1.2 FMT_MOF.1/INTERRUPT Management of Security Functions Behaviour

FMT_MOF.1.1/INTERRUPT: The TSF shall restrict the ability to ***use*** the ***interrupts*** [assignment: list of ***interrupts***] to [assignment: the authorised identified ***entities***].

7.1.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [

- ***The following services provided by the HAL*** [assignment: list of HAL services]
- ***The following interrupt handling*** [assignment: list of interrupt handling implemented by the HAL]

]

7.2 Security Requirements Rationale

	OT.HAL_INTERRUPT	OT.HAL_SERVICE
FMT_SMF.1	X	X
FMT_MOF.1/INTERRUPT	X	
FMT_MOF.1/SERVICE		X

Table 2: SFR Rationale

OT.HAL_INTERRUPT

FMT_SMF.1 ensures that interrupt management services are implemented. FMT_MOF.1/INTERRUPT ensures that use of interrupts is appropriately restricted.

OT.HAL_SERVICE

FMT_SMF.1 ensures that HAL services are implemented. FMT_MOF.1/SERVICE ensures that use of HAL services is appropriately restricted.

7.3 Security Functional Requirements Dependencies Analysis

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

SFR	Dependencies	Satisfied?
FMT_MOF.1	FMT_SMF.1	yes
	FMT_SMR.1	N – The TOE does not implement roles. The entities accessing the resources are trusted partitions that do not play different roles in the access to such resources
FMT_SMF.1/INTERRUPT	None	yes
FMT_SMF.1/SERVICE	None	yes

Table 3: SFR Functional Requirements Dependencies Analysis

Chapter 8 Application Notes

A HAL typically contains an initialization function, and it is invoked before the SK is invoked. The (important) task of correct board initialization has to be ascertained by the security architecture of the TOE.

Typical HAL services include triggering shutdown or restart of the platform, or changes to cache behaviour. These services usually must be restricted by use of FMT_MOF.1.1/SERVICE.

A typical instantiation of some interrupts can be that no external entity can manage them, e.g. say all timer interrupts are handled by the operating system. For instance, FMT_MOF.1.1/INTERRUPT: The TSF shall restrict the ability to ***use*** the timer interrupts to the operating system scheduler.

Chapter 9 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
HAL	Hardware Abstraction Layer
MILS	Multiple Independent Levels of Safety / Security
OS	Operating System
PP	Protection Profile
SK	Separation Kernel
SFR	Security Functional Requirement
SAR	Security Assurance Requirement
TOE	Target of Evaluation

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