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 Cryptographic Services 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 the cryptographic functions that a TOE compliant with the Base MILS Platform Protection Profile has to provide for its own use as well as for use by authorized partitions.

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 cryptographic functions.

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.CRYPTO_SERVICE

This OSP extends the security problem definition of the base PP by adding basic cryptographic functions that the TOE may use internally. Such extension of the SPD is independent and compatible to the original SPD of the base PP.

2.2.4 Assumptions

This PP module defines the following additional assumptions:

- A.IMPORT

This additional assumption is compatible with the assumptions defined in the base PP. The assumptions included in 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.CRYPTO_SERVICE

This security objective adds security functionality to the TOE by including cryptographic 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 the base PP, this PP module defines:

- FCS_RNG.1 Random Number Generation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to random number generation.
- FCS_CKM.1(SYM) Cryptographic Key Generation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to key generation for symmetric encryption/decryption cryptographic algorithms.
- FCS_CKM.1(RSA) Cryptographic Key Generation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to key generation for RSA.
- FCS_CKM.1(ECDSA) Cryptographic Key Generation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to key generation for RSA.
- FCS_CKM.4 Cryptographic Key Destruction – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to cryptographic key destruction.
- FCS_COP.1(CRYPTO-ENC) Cryptographic Operation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to cryptographic encryption and decryption.
- FCS_COP.1(CRYPTO-MD) Cryptographic Operation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to message digest generation.
- FCS_COP.1(CRYPTO-ECDSA) Cryptographic Operation – This SFR is compatible with the set of SFRs defined in the base PP as it adds independent and specific functionality relative to digital signature generation and verification.

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 extended.

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. The functions it provides may be used by the TSF or by applications executing on the TOE to counter threats related to the confidentiality of information as well as protecting/verifying the integrity and authenticity of information. How the functions provided by this PP module are used within a specific TOE depends on the TOE. A ST claiming compliance to the base PP plus this PP module may therefore list additional threats to those specified in the base PP and the functions specified in this PP module may contribute to counter those threats.

4.2 Organizational Security Policies

This PP module addresses the following organizational security policy.

P.CRYPTO_SERVICE

The PP module provides basic cryptographic 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.

4.3 Assumptions

A.IMPORT

Any critical security parameter imported by the functions of this PP module have been generated in accordance with the requirements for those parameters and are protected accordingly within the TOE environment until and after they are imported to the TOE.

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.CRYPTO_SERVICE

A TOE compliant with this PP module provides its services to entities of the TOE (including the TSF) via the defined interfaces of the module. It is up to the TSF of the TOE to allow or disallow use of the services provided by this module to any active entity controlled by the TSF of the whole TOE.

The following objective is defined for the TOE.

The TSF must provide the following cryptographic services for general use by authorized entities:

- symmetric and asymmetric ciphers,
- message digest generation,
- symmetric and asymmetric key generation.

Note: a TOE that claims compliance to this PP module may use the functions of provided by the PP module to address additional security objectives.

5.2 Security Objectives for the Operational Environment

OE.IMPORT

Any critical security parameter imported by the functions of this PP module have been generated in accordance with the requirements for those parameters and are protected accordingly within the TOE environment until and after they are imported to the TOE.

5.3 Security Objectives Rationale

The security objective OT.CRYPTO_SERVICE addresses the organizational security policy P.CRYPTO_SERVICE.

OE.IMPORT as a security objective for the operational environment addresses the assumption A.IMPORT.

Chapter 6 Extended Components Definition

This section includes possible extended functional components definitions where new functional components not included in CC Part 2 are introduced.

6.1 FCS_RNG Generation of Random Numbers

FCS_RNG.1 Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

6.1.1 Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

6.1.2 Component Levelling

FCS_RNG.1 is not hierarchical to any other component within the FCS_RNG family.

6.1.3 Management

There are no management activities foreseen.

6.1.4 Audit

There are no actions defined to be auditable.

6.1.5 FCS_RNG.1 Random Number Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, physical hybrid, deterministic hybrid] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric].

6.1.6 Rationale

The quality of the random number generator is defined using this SFR. The quality metric required in FCS_RNG.1.2 can be derived from national or international standards.

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 Cryptographic Key Management

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a *deterministic* random number generator that implements: [assignment: standard defining the DRNG algorithm].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric].

Application Note: The quality metric is derived from the properties of the DRNG, the quality of the random numbers used for seeding and the re-seeding intervals.

FCS_CKM.1(SYM) Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [capable of generating a random bit sequence] and specified cryptographic key sizes:

[

1. 128 bits,
2. 256 bits,
3. [assignment: other cryptographic key sizes]

]

that meet the following: [assignment: cryptographic key generation algorithm that has the following properties: Compromising the security of the key generation method shall require at least as many operations as determining the value of the generated key by exhaustive search of the key space]**.**

Application Note: it is expected that the key generation process uses the DRNG defined by the SFR FCS_RNG.1 above.

FCS_CKM.1 (RSA) Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate RSA cryptographic keys in accordance with a specified cryptographic key generation algorithm [defined in U.S. NIST FIPS PUB 186-4 chapter 5.1] and specified cryptographic key sizes:

[

1. 2048 bits,
2. 4096 bits
3. [assignment: other cryptographic key sizes]

]

that meet the following:

[

U.S. NIST FIPS PUB 186-4,

[assignment: list of standards].

]

FCS_CKM.1(ECDSA) Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate ECDSA cryptographic keys in accordance with a specified cryptographic key generation algorithm [defined in ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA)] and specified cryptographic key sizes [as defined by the selected curves and the following curves**:**

- [assignment: list of standards defining elliptic curve parameter]

]

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method of [selection: zeroization, [assignment: other cryptographic key destruction method]] that meets the following: [selection: vendor-specific zeroization, [assignment: list of applicable standards]]

7.1.2 Cryptographic Operation

FCS_COP.1(CRYPTO-ENC) Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [encryption and decryption] in accordance with ~~a specified~~ the following cryptographic algorithms [AES, RSA] and cryptographic key sizes [128, 256 bit (AES), 2048, 4096 bit (RSA)] that meet the following:

[

AES with the following encryption modes:

- CBC,
- [assignment: other block chaining modes or none]

and with the following key sizes:

- 128 bits,
- 256 bits,
- [assignment: other cryptographic key sizes or none],

as defined by FIPS PUB 197;

RSA with the following key sizes:

- 2048 bits,
- 4096 bits
- [assignment: other cryptographic key sizes],

as defined by PKCS #1 v2.2 (RFC 8017)

]

FCS_COP.1(CRYPTO-MD) Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [message digest generation] in accordance with ~~a specified~~ the following cryptographic algorithms [SHA-256, SHA-512, [assignment:: other cryptographic hash functions or none]],

and cryptographic keys sizes [none] that meet the following:

[

- SHA-256 as defined by FIPS PUB 180-4;
- SHA-512 as defined by FIPS PUB 180-4;
- [assignment: standards for other cryptographic hash functions or none]

]

FCS_COP.1(CRYPTO-ECDSA) Cryptographic Operation

FCS_COP.1.1 The TSF shall perform digital signature generation and digital signature verification in accordance with ~~a~~ the specified cryptographic algorithms [RSA and ECDSA] and cryptographic key sizes as defined below that meet the following:
[

- RSA with 2048 bit and 4096 bit as defined in PKCS#1 V2.2 (RFC 8017)
- ECDSA with curves as defined in FCS_CKM.1(ECDSA) following ANSI X9.62-2005 sections 7.3 and 7.4.

]

7.2 Security Requirements Rationale

	OT.CRYPTO_SERVICE
FCS_RNG.1	X
FCS_CKM.1 (SYM)	X
FCS_CKM.1 (RSA)	X
FCS_CKM.1 (ECDSA)	X
FCS_CKM.4	X
FCS_COP.1 (CRYPTO-ENC)	X
FCS_COP.1 (CRYPTO-MD)	X
FCS_COP.1 (CRYPTO-ECDSA)	X

The purpose of this PP module is the provision of some basic cryptographic functions that can be used by the TSF or by applications. Those functions have to include the key generation functionality for the algorithms defined (including the random number generation), the basic method of use for the cryptographic algorithms (encryption/decryption, signature generation/verification, secure hashing), and the destruction of keys. Other parts of key management (including key import/export, key storage, protection, and access, etc.) are left to the specific TOE and not specified in this PP module.

The functions provided by this PP module may well be used for higher level functionality like the implementation of cryptographic protocols. If a TOE does this, it needs to specify the SFRs for those protocols in addition to the SFRs defined in this PP module.

7.3 Security Functional Requirements Dependencies Analysis

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

SFR	Dependencies	Satisfied?
FCS_RNG.1	none	yes
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	yes yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	yes
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	yes yes

This table shows that all dependencies as defined by the extended component definition and by part 2 of the CC are satisfied.

Chapter 8 Application Notes

The purpose of this PP module is the specification of cryptographic services the TSF of a TOE that claims compliance to this PP module has to provide to other parts of the TSF and to authorized partitions. This PP module does not prescribe how those cryptographic functions are implemented and how the TSF defines the conditions under which a partition is allowed to use the services provided by this module. A product compliant with this PP module may implement the functions as part of the kernel, as a kernel extension, as a device driver or as a dedicated partition. It is just important that interfaces exist that allow the use of the functions within the TSF as well as by partitions.

This PP module requires a compliant product to provide the basic algorithms for symmetric encryption and decryption, digital signature generation and verification, secure hashing, key generation for the encryption/decryption and signature generation/verification algorithms, and deterministic random number generation. In the case of ECDSA, this PP module only requires to implement at least on algorithm based on some standardized curve. No specific curve is mandated. Additional algorithms may be added to any ST claiming conformance to this PP module.

The TSF of a compliant product may define their own policy to decide if a partition is allowed to use the services provided by this PP module. Usually the existing services within the TSF to restrict the use of functions to partitions are also used to restrict access to the services of this PP module. The policy defining the conditions for use is therefore not part of this PP module but is part of the TSF of a complaint product in general.

Critical security parameters used by the module may be generated within the module or may be imported by the TSF or by a partition using the module. While the functions to generate some critical security parameters are required to be provided by the module, importing them is also allowed. Since the import itself is not controlled by the module but by the entity using the services of this module, no SFR for external import of such data is defined in the PP module. Such import is subject to the TSF in general and would need to be specified in the ST of a product in addition to the SFRs in this PP module if such an import function exists that is also used for the import of critical security parameter used by the Crypto Services PP module.

A mandatory function for this PP module is the ability to generate keys for the symmetric and asymmetric algorithms specified in the SFRs. The key generation functions will need random numbers with sufficient entropy as input. This generation of the raw entropy is not mandated to be part of the PP module but may instead be generated in the TOE environment e. g. by using a hardware based entropy source. The only function that is mandated as part of this module is the implementation of a deterministic random number generation function (DRNG) which uses the input from the entropy source for seeding the DRNG.

Chapter 9 List of Abbreviations

Abbreviation	Translation
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cypher Block Chaining
DRNG	Deterministic Random Number Generator
FIPS	Federal Information Processing Standard
NIST	National Institute for Standards and Technology
RSA	Rivest, Shamir, Adleman
ECDSA	Elliptic Curve Digital Signature Algorithm
SHA	Secure Hash Algorithm

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

[5] FIPS PUB 180-4 Secure Hash Standard (SHS), National Institute for Standards and Technology, August 2015

[6] FIPS PUB 186-4 Digital Signature Standard (DSS), National Institute for Standards and Technology, July 2013

[7] PKCS#1 V2.2 RSA Cryptography Standard, RSA Laboratories, October 27, 2012

[8] RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2, IETF, November 2016

[9] ANS X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA), November 2005