



**Global
Platform®**

Securing the digital future

GlobalPlatform Technology

Multi-Scope Manager Protection Profile

Version 0.0.0.17

Public Review

December 2025

Document Reference: GPC_SPE_246

Copyright © 2024-2025 GlobalPlatform, Inc. All Rights Reserved.

Recipients of this document are invited to submit, with their comments, notification of any relevant patents or other intellectual property rights of which they may be aware which might be necessarily infringed by the implementation of the specification or other work product set forth in this document, and to provide supporting documentation. This document (and the information herein) is subject to updates, revisions, and extensions by GlobalPlatform, and may be disseminated without restriction. Use of the information herein (whether or not obtained directly from GlobalPlatform) is subject to the terms of the corresponding GlobalPlatform license agreement on the GlobalPlatform website (the "License"). Any use (including but not limited to sublicensing) inconsistent with the License is strictly prohibited.

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Editor note:

Additional requirements for CRA conformance may be added during the Public Review, if necessary.

Contents

1	Introduction	7
1.1	Identification	7
1.2	Audience	7
1.3	IPR Disclaimer	7
1.4	References	8
1.5	Terminology and Definitions	10
1.6	Abbreviations	10
1.7	Revision History	11
2	TOE Overview	12
2.1	TOE Type	12
2.2	TOE Description	12
2.2.1	Isolation	13
2.2.2	Resource Management	14
2.2.3	Dispatcher	14
2.3	TOE Major Security Features	15
2.4	TOE Usage	15
2.5	Non-TOE Hardware/Software/Firmware Available to the TOE	15
2.6	TOE Life Cycle	15
2.7	Instructions for PP-conformant Security Targets	16
3	CC Conformance Claim	17
3.1	PP Conformance Claim	17
3.2	Package Claim	17
3.2.1	Functional Package Claim	17
3.2.2	Assurance Package Claim	17
3.3	Conformance Statement	17
4	Security Problem Definition	18
4.1	Assets	18
4.1.1	User Data	18
4.1.2	TSF Data	18
4.2	Users and Subjects	19
4.3	Threats	19
4.4	Organizational Security Policies	21
4.5	Assumptions	22
5	Security Objectives	23
5.1	Security Objectives for the TOE	23
5.2	Security Objectives for the TOE Operational Environment	24
5.3	Security Objectives Rationale	25
6	Security Requirements	28
6.1	Security Functional Requirements	28
6.1.1	General	28
6.1.2	Security Policies	28
6.1.3	For O.MSM_BEHAVIOUR	29
6.1.3.1	FMT_MOF.1 Management of security functions behaviour	29
6.1.3.2	Dependencies	29

6.1.3.2.1	FMT_SMR.1 Security roles (FMT_SMR.1/MSM_BEHAVIOUR)	30
6.1.3.2.2	FIA_UID.1 Timing of identification (FIA_UID.1/MSM_BEHAVIOUR)	30
6.1.3.2.3	FMT_SMF.1 Specification of Management Functions (FMT_SMF.1/MSM_BEHAVIOUR)	30
6.1.4	For O.SCOPE_COMMUNICATION	31
6.1.4.1	FDP_IFC.1 Subset information flow control	31
6.1.4.2	FDP_IFF.1 Simple security attributes	31
6.1.4.3	Dependencies	32
6.1.4.3.1	FMT_MSA.3 Static attribute initialization (FMT_MSA.3/SCOPE_COMM)	32
6.1.4.4	Discarded Dependencies	33
6.1.5	For O.SCOPE_ID	33
6.1.5.1	FMT_MTD.1 Management of TSF data (FMT_MTD.1/SCOPE_ID)	33
6.1.5.2	Discarded dependencies	33
6.1.6	For O.SCOPE_ISOLATION	34
6.1.6.1	FDP_ACC.1 Subset access control	34
6.1.6.2	FDP_ACF.1 Security attribute-based access control	34
6.1.6.3	FDP_RIP.2 Full residual information protection	35
6.1.6.4	Dependencies	35
6.1.6.4.1	FMT_MSA.3 Static attribute (FMT_MSA.3/SCOPE_ISOLATION)	35
6.1.6.4.2	FMT_MSA.1 Management of security attributes	36
6.1.6.4.3	FMT_SMR.1 Security roles (FMT_SMR.1/SCOPE_ISOLATION)	36
6.1.6.4.4	FIA_UID.1 Timing of identification (FIA_UID.1/SCOPE_ISOLATION)	37
6.1.6.4.5	FMT_SMF.1 Specification of Management Functions (FMT_SMF.1/SCOPE_ISOLATION)	37
6.1.7	For O.SCOPE_LC	37
6.1.7.1	FMT_MTD.1 Management of TSF data (FMT_MTD.1/SCOPE_LC)	37
6.1.7.2	Dependencies	38
6.1.7.2.1	FMT_SMR.1 Security roles (FMT_SMR.1/SCOPE_LC)	38
6.1.7.2.2	FIA_UID.1 Timing of identification (FIA_UID.1/SCOPE_LC)	38
6.1.7.2.3	FMT_SMF.1 Specification of Management Functions (FMT_SMF.1/SCOPE_LC)	39
6.1.8	For O.SCOPE_PROTECTION	39
6.1.8.1	FPR_UNO.1 Unobservability	39
6.2	Security Assurance Requirements	39
6.3	Security Requirements Rationale	39
6.3.1	Rationale for the SFRs and Objectives	39
6.3.2	Dependencies	41
6.3.2.1	SFRs Dependencies	41
6.3.2.2	SARs Dependencies	43
6.3.3	Rationale for the Security Assurance Requirements	44
6.3.4	ALC_DVS.2 Sufficiency of Security Measures	44
6.3.5	ALC_FLR.2 Flaw Remediation Procedures	44
6.3.6	AVA_VAN.5 Advanced Methodical Vulnerability Analysis	45
7	Functional Package for Resource Allocation	46
7.1	Introduction	46
7.1.1	Identification	46
7.1.2	Overview	46
7.2	Security Problem Definition	46
7.2.1	Organisational Security Policy	46
7.3	Security Objectives	46
7.3.1	Security Objectives for the TOE	46
7.3.2	Security Objectives Rationale	47
7.4	Security Functional Requirements	47

7.4.1	FRU_RSA.2 Minimum and maximum quotas	47
7.5	Security Requirements Rationale	47
7.5.1	Rationale for the SFR and Objectives.....	47
7.5.2	Dependencies	47

Tables

Table 1-1: References	8
Table 1-2: Terminology and Definitions	10
Table 1-3: Abbreviations	10
Table 1-4: Revision History	11
Table 2-1: MSM Life Cycle	16
Table 5-1: Security Objectives Rationale	25
Table 6-1: Security Objectives and SFRs – Coverage	41
Table 6-2: SFRs Dependencies	42
Table 6-3: SARs Dependencies	43

1 INTRODUCTION

This document defines the Protection Profile for the Multi-Scope Manager (PP-MSM) within a Multi-Scope Platform (MSP).

An MSP is a Secure Element (SE) that implements the Java Card specifications [JCVM], [JCAPI], [JCRE] and the GlobalPlatform Card Specification ([GPCS]), and that supports multiple isolated Scopes. The form factor of an MSP includes smartcards, eUICCs, and eSEs.

A Scope consists of a set of Security Domains (SD) and Java Card applications. A Scope may be either a SAM Scope ([GP-SAM]), an eUICC ([SGP.21], [SGP.22]), or an ISD-controlled eSE.

This Protection Profile (PP) applies in the context of MSPs that comply with the GlobalPlatform Protection Profile for Secure Elements ([PP-SE]). It extends [PP-SE] with the security requirements for managing multiple isolated Scopes.

1.1 Identification

Title	Protection Profile for Multi-Scope Manager (PP-MSM)
Reference	GPC_SPE_246
Date	December 2025
Version	0.0.0.17
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Internet of Trust
CC Version	CC:2022 Revision 1
Assurance Level	EAL4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5

1.2 Audience

This document is intended primarily for the use of:

- **Developers:** This document presents the security requirements to implement the management of multiple Scopes in an MSP.
- **Scope Issuers and Service Providers:** This document allows comparison between MSP-enabled products and gives confidence in the product security.
- **Evaluators:** This document is a normative document for the evaluation of MSPs.
- **Certification Bodies:** This document is a normative document for the certification of MSPs.

1.3 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit <https://globalplatform.org/specifications/ip-disclaimers/>. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.4 References

This section lists references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: References

Standard / Specification	Description	Ref
GlobalPlatform Card Specification	GlobalPlatform Technology Card Specification v2.4, November 2025 Document Reference: GPC_SPE_034	[GPCS]
GPCS SAM Configuration	GlobalPlatform Technology SAM Configuration v1.0 Document Reference: GPC_GUI_217	[GP-SAM]
Java Card API	Application Programming Interface, Java Card™ Platform, version 3.2 Oldest Accepted Version: 2.2	[JCAPI]
Java Card VM	Virtual Machine Specification, Java Card™ Platform, version 3.2 Oldest Accepted Version: 2.2	[JCVN]
Java Card RE	Runtime Environment Specification, Java Card™ Platform, version 3.2 Oldest Accepted Version: 2.2	[JCRE]
GSMA SGP.21	GSM Association Remote SIM Provisioning (RSP) Architecture Version 3.0	[SGP.21]
GSMA SGP.22	GSM Association Remote SIM Provisioning (RSP) Technical Specification, Version 3.0	[SGP.22]
CC:2022 R1	Common Criteria for information Technology Security Evaluation, Parts 1 to 5 CC:2022 Revision 1, November 2022	[CC:2022]
CC:2022 Part 1	Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022 Revision 1, November 2022 Document reference: CCMB-2022-11-001	[CC1]
CC:2022 Part 2	Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements, CC:2022 Revision 1 Part 2 November 2022 Document reference: CCMB-2022-11-002	[CC2]
CC:2022 Part 3	Common Criteria for information Technology Security Evaluation, Part 3: Security assurance components, CC:2022 Revision 1, November 2022 Document reference: CCMB-2022-11-003	[CC3]

Standard / Specification	Description	Ref
CC:2022 Part 5	Common Criteria for information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1, November 2022 Document reference: CCMB-2022-11-005	[CC5]
CEM:2022 R1	Common Evaluation Methodology, CEM:2022 Revision 1, November 2022 Document reference: CCMB-2022-11-006	[CEM]
CC Composite evaluation	Enisa, EUCC scheme, State-of-the-art document, Composite product evaluation and certification for CC:2022, version 1, February 2025	[CC-Comp]
Secure Element PP	GlobalPlatform Technology Secure Element Protection Profile, version 2.0, July 2025 Document reference: GPC_SPE_174	[PP-SE]
Java Card PP	Oracle Java Card System - Open Configuration Protection Profile, version 3.2, July 2024 Document reference: BSI-CC-PP-0099-V3-2024	[PP-0099]
eUICC PP	GSMA eUICC for Consumer and IoT Devices Protection Profile, version 2.1, February 2025 Document reference: SGP.25	[SGP.25]
Security IC Platform PP	Eurosmart Security IC Platform Protection Profile, version 1.0, January 2014 Document reference: BSI-CC-PP-0084-2014	[PP-0084]
3S in SoC PP	Eurosmart Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, version 1.8, 23 October 2023 Document reference: BSI-CC-PP-0117-V2-2023	[PP-0117]
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]

Application note: ST authors can use a different (newer or older) version of a reference if a rationale is provided, and the evaluation confirms that the used versions are appropriate and do not impact the conformity to the PP. For GlobalPlatform specifications, the version used must not be older than the oldest accepted version¹ indicated in Table 1-1, and newer versions than the versions referenced in this document can be used under evaluated rationale.

¹ The oldest accepted versions are those referenced in [PP-SE].

1.5 Terminology and Definitions

Selected terms used in this document are included in Table 1-2.

Table 1-2: Terminology and Definitions

Term	Definition
SAM Scope	Scope where a unique SAM SD and possibly several ASP-controlled applications are installed. <i>(See [GP-SAM] section 3.3.)</i>
Scope	A set of isolated SDs and applications under the control of the Scope SD, with managed access to resources and mediated communication channels that preserve confidentiality and integrity.
Scope Issuer	An entity that owns the Scope and is ultimately responsible for the behaviour of the Scope.
Scope SD	Primary on-card entity of a Scope providing support for the control, security, and communication requirements of the Scope Issuer.

1.6 Abbreviations

The abbreviations used in this document are included in Table 1-3.

Table 1-3: Abbreviations

Abbreviation	Meaning
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASP	Application Service Provider
CPU	Central Processing Unit
eSE	embedded Secure Element
eUICC	embedded Universal Integrated Circuit Card
I2C	Inter-Integrated Circuit
I3C	Improved Inter-Integrated Circuit
IPR	Intellectual Property Rights
ISD	Issuer Security Domain
JCS	Java Card System
MSM	Multi-Scope Manager
MSP	Multi-Scope Platform
OSP	Organisational Security Policy
PP	Protection Profile
PP-MSM	Protection Profile for Multi-Scope Manager (this document)
RAM	Random Access Memory

Abbreviation	Meaning
RNG	Random Number Generator
SAM	Secured Applications for Mobile
SAR	Security Assurance Requirement
SD	Security Domain
SE	Secure Element
SFP	Security Function Policy
SFR	Security Functional Requirement
SPD	Security Problem Definition
SPI	Serial Peripheral Interface
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

1.7 Revision History

GlobalPlatform technical documents numbered $n.0$ are major releases. Those numbered $n.1$, $n.2$, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered $n.n.1$, $n.n.2$, etc., are maintenance releases that incorporate errata and clarifications; all non-trivial changes are indicated, often with revision marks.

Table 1-4: Revision History

Date	Version	Description
Apr 2025	0.0.0.10	Committee Review
Aug 2025	0.0.0.14	Member Review
Dec 2025	0.0.0.17	Public Review
TBD	1.0	Public Release

2 TOE OVERVIEW

2.1 TOE Type

The Target of Evaluation (TOE) type is the Multi-Scope Manager (MSM) for the support of multiple isolated Scopes within a Multi-Scope Platform (MSP) implementing Java Card specifications and the GlobalPlatform Card Specification ([GPCS]). A Scope hosts Java Card applications, Security Domains (SDs) and native applications. A Scope is managed by a unique Scope Security Domain (Scope SD), which behaves like the ISD of a classic GlobalPlatform SE for that Scope. A Scope can be either a SAM Scope ([GP-SAM]), an eUICC ([SGP.21], [SGP.22]), or an ISD-controlled eSE.

The TOE security guidance is part of the TOE.

The MSP consists of the MSM embedded in an SE. The MSP includes the following components:

- The hardware, either a secure IC or a secure sub-system in SoC (3S in SoC), and dedicated software.
- The Java Card System (JCS) including the runtime environment, the virtual machine, and the API compliant with the Java Card specifications [JCRE], [JCVM], [JCAPI].
- The GlobalPlatform Framework compliant with [GPCS], to manage applications within the Scopes, as well as the Scope SDs.²
- The MSM for ensuring the isolation of the Scopes from each other.

The MSP shall meet [PP-SE], which means that the JCS shall meet [PP-0099] and the hardware shall meet either [PP-0084] or [PP-0117].

The MSP may contain native applications in line with the [PP-0099].

Application note:

- The PP-MSM focuses on the requirements for the management of multiple isolated Scopes only; that is, on the requirements for the MSM. This avoids duplicating definitions and requirements for the embedding SE, which are defined in [PP-SE], [PP-0099], and [PP-0084] / [PP-0117]. Nevertheless, for any PP-MSM-conformant Security Target (ST), the TOE is the PP-SE-conformant MSP, including the MSM.
- The evaluation of an MSP against the PP-MSM and the [PP-SE] can be performed at the same time, or the composite evaluation approach defined in [CC-Comp] can be used. In the latter case, the MSP is evaluated against [PP-SE] first and then against the PP-MSM, as defined in the _COMP assurance package (see [CC5]).

2.2 TOE Description

The MSP provides all the features of the SE plus the complete isolation of storage and execution of the different Scopes managed by the MSM.

A Scope hosts SDs, Java Card applications and related data and, potentially, native applications. Each Scope operates as the only resident entity in the MSP, using its own exclusive interface for communication. Additionally, the Scopes are isolated from any native application present in the platform which is not included in any Scope.

² Scope SDs are fixed in the MSP. The creation of Scopes is not covered in this PP.

Multiple Scopes can be active in the MSP at a time. Resources can be shared but Scopes have an exclusive access to the resources allocated to them.

The MSM stands for the entity responsible for enforcing the isolation of the Scopes within the MSP. The main functionalities of the MSM are:

- **Isolation:** Ensures separation between Scopes, preventing any direct or indirect interaction between Scopes, while executing within the same physical environment.
- **Resource management:** Handles the allocation of resources, such as CPU, volatile and non-volatile memory, RNG, and cryptographic co-processors to the Scopes.
- **Dispatcher:** Determines the presence and availability of a requested Scope, and dispatches requests to the selected Scope, managing multiple active Scopes if supported.

The Scopes are created and provisioned before delivery in a secure environment. The MSM can define a Scope life cycle policy to manage the states after delivery, which at a minimum should prevent re-entering the irreversible provisioning stage.

Scopes are accessible to their users (Issuers and any external entities) through exclusive I/O interfaces. The I/O interfaces of the Scopes are logically separated regardless of the underlying physical implementation. Logical separation is maintained whether Scopes share a single physical I/O interface (e.g., SPI, I2C, I3C), utilize multiple distinct physical interfaces, or a combination of both (e.g., two Scopes sharing one physical interface while a third Scope operates on a separate physical interface). Each Scope I/O interface operates as a distinct communication channel over the physical interface, ensuring secure and isolated access to the corresponding Scope.

The Scopes are isolated entities in the platform, which are considered out of the MSP (in the sense of the TOE).

This PP does not assume or mandate any specific implementation of the MSM. The implementation may utilize low-level separation mechanisms such as micro-kernel hypervisors or implement software-based mechanisms to ensure isolation between Scopes, potentially supported by hardware mechanisms.

2.2.1 Isolation

The MSM ensures the confidentiality and integrity of Scopes (code, data, and operations) by enforcing multiple layers of isolation. This prevents interference or unauthorised access among Scopes and between Scopes and the MSP.

- **Memory isolation**
 - Isolation mechanisms are used to enforce memory boundaries.
 - Policies are enforced to prevent Scopes from accessing memory outside their own allocation.
 - Any attempt by a Scope to read or write memory owned by a different scope is detected and the operation is blocked. (Such an event should lead to an immediate exception or error and subsequent actions to maintain a secure state.)
 - When memory allocated to a Scope is released, the memory contents are securely erased before reallocating it, e.g. to another Scope. This prevents residual data from being accessible outside the owner Scope.
- **Execution isolation**
 - Policies are enforced to ensure each Scope uses an exclusive execution environment isolating the execution of the processes and data-in-use of each Scope.
 - A Scope cannot observe or interfere with the execution of other Scopes.

- **Communication isolation**

- Exclusive communication channels and interfaces are defined through which Scopes and their Issuers (or any authorised entity on behalf the Scope Issuers) can interact (send and receive APDUs).
- Scopes and Scope Issuers are restricted to use these designated interfaces for all communications.
- Unauthorised communication attempts are denied.
- Inter-Scope communications are not allowed.

2.2.2 Resource Management

The MSM ensures secure management of platform resources among Scopes in accordance with defined security policies, based on the initial allocation. This includes:

- **CPU management**

- Processing power among Scopes

- **Memory management**

- Memory is allocated to Scopes based on their needs.
- Allocated memory is only accessible to the owner Scope.
- Data stored in memory is erased upon allocation or deallocation.
- Optionally, memory limits prevent any Scope from overconsuming resources.

- **(Cryptographic) co-processor access**

- Control exclusive access to the same (cryptographic) co-processors by Scopes.
- The access of (cryptographic) co-processors by Scopes can only be achieved using APIs such as the Java Card API.
- Data stored in volatile memory of (cryptographic) co-processors is securely erased upon deallocation.

- **Random Number Generator (RNG) access**

- Policies are enforced to control exclusive access to the same RNG by Scopes.
- Scopes can only access the RNG by using APIs such as the Java Card API.
- Data stored in volatile memory of the RNG is securely erased upon deallocation.

2.2.3 Dispatcher

The MSM handles in/out commands and logical channel operations ensuring accurate delivery of requests/answers to/from the appropriate Scopes, protected from disclosure and modification.

- **Authentication and authorisation**

- Policies are enforced to verify the identity of the entity requesting services from Scopes and check if it is authorised to access the requested Scope.

- **Scope presence and availability**

- Dispatching checks whether a requested Scope is installed within the MSP.

- Dispatching determines whether the requested Scope is currently operational and ready to process incoming commands and activates the requested Scope if necessary.
- **Request dispatching and protection**
 - Policies are enforced to establish and manage logical channels for communication between external entities and Scopes, including termination of such channels and erasure of any residual data.
 - Incoming authorised requests are directed to the corresponding active Scope based on identifiers.
 - IN/OUT data integrity and confidentiality are protected both between the MSP and the external users and within the MSP.

2.3 TOE Major Security Features

The TOE major security features consist in the isolation of Scopes within an SE and the controlled access to Scopes' resources and communication channels. This enables the SE to be shared amongst Scope Issuers without any interference between the Scopes and without compromising their assets, which cannot be accessed from outside the owner Scope.

2.4 TOE Usage

The TOE is intended to be used for the implementation of security-intensive digital services that are controlled by different entities through different Scopes within the SE, in form factor such as smart cards, eUICC, or eSE.

The TOE targets environments that require deployments of different services under strict separation. Envisaged services include telecom, payment and financial services, identity and authentication, and any services that rely on cryptographic, storage, and execution capabilities that are resistant to hardware and software attacks at high levels of attack potential. The TOE enables these services to operate securely and concurrently on an SE while preserving their independence.

2.5 Non-TOE Hardware/Software/Firmware Available to the TOE

The non-TOE hardware/software/firmware that is available to the TOE includes the device supporting services.

From the PP-MSM point of view, the SE platform on which the MSP is built-in is logically part of the environment of the TOE and supports the provision of the TOE features. Nevertheless, the TOE of a PP-MSM-conformant ST is the MSP.³

2.6 TOE Life Cycle

The MSM is integrated into the MSP and therefore follows the seven life cycle phases already defined in [PP-SE]. This section does not replace those requirements but highlights additional activities that apply to the MSM.

Table 2-1 presents the life cycle phases and details the additional activities applicable to the MSM components. It further indicates the phases during which the MSM may be subject to delivery, in accordance with the overall SE life cycle.

³ The MSP security is driven by the PP-MSM and the PP-SE. This means that the assumption on the off-card Java Card bytecode verification of CAP files applies.

Table 2-1: MSM Life Cycle

Phase	MSM Specific Additions	Delivery
Phases 1 and 2: Product Development	Design, implement, test, and document the MSM.	
Phase 3: IC Manufacturing	May: <ol style="list-style-type: none"> 1. Embed the MSM binary in the IC 2. Configure the MSM 3. Create Scopes 4. Allocate resources 5. Provision / personalise Scopes (Scope SD keys) 6. Enable Scopes 	X
Phase 4: IC Packaging	-	
Phase 5: Composite Product Integration	May: <ol style="list-style-type: none"> 1. Embed the MSM binary in the IC 2. Configure the MSM 3. Create Scopes 4. Allocate resources 5. Provision / personalise Scopes (Scope SD keys) 6. Enable Scopes 	X
Phase 6: Personalisation	-	
Phase 7: Operational Usage	Enforce the MSM life cycle policy	

MSM development is carried out in Phase 1, under the same controlled and security-protected environment required for TOE development in [PP-SE]. During this phase the manufacturer specifies, implements, tests, and documents the MSM so that it meets the functional and design requirements of the final product and remains consistent with IC user guidance. The development environment must therefore prevent unauthorised disclosure of MSM source code, test data, and sensitive documentation and must preserve their integrity. Conformance evaluation for this PP-MSM shall include the MSM development environment.

Similarly to the SE life cycle, delivery of MSM components may occur in Phase 3 (IC Manufacturing), in Phase 5 (Composite-Product Integration), or be split between the two.

Before delivery, the manufacturer performs the following activities: embed the MSM binary in the IC, configure the MSM, create the Scopes, allocate resources, provision Scopes, and enable Scopes. The environments where these activities occur (in Phase 3 or 5), shall protect the confidentiality and integrity of all components of the TOE and any related material. The relevant sites and procedures are included in the evaluation.

During Phase 7,⁴ the MSM enforces its life cycle policy where no transition can return a Scope to the irreversible provisioning stage completed in Phase 3 or 5. State-change commands after delivery must be authenticated by the Scope Issuer.

2.7 Instructions for PP-conformant Security Targets

The SE evaluation against [PP-SE] can be done at the same time as the MSM evaluation, to form an MSP evaluation. In this case, the objective for the TOE operational environment OE.SUPPORT_SE shall become an objective for the TOE.

⁴ Elsewhere in this document, Phase 7 is referred to as the end user phase.

3 CC CONFORMANCE CLAIM

The PP-MSM claims conformance to CC:2022 Revision 1 [CC:2022]. It is

- CC Part 2-conformant [CC2] and
- CC Part 3-conformant [CC3].

3.1 PP Conformance Claim

The PP-MSM does not claim conformance to any other PP. Nevertheless, the PP-MSM extends [PP-SE] and indirectly [PP-0099] and [PP-0084] or [PP-0117].

Security Targets can claim conformance to PP-MSM and [PP-SE] at the same time.

3.2 Package Claim

3.2.1 Functional Package Claim

The PP-MSM claims conformance to the functional package defined in this document:

- Resource Allocation, see section 7.

This package is optional and shall be claimed in an SE PP-conformant ST if the underlying functionality is supported by the TOE.

3.2.2 Assurance Package Claim

The PP-MSM claims conformance to the assurance package EAL4 augmented with:

- ALC_DVS.2 Sufficiency of security measures
- ALC_FLR.2 Flaw reporting procedures
- AVA_VAN.5 Advanced methodical vulnerability analysis.

3.3 Conformance Statement

The PP-MSM requires demonstrable conformance of STs and PPs claiming conformance to it.

4 SECURITY PROBLEM DEFINITION

4.1 Assets

4.1.1 User Data

The user data constitutes the primary assets of the TOE. User data stands for the code and data of the applications and libraries belonging to the Scopes. It can be either persistent or transient.

User data falls in one of the following categories:

- **Scope code:** The code of the Java Card applications and libraries belonging to a Scope. GlobalPlatform Security Domains are a special type of application.

This forms the program basis needed for services/functionalities provided by the Scope to the user. This is stored in non-volatile memory allocated to the Scope.

Properties: Integrity, confidentiality (execution on behalf of authorised users only).
- **Scope persistent data:** The persistent data of the Java Card applications and libraries belonging to a Scope.

This data is stored in non-volatile memory allocated to the Scope.

For example, cryptographic keys of GlobalPlatform SDs, certificates, application personalisation data.

Properties: Integrity, confidentiality (access on behalf of authorised users only, by the owner Scope).
- **Scope transient data:** The runtime data of the Java Card applications and libraries belonging to a Scope.

This data is stored in volatile memory allocated to the Scope, e.g. RAM, or cryptographic co-processors' memory.

For example, session keys.

Properties: Integrity, confidentiality (access on behalf of authorised users only, by the owner Scope).

Application note:

- Scope code maps to D.APP_CODE defined in [PP-0099] and PP-SE.
- Scope persistent and transient data maps to D.APP_C_DATA, D.APP_I_DATA, D.APP-KEYS, and D.CRYPTO defined in [PP-0099] and PP SE.
- Scope code and data belong to the embedded software defined in [PP-0084] and [PP-0117].

4.1.2 TSF Data

The TSF data constitutes the secondary assets of the TOE. TSF data stands for the code and data of the MSM. It can be either persistent or transient.

TSF data falls in one of the following categories:

- **MSM code:** All the software and firmware of the TSF.

This is stored in persistent memory.

Properties: Integrity

- **MSM Registry:** Set of identification and life cycle data that serves to uniquely identify the Scopes and determine their status.
This is persistent data.
Properties: Integrity.
- **MSM persistent data:** Internal data used to enforce the policies for the isolation of the Scopes, the allocation of resources, and the dispatching of commands to the Scopes.
This data is stored in persistent memory.
The MSM Registry is part of the MSM persistent data.
Properties: Integrity.
- **MSM transient data:** Runtime data required to handle the Scopes and to enforce the policies for the isolation of the Scopes, the allocation of resources, and the dispatching of commands to the Scopes.
This data is stored in persistent memory.
Properties: Integrity and confidentiality.

4.2 Users and Subjects

The users of the TOE are the following:

- The Scopes installed in the MSP
- The Scope Issuers
- The external entities interacting with the MSP and the Scopes.

The Scopes are also the subjects of the TOE.

4.3 Threats

The threats to the TOE are the unauthorised disclosure or modification of the assets and the unauthorised or modified execution of the Scopes' applications. Both runtime attacks to defeat (bypass or corrupt) its security functionality that are realized through the execution of an application (belonging to a Scope), which in turn may require the exploitation of unsecure (series of) commands and shared resources (memory or co-processors), and physical attacks are in the scope.

Remark: Denial-of-service (DoS) threat is out of scope of this PP.

T.ABUSE_MSM

The attacker executes an application of a Scope or interacts with the MSM to modify its behaviour and gain control over the MSP and get unauthorised access to Scopes.

Directly Threatened Asset(s): MSM code, MSM persistent data, MSM transient data, MSM Registry.

Application note: The effect of such attack may be the modification of MSM configuration data (e.g. isolation policies), the injection of malicious code, the (partial) enabling/disabling of the isolation, resource allocation, or dispatching mechanisms.

T.EXPLOIT_COMMUNICATION

The attacker executes an application within a Scope to exploit the communication channels of other Scopes and compromise the integrity and/or confidentiality of the transferred data (IN/OUT).

Directly Threatened Asset(s): Scope persistent data, Scope transient data (integrity, confidentiality).

T.EXPLOIT_EXECUTION

The attacker executes an application within a Scope to trigger the execution and take control of an application of another Scope. This leads to unauthorised access to Scope's data.

Directly Threatened Asset(s): Scope code, Scope persistent data, Scope transient data (integrity, confidentiality).

T.EXPLOIT_MEMORY

The attacker executes an application within a Scope to exploit the memory that is or has been shared with other Scopes and compromise the integrity and/or the confidentiality of the data of those Scopes.

Directly Threatened Asset(s): Scope persistent data, Scope transient data (integrity, confidentiality).

T.EXPLOIT_RESOURCES

The attacker executes an application within a Scope to exploit a co-processor that is or has been shared with other Scopes and compromise the integrity and/or confidentiality of the data of those Scopes that is managed or stored at co-processor level.

Directly Threatened Asset(s): Scope persistent data, Scope transient data (integrity, confidentiality).

T.IMPERSONATE_ISSUER

The attacker impersonates the Scope Issuer, thus leading to unauthorised access to the Scope applications and their data.

Directly Threatened Asset(s): Scope code, Scope persistent data, Scope transient data (integrity, confidentiality).

T.MODIFY_EXECUTION

The attacker executes an application within a Scope to modify (interfere with) the execution of other Scopes and compromise the integrity of the services and the data of those Scopes.

Directly Threatened Asset(s): Scope code, Scope persistent data, Scope transient data (integrity).

T.OBSERVE_EXECUTION

The attacker executes an application within a Scope to observe the execution of other Scopes and compromise the confidentiality of the data of those Scopes when they are transferred inside the MSP.

Directly Threatened Asset(s): Scope persistent data, Scope transient data (confidentiality).

T.PHYSICAL

The attacker applies physical tampering techniques to disclose or modify the design of the TOE, its sensitive data or code, or its runtime execution.

Directly Threatened Asset(s): All assets.

T.UNAUTHORISED_SCOPE_MGT

The attacker performs unauthorised Scope management operations to alter the status of a Scope and make it potentially accessible/inaccessible under different conditions than expected.

Directly Threatened Asset(s): MSM registry (integrity)

Application note: The Security Target should provide information about the valid status of a Scope, which is not specified in this PP (e.g. inactive, active, blocked, terminated).

4.4 Organizational Security Policies

OSP.SCOPE_CREATION

The creation of all the Scopes of the MSP shall be conducted securely and supervised by authorised entities before the end user phase.

This includes:

- The initial allocation of dedicated persistent memory and exclusive resources
- The initial binding to exclusive interfaces

Application note: The TOE can provide means of changing the initial allocation and interfaces.

OSP.SCOPE_LC

A Scope life cycle policy shall be defined, and the MSM shall enforce this policy.

OSP.SCOPE_RESOURCES

The allocation of system resources to Scopes shall be sufficient for the functioning of their services. This includes:

- The initial allocation of system resources, including dedicated persistent memory and any exclusive resources
- The initial binding to the allowed interfaces

OSP.SCOPE_SD

Each Scope shall have a unique Scope Security Domain (Scope SD), which is created, installed, and initialized securely before the end user phase.

The Scope SD shall operate independently (without a parent SD) and shall be explicitly recognized and registered as a trusted entity.

A Scope shall be under the exclusive control of its Scope SD.

OSP.SCOPE_SD_KEYS

The security of the Scope SD keys shall be ensured by a well-defined security policy that covers their generation, storage, distribution, destruction, and recovery. This policy is enforced by the Scope Issuer and the entity responsible for the provisioning/personalisation of the Scope.

4.5 Assumptions

A.ISSUER

It is assumed that the Scope Issuer is responsible for the Scope's services and behaviour.

A.PROTECTION_AFTER_DELIVERY

It is assumed that security procedures are applied to the TOE after delivery up to the end user phase to prevent any possible copy, modification, retention, theft, or unauthorised use.

5 SECURITY OBJECTIVES

5.1 Security Objectives for the TOE

O.MSM_BEHAVIOUR

The TOE shall ensure that either the configuration of the MSM functions is unmodifiable or the configuration of the MSM can only be performed by authorised entities and that such operations do not impact the Scope's policies which are under exclusive control of the Scope SDs.

O.SCOPE_COMMUNICATION

The TOE shall ensure that Scopes receive/send commands through the allowed interfaces only.

Application note: Scopes operate under the control of the Scope SD.

O.SCOPE_ID

The TOE shall ensure that each Scope is identified with a unique unmodifiable identifier.

O.SCOPE_ISOLATION

The TOE shall enforce the isolation of resources, including memory, execution, and communication, for all Scopes, ensuring that each Scope has exclusive access to its allocated memory, execution environment, and an exclusive logical I/O interface for communication.

O.SCOPE_LC

The TOE shall provide a policy for managing the life cycle of Scopes. It shall ensure that the Scope Issuer is the only entity authorised to manage the life cycle of that Scope and to change its state according to that policy.

Application note:

- The management of the Scope encompasses the management of the Scope SD.
- The life cycle contains at a minimum two states: Enabled and Permanently Disabled. Any other implementation-dependent state is part of the Enabled state.
- Enabled Scopes are assigned permanent resources for exclusive use. Scopes can use temporary resources, allocated at runtime.

O.SCOPE_PROTECTION

The TOE shall ensure that Scopes are protected from observation or interference by other Scopes.

5.2 Security Objectives for the TOE Operational Environment

OE.ISSUER

The Scope Issuer shall be responsible for the Scope's services and behaviour.

OE.PROTECTION_AFTER_DELIVERY

Security procedures shall be applied to the TOE after delivery up to the end user phase to prevent any possible copy, modification, retention, theft, or unauthorised use.

OE.SCOPE_CREATION

The creation of all the Scopes of the MSP shall be conducted securely and supervised by authorised entities before delivery.

OE.SCOPE_RESOURCES

Scopes shall be granted a set of system resources that is sufficient for the functioning of their services. This includes:

- the initial allocation of system resources, including dedicated persistent memory and any exclusive resources,
- the initial binding to the allowed interfaces.

OE.SCOPE_SD

Each Scope shall have a unique Scope Security Domain (Scope SD), which is created, installed, and initialized securely before delivery.

The Scope SD shall operate independently (without a parent SD) and shall be explicitly recognized and registered as a trusted entity.

A Scope shall be under the exclusive control of its Scope SD.

OE.SCOPE_SD_KEYS

The security of the Scope SD keys shall be ensured in the environment of the TOE.

OE.SUPPORT_SE

The SE shall provide security mechanisms to protect the management of the Scopes and their isolation by the MSM from logical and physical attacks.

Those mechanisms shall be sufficient to allow the MSP to meet [PP-SE], and indirectly either [PP-0084] or [PP-0117].

Application note:

- From the PP-MSM point of view, SE physical and logical security is the responsibility of the TOE environment.
- From the point of view of a PP-conformant ST, SE physical and logical security is enforced by the TOE.

5.3 Security Objectives Rationale

Table 5-1: Security Objectives Rationale

SPD Elements	Security Objectives Rationale
A.ISSUER	OE.ISSUER The Scope Issuer is responsible for the Scope's services and behaviour.
A.PROTECTION_AFTER_DELIVERY	OE.PROTECTION_AFTER_DELIVERY Prevents any compromise or unauthorised use of the TOE in the operational environment before the end user phase.
OSP.SCOPE_CREATION	OE.SCOPE_CREATION All Scopes in the MSP are securely created under the supervision of authorised entities before entering the end user phase.
OSP.SCOPE_LC	O.SCOPE_LC Enforces the life cycle policy and ensures that the Scope Issuer is the only entity that acts according to that policy.
OSP.SCOPE_RESOURCES	OE.SCOPE_RESOURCES The OSP is directly enforced by the security objective for the operational environment.
OSP.SCOPE_SD	OE.SCOPE_SD Ensures that the Scope SD is created, installed, and initialized securely before the end user phase.
OSP.SCOPE_SD_KEYS	OE.SCOPE_SD_KEYS The OSP is directly enforced by the security objective for the operational environment.
T.ABUSE_MSM	O.SCOPE_ID Ensures that Scope identifiers are unique and unmodifiable. O.MSM_BEHAVIOUR Ensures that only authorised entities apply configuration changes respecting the Scope's policy that is under control of the Scope SD. OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.

SPD Elements	Security Objectives Rationale
T.EXPLOIT_COMMUNICATION	<p>O.SCOPE_ISOLATION Limits authorised users to their designated interfaces, ensuring the confidentiality and integrity of communication data.</p> <p>OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.</p>
T.EXPLOIT_EXECUTION	<p>O.SCOPE_ISOLATION Restricts Scopes to access to their allocated execution resources and context.</p> <p>OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.</p>
T.EXPLOIT_MEMORY	<p>O.SCOPE_ISOLATION Enforces memory boundaries and limits Scopes to their allocated memory.</p> <p>OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.</p>
T.EXPLOIT_RESOURCES	<p>O.SCOPE_ISOLATION Restricts Scopes to access to their allocated execution resources and context.</p> <p>OE.SCOPE_RESOURCES Enforces the MSM resource allocation policy.</p> <p>OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.</p>
T.IMPERSONATE_ISSUER	<p>O.SCOPE_COMMUNICATION Verifies the identity and authorisation of entities that issue or receive commands through allowed interfaces.</p> <p>OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.</p>
T.MODIFY_EXECUTION	<p>O.SCOPE_PROTECTION Ensures that only authorised users have access to the execution processes.</p> <p>OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.</p>

SPD Elements	Security Objectives Rationale
T.OBSERVE_EXECUTION	O.SCOPE_PROTECTION Ensures that execution resources or services usage remains undisclosed to unauthorised entities. OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.
T.PHYSICAL	OE.SUPPORT_SE The SE provides mechanisms against physical tampering.
T.UNAUTHORISED_SCOPE_MGT	O.SCOPE_ID Ensures that Scope identifiers are unique and unmodifiable. O.SCOPE_LC Ensures that Scope management operations are authenticated and authorised based on the entity's identity. OE.SUPPORT_SE The SE provides mechanisms to prevent logical and physical attacks.

6 SECURITY REQUIREMENTS

6.1 Security Functional Requirements

6.1.1 General

In this document the SFRs are presented per security objective, SFRs are iterated as necessary, and the CC dependencies are placed in dedicated subsections. Moreover, for the SFRs that are instantiated, the original text is provided in boxes. Refinements are underlined>.

6.1.2 Security Policies

This PP defines two security policies for the TSF:

- Scope Communication Information Flow Control SFP
- Scope Isolation Access Control SFP.

The definition of policies uses the following representation of the TSF in terms of TSF data, subjects, objects, information, operations, security attributes, users and roles:

- TSF data:
 - Scope registry
 - Resource registry
 - Security attributes of subjects and objects
- Subjects:
 - Scopes, with security attributes:
 - identifier (unmodifiable)
 - status [Enabled, Permanently Disabled, implementation-dependent status]
 - allowed interfaces
- Objects:
 - Resources, with security attributes:
 - Identifier (unmodifiable)
 - status [free, allocated, permanently allocated]
 - owner [Scope] (unmodifiable if permanently allocated)

where Resource stands for:

 - Memory resource: physical and virtual memory regions allocated to Scopes
 - Execution resource: CPU, (cryptographic) co-processor, random number generator (RNG)
 - Communication resource: physical or virtual interface
- Allowed operations:
 - In/out APDU commands
 - Internal operations:

- allocate a resource (to a Scope)
- deallocate a resource (from a Scope)
- access a resource (by a Scope) – read/write/execute
- Users:
 - External users of the services provided by the Scopes
 - Scope Issuers
- Roles:
 - The MSM itself, for the management of the Scopes' life cycle
 - (Optional) Role for the configuration of the MSM (e.g. MSM administrator)
 - (Optional) Role for the management of security attributes.

6.1.3 For O.MSM_BEHAVIOUR

6.1.3.1 FMT_MOF.1 Management of security functions behaviour

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Refinement to cover the case where the MSM functions are unmodifiable.

The TSF shall [selection: *disallow any changes to the MSM functions, restrict the ability to*] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: ***list of configurable MSM functions***] to [assignment: *the authorised identified roles*].

Application note:

- The MSM functions include those used to enforce the isolation of Scopes, to manage the resources, and to dispatch the commands.
- If the MSM configuration is not disabled, then:
 - The list of configurable MSM functions cannot be empty.
 - There must be at least one role, e.g. MSM Administrator, allowed to perform the configuration operations.

6.1.3.2 Dependencies

The dependencies issued from FMT_MOF.1 apply if the MSM is configurable:

- FMT_SMR.1 applies if the MSM is configurable.

- FMT_SMF.1 applies if the MSM is configurable and if there is any management function related to the MSM configuration, for instance the management of the role(s).
- FIA_UID.1 applies if the MSM is configurable.

6.1.3.2.1 FMT_SMR.1 Security roles (FMT_SMR.1/MSM_BEHAVIOUR)

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/MSM_BEHAVIOUR

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

The TSF shall maintain the roles [assignment: ***the authorised identified roles for the configuration of the MSM***].

FMT_SMR.1.2/MSM_BEHAVIOUR

The TSF shall be able to associate users with roles.

6.1.3.2.2 FIA_UID.1 Timing of identification (FIA_UID.1/MSM_BEHAVIOUR)

Dependencies: No dependencies.

FIA_UID.1.1/MSM_BEHAVIOUR

The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/MSM_BEHAVIOUR

The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

Application note: The user is the one that plays the role defined in FMT_SMR.1/MSM_BEHAVIOUR.

6.1.3.2.3 FMT_SMF.1 Specification of Management Functions (FMT_SMF.1/MSM_BEHAVIOUR)

Dependencies: No dependencies.

FMT_SMF.1.1/MSM_BEHAVIOUR

The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

Application note: This is an optional SFR. The management functions, if any, are those necessary for the configuration of the MSM, for example, the management of roles. If there is no such management function, the dependency should be discarded.

6.1.4 For O.SCOPE_COMMUNICATION

6.1.4.1 FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

The TSF shall enforce the **Scope Communication Information Flow Control SFP** on:

- Subjects: **Scopes**
- Information: **Any information carried by in/out APDU commands or internal communication**
- Operations:
 - **In and out APDU commands originating in or received by Scopes**
 - **Inter-Scope communication.**

6.1.4.2 FDP_IFF.1 Simple security attributes

Dependencies:

FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute

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: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

The TSF shall enforce the **Scope Communication Information Flow Control SFP** based on the following types of subject and information security attributes: **Scope identifier, Scope status, Scope allowed interfaces.**

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: [assignment: *for each operation, the security attribute-based relationship that hold between subject and information security attributes*].

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **The Scope involved in the operation is [selection: Enabled, [assignment: *list of any specific implementation-dependent life cycle states within the Enabled state*]], and**
- **The operation uses an interface that is allowed for the Scope that sends or receives the information.**

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*].

The TSF shall explicitly deny an information flow based on the following rules:

- **The information flows from one Scope to another (inter-Scope communication is forbidden), or**
- **The interface is not allowed for the Scope that sends or receives the information, i.e. the rule defined in FDP_IFF.1.2 does not hold.**

6.1.4.3 Dependencies

6.1.4.3.1 FMT_MSA.3 Static attribute initialization (FMT_MSA.3/SCOPE_COMM)

Dependencies:

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1/SCOPE_COMM

The TSF shall enforce the [assignment: *access control SFP, 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.

The TSF shall enforce the **Scope Communication Information Flow Control SFP** to provide **no** default values for security attributes that are used to enforce the SFP.

Application note: The values of the security attributes are either defined at the creation of the Scopes, which is out of the scope of the PP, or updated under certain conditions.

FMT_MSA.3.2/SCOPE_COMM

The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

The TSF shall allow ~~the~~ **no role** to specify alternative initial values to override the default values when an object or information is created.

Application note: The information (APDU command) has no security attribute relevant for this policy.

6.1.4.4 Discarded Dependencies

The following dependencies of FMT_MSA.3 are not applicable:

- FMT_MSA.1 Management of security attributes: The **Scope Communication Information Flow Control SFP** does not manage the security attributes used to enforce the rules of the SFP.
- FMT_SMR.1 Security roles: There is no authorised role.

6.1.5 For O.SCOPE_ID

6.1.5.1 FMT_MTD.1 Management of TSF data (FMT_MTD.1/SCOPE_ID)

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SCOPE_ID

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

The TSF shall restrict the ability to **query** the **identifiers stored in the Scope Registry to itself**.

6.1.5.2 Discarded dependencies

The following dependencies of FMT_MTD.1 are not applicable:

- FMT_SMR.1 Security roles: The operations can only be performed by the TSF itself.
- FMT_SMF.1 Specification of management functions: There is no other management function than query.

6.1.6 For O.SCOPE_ISOLATION

6.1.6.1 FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

The TSF shall enforce the **Scope Isolation Access Control SFP** on:

- Subjects: **Scopes**
- Objects: **Resources (memory resources, execution resources, communication resources)**
- Operations: **allocate, deallocate, read, write, execute.**

6.1.6.2 FDP_ACF.1 Security attribute-based access control

Dependencies:

FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute

FDP_ACF.1.1

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

The TSF shall enforce the **Scope Isolation Access Control SFP** to objects based on the following: **Scope identifier, Scope status, resource identifier, resource status, resource owner.**

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The operation is performed by or on behalf of a Scope in any of the following states [selection: Enabled, [assignment: *list of any specific implementation-dependent life cycle states within the Enabled state*]], and**
- **(allocation) The resource to allocate is free (it is not allocated to any Scope), or**

- (deallocation) The resource to deallocate is not permanently allocated to the requesting Scope, or
- (read/write/execute) The resource involved in the operation is allocated to the requesting Scope.

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **A Scope is denied access to any resource that is not allocated to it.**

6.1.6.3 FDP_RIP.2 Full residual information protection

Dependencies: No dependencies.

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] all objects.

Editorial refinement:

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] any object.

Application note: The author of the Security Target can select allocation or deallocation depending on the type of resource or object, using either one or multiple iterations of FDP_RIP.2.

6.1.6.4 Dependencies

6.1.6.4.1 FMT_MSA.3 Static attribute (FMT_MSA.3/SCOPE_ISOLATION)

Dependencies:

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1/SCOPE_ISOLATION

The TSF shall enforce the [assignment: *access control SFP, 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.

The TSF shall enforce the **Scope isolation Access 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.

Application note: It is acceptable to provide “no” default values.

FMT_MSA.3.2/SCOPE_ISOLATION

The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Application note: It is allowed to not authorise any role to specify alternative initial values, and therefore to assign “None”.

6.1.6.4.2 FMT_MSA.1 Management of security attributes

Dependencies:

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1

The TSF shall enforce the [assignment: *access control SFP(s), 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*].

The TSF shall enforce the **Scope Isolation Access Control SFP** 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*].

6.1.6.4.3 FMT_SMR.1 Security roles (FMT_SMR.1/SCOPE_ISOLATION)

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/SCOPE_ISOLATION

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

The TSF shall maintain the roles [assignment: *the authorised identified roles related to the management of security attributes used in the Scope Isolation SFP*].

FMT_SMR.1.2/SCOPE_ISOLATION

The TSF shall be able to associate users with roles.

6.1.6.4.4 FIA_UID.1 Timing of identification (FIA_UID.1/SCOPE_ISOLATION)

Dependencies: No dependencies.

FIA_UID.1.1/SCOPE_ISOLATION

The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/SCOPE_ISOLATION

The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

Application note: The user is the one that plays the role defined in FMT_SMR.1/SCOPE_ISOLATION.

6.1.6.4.5 FMT_SMF.1 Specification of Management Functions (FMT_SMF.1/SCOPE_ISOLATION)

Dependencies: No dependencies.

FMT_SMF.1.1/SCOPE_ISOLATION

The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

Application note: This is an optional SFR. The management functions, if any, are those necessary for the isolation of the Scopes, for example the management of roles. If there is no such management function, the dependency should be discarded.

6.1.7 For O.SCOPE_LC

6.1.7.1 FMT_MTD.1 Management of TSF data (FMT_MTD.1/SCOPE_LC)

Dependencies:

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SCOPE_LC

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

The TSF shall restrict the ability to **modify** the **life cycle state of a Scope** to the **Scope Issuer**.

Application note:

- The TSF should support two states at least: Enabled and Permanently Disabled. A permanently disabled Scope cannot receive, send, or process any further request.
- The Enabled state is the default state given upon creation and provisioning of the Scope.
- The Enabled state cannot be reached from the Permanently Disabled state.

6.1.7.2 Dependencies

6.1.7.2.1 FMT_SMR.1 Security roles (FMT_SMR.1/SCOPE_LC)

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/SCOPE_LC

The TSF shall maintain the roles [assignment: *the authorised identified roles*].

The TSF shall maintain the roles **Scope Issuer**.

FMT_SMR.1.2/SCOPE_LC

The TSF shall be able to associate users with roles.

6.1.7.2.2 FIA_UID.1 Timing of identification (FIA_UID.1/SCOPE_LC)

Dependencies: No dependencies.

FIA_UID.1.1/SCOPE_LC

The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

The TSF shall allow **no TSF-mediated action** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/SCOPE_LC

The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

6.1.7.2.3 FMT_SMF.1 Specification of Management Functions (FMT_SMF.1/SCOPE_LC)

Dependencies: No dependencies.

FMT_SMF.1.1/SCOPE_LC

The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

The TSF shall be capable of performing the following management functions: **Scope life cycle management [assignment: list of transition rules]**.

Application note:

- The transition rules should address all the reachable states (Enabled, Permanently Disabled, and implementation-dependent life cycle states).

6.1.8 For O.SCOPE_PROTECTION

6.1.8.1 FPR_UNO.1 Unobservability

Dependencies: No dependencies.

FPR_UNO.1.1

The TSF shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*].

Refinement:

The TSF shall ensure that **applications within a specific Scope** are unable to observe or interfere with the **operations on any object by other Scopes**.

6.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5.

6.3 Security Requirements Rationale

6.3.1 Rationale for the SFRs and Objectives

Table 6-1 presents the coverage of the security objectives for the TOE by the SFR. The rationale is the following:

O.MSM_BEHAVIOUR The following requirements fulfil the objective:

- FMT_MOF.1 ensures that MSM functions are either entirely unmodifiable or strictly modifiable by authorised entities only, preventing unauthorised changes and protecting the exclusive control of Scope policies by Scope SDs.
- FMT_SMR.1/MSM_BEHAVIOUR (Applies if the MSM is configurable) defines security roles to distinguish authorised entities permitted to manage MSM configurations, ensuring that exclusive MSM control remains with designated users.
- FIA_UID.1/MSM_BEHAVIOUR (Applies if the MSM is configurable) ensures identification of users prior to allowing MSM configuration changes.
- FMT_SMF.1/MSM_BEHAVIOUR (Applies if the MSM is configurable) explicitly defines the management functions available for MSM configuration.

O.SCOPE_COMMUNICATION The following requirements fulfil the objective:

- FDP_IFC.1 enforces the Scope Communication Information Flow Control SFP by restricting APDU and internal communication flows for Scopes.
- FDP_IFF.1 enforces information flow based on defined security attributes and rules, ensuring that only specified and authorised interfaces are used to send/receive commands to Scopes considering the Scope status.
- FMT_MSA.3/SCOPE_COMM enforces strict control over Scopes communication by ensuring that the Scope Communication Information Flow Control SFP defines no default security attribute values and prevents any role from overriding initial values.

O.SCOPE_ID The following requirement fulfils the objective:

- FMT_MTD.1/SCOPE_ID ensures that only the TSF can access Scope identifiers from the Scope Registry.

O.SCOPE_ISOLATION The following requirements fulfil the objective:

- FDP_ACC.1 ensures that each Scope has exclusive access to its allocated memory, execution environment, and communication resources, enforcing the Scope Isolation Access Control SFP.
- FDP_ACF.1 enforces the Scope Isolation Access Control SFP based on security attributes to ensure that Scopes/entities acting on behalf of Scopes can only perform operations on the resources according to defined isolation rules.
- FDP_RIP.2 ensures that residual data from deallocated resources is completely cleared before reuse.
- FMT_MSA.3/SCOPE_ISOLATION ensures that default security attribute values for enforcing the Scope Isolation Access Control SFP are explicitly defined to prevent unintended access. The SFR restricts modification of initial values to authorised roles.
- FMT_MSA.1 enforces the Scope Isolation Access Control SFP by restricting the ability to modify security attributes to authorised roles only.
- FMT_SMR.1/SCOPE_ISOLATION defines and maintains the authorised roles responsible for managing security attributes under the Scope Isolation Access Control SFP.
- FIA_UID.1/SCOPE_ISOLATION ensures that users must be successfully identified before performing any TSF-mediated actions, except those explicitly permitted prior to identification.
- FMT_SMF.1/SCOPE_ISOLATION ensures that the TSF provides defined management functions necessary to enforce the isolation of Scopes.

O.SCOPE_LC The following requirements fulfil the objective:

- FMT_MTD.1/SCOPE_LC ensures that only the Scope Issuer can modify the Scope life cycle state, preventing unauthorised state changes.

- FMT_SMR.1/SCOPE_LC defines and maintains the Scope Manager role responsible for managing the Scope life cycle.
- FIA_UID.1/SCOPE_LC ensures that no TSF-mediated actions related to Scope life cycle management can be performed before a user is identified.
- FMT_SMF.1/SCOPE_LC ensures that the TSF provides management functions for Scope life cycle control, enforcing the life cycle states transition rules.

O.SCOPE_PROTECTION The following requirement fulfils the objective:

- FPR_UNO.1 prevents applications within a Scope from observing or interfering with objects of other Scopes.

Table 6-1: Security Objectives and SFRs – Coverage

Security Objectives	Security Functional Requirements
O.MSM_BEHAVIOUR	FMT_MOF.1 FMT_SMR.1/MSM_BEHAVIOUR FMT_SMF.1/MSM_BEHAVIOUR FIA_UID.1/MSM_BEHAVIOUR
O.SCOPE_COMMUNICATION	FDP_IFC.1 FDP_IFF.1 FMT_MSA.3/SCOPE_COMM
O.SCOPE_ID	FMT_MTD.1/SCOPE_ID
O.SCOPE_ISOLATION	FDP_ACC.1 FDP_ACF.1 FDP_RIP.2 FMT_MSA.3/SCOPE_ISOLATION FMT_MSA.1 FMT_SMR.1/SCOPE_ISOLATION FMT_SMF.1/SCOPE_ISOLATION FIA_UID.1/SCOPE_ISOLATION
O.SCOPE_LC	FMT_MTD.1/SCOPE_LC FMT_SMR.1/SCOPE_LC FMT_SMF.1/SCOPE_LC FIA_UID.1/SCOPE_LC
O.SCOPE_PROTECTION	FPR_UNO.1

6.3.2 Dependencies

6.3.2.1 SFRs Dependencies

Table 6-2 presents the SFR dependencies defined in [CC2] and which components satisfy them.

Table 6-2: SFRs Dependencies

Security Functional Requirement	CC Dependencies	Satisfied Dependencies
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3/SCOPE_ISOLATION
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3/SCOPE_COMM
FDP_RIP.2	No dependencies	
FIA_UID.1/MSM_BEHAVIOUR	No dependencies	
FIA_UID.1/SCOPE_ISOLATION	No dependencies	
FIA_UID.1/SCOPE_LC	No dependencies	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1/MSM_BEHAVIOUR FMT_SMF.1/MSM_BEHAVIOUR Apply if the MSM is configurable
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1/SCOPE_ISOLATION FMT_SMF.1/SCOPE_ISOLATION
FMT_MSA.3/SCOPE_COMM	FMT_MSA.1 FMT_SMR.1	Dependencies are not applicable See section 6.1.4.4
FMT_MSA.3/SCOPE_ISOLATION	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1/SCOPE_ISOLATION
FMT_MTD.1/SCOPE_ID	FMT_SMR.1 FMT_SMF.1	Dependencies are not applicable See section 6.1.5.2
FMT_MTD.1/SCOPE_LC	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1/SCOPE_LC FMT_SMF.1/SCOPE_LC
FMT_SMF.1/MSM_BEHAVIOUR	No dependencies	
FMT_SMF.1/SCOPE_ISOLATION	No dependencies	
FMT_SMF.1/SCOPE_LC	No dependencies	
FMT_SMR.1/MSM_BEHAVIOUR	FIA_UID.1	FIA_UID.1/MSM_BEHAVIOUR Applies if the MSM is configurable
FMT_SMR.1/SCOPE_ISOLATION	FIA_UID.1	FIA_UID.1/SCOPE_ISOLATION
FMT_SMR.1/SCOPE_LC	FIA_UID.1	FIA_UID.1/SCOPE_LC

6.3.2.2 SARs Dependencies

Table 6-3 presents the SAR dependencies defined in [CC3] and which components satisfy them.

Table 6-3: SARs Dependencies

SARs	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	ADV_FSP.4 ADV_TDS.3
ADV_FSP.4	ADV_TDS.1	ADV_TDS.3
ADV_IMP.1	ADV_TDS.3 ALC_TAT.1	ADV_TDS.3 ALC_TAT.1
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4
AGD_OPE.1	ADV_FSP.1	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_FLR.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1 ASE_INT.1 ASE_REQ.2	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1 ASE_OBJ.2	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	ADV_FSP.4 ASE_INT.1 ASE_REQ.2	ADV_FSP.4 ASE_INT.1 ASE_REQ.2
ATE_COV.2	ADV_FSP.4 ATE_FUN.1	ADV_FSP.4 ATE_FUN.1

SARs	CC Dependencies	Satisfied Dependencies
ATE_DPT.1	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	ADV_FSP.4 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.5	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1

6.3.3 Rationale for the Security Assurance Requirements

EAL4 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. The targeted EAL4 is augmented with AVA_VAN.5 implementing the resistance requirement against attackers with high attack potential, ALC_DVS.2 and ALC_FLR.2. This evaluation assurance level allows a developer to gain high assurance from positive security engineering based on good practices. The targeted EAL4 represents the best current practical compromise between the level of assurance and resistance to attackers. The level AVA_VAN.5 is only achieved if the vulnerability assessment is based on analysis of low-level hardware design and source code analysis.

6.3.4 ALC_DVS.2 Sufficiency of Security Measures

Development security is concerned with physical, procedural, personnel, and other technical measures that shall be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the sensitivity of the TOE and embedded software, it is necessary to justify the sufficiency of these requirements protecting the integrity and confidentiality of the TOE during development. ALC_DVS.2 has no dependencies.

6.3.5 ALC_FLR.2 Flaw Remediation Procedures

The TOE is expected to host highly sensitive applications which require tracking and remediation of any reported security flaw. The TOE developer must therefore define and use procedures to ensure timely reception and management of flaw reports and communication of associated corrective measures and fixes. ALC_FLR.2 provides sufficient assurance about flaw remediation procedures applicable to any release of the TOE. ALC_FLR.2 does not have any dependency.

6.3.6 AVA_VAN.5 Advanced Methodical Vulnerability Analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for Java Card/GlobalPlatform technology-based products hosting sensitive applications, particularly in payment and identity areas. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1, and AGD_OPE.1. All these assurance requirements are met by EAL4.

7 FUNCTIONAL PACKAGE FOR RESOURCE ALLOCATION

7.1 Introduction

7.1.1 Identification

Name	Functional Package for Resource Allocation
Version	0.0.0.17
Date	December 2025
Sponsor	GlobalPlatform, Inc.
CC Edition	CC:2022 Revision 1

7.1.2 Overview

The functional package Resource Allocation applies when the MSP offers a resource allocation service for shared resources that may be used by Scopes on the platform. Examples of resource allocation include, but are not limited to, volatile memory, non-volatile memory, execution time slots on the processing unit, and access to cryptographic co-processors or other hardware functions. The MSM enforces quotas whenever a Scope requests shared resources, ensuring that no single Scope can exhaust or lock the resource and thus preserving overall system responsiveness.

This functional package does not address denial-of-service (DoS) in general, which is considered out of scope.

7.2 Security Problem Definition

7.2.1 Organisational Security Policy

OSP.RESOURCE_ALLOCATION

The dynamic allocation of system resources to Scopes shall enforce constraints to mitigate deliberate or undeliberate abuse of resources.

7.3 Security Objectives

7.3.1 Security Objectives for the TOE

O.RESOURCE_ALLOCATION

The TOE shall provide mechanisms that enforce constraints on the dynamic allocation of system resources to Scopes.

7.3.2 Security Objectives Rationale

OSP.RESOURCE_ALLOCATION

The objective O.RESOURCE_ALLOCATION directly covers the OSP.

7.4 Security Functional Requirements

7.4.1 FRU_RSA.2 Minimum and maximum quotas

Dependencies: No dependencies.

FRU_RSA.2.1

The TSF shall enforce maximum quotas of the following resources [assignment: *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

The TSF shall enforce maximum quotas of the following resources [assignment: *controlled resources*] that **Scopes** can use [selection: *simultaneously, over a specified period of time*].

FRU_RSA.2.2

The TSF shall ensure the provision of minimum quantity of each [assignment: *controlled resource*] that is available for [selection: *an individual user, defined group of users, subjects*] to use [selection: *simultaneously, over a specified period of time*].

The TSF shall ensure the provision of minimum quantity of each [assignment: *controlled resource*] that is available for **Scopes** to use [selection: *simultaneously, over a specified period of time*].

Application note: “controlled resource” stands for the system resources whose dynamic allocation is controlled by the MSM to ensure fair access and prevent overconsumption, e.g. CPU / co-processor processing power, volatile / non-volatile memory.

7.5 Security Requirements Rationale

7.5.1 Rationale for the SFR and Objectives

O.RESOURCE_ALLOCATION

FRU_RSA.2 enforces minimum and maximum resource quotas allocated to Scopes ensuring controlled and constrained dynamic resource allocation.

7.5.2 Dependencies

FRU_RSA.2 does not have dependencies.