GlobalPlatform Technology

Secure Media Path Protection Profile Module

Version 0.0.6

Public Review

September 2020

Document Reference: GPD_SPE_090

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.

This document is provided as a member benefit to GlobalPlatform members only. Please help us maintain the value of your membership and encourage recruitment by observing this restriction.

Contents

Figures

Tables

1 Introduction

This document defines the Secure Media Path (SMP) Protection Profile Module on top of the Trusted Execution Environment Protection Profile (TEE PP) for the Content Protection use case.

This version of the document contains a description of the SMP platform, the definition of the assets and the definition of the environment in terms of threats, assumptions and policies. The document also defines the security objectives and requirements for the SMP platform, which complete the TEE objectives and requirements defined in the TEE PP.

This document states the security requirements for Enhanced Content protection within TEE-enabled devices.

1.1 Audience

This document is intended primarily for the use of TEE and TA developers, OEMs, content service providers, as well as evaluation laboratories, certification bodies, and consumers of Common Criteria (CC) or GlobalPlatform certificates.

1.2 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.

1.3 References

Table 1-1 and Table 1-2 list normative and informative references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: Normative References

Standard / Specification	Description	Ref
CC Part 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.	[CC1]
CC Part 2	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, revision 5, April 2017. CCMB-2017-04-002.	[CC2]
CC Part 3	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, revision 5, April 2017. CCMB-2017-04-003.	[CC3]
CEM	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017. CCMB-2017-04-004.	[CEM]

Standard / Specification	Description	Ref
GPD_SPE_007	TEE Client API Specification (Last applicable version)	[TEE Client API]
GPD_SPE_009	TEE System Architecture (Last applicable version)	[TEE Arch]
GPD_SPE_010	TEE Internal Core API Specification (Last applicable version)	[TEE Core API]
GPD_SPE_021	TEE Protection Profile v1.2.1 (Core PP)	[TEE PP]
GPT_SPE_140	TEE Protection Profile with Debug PP-Module v1.2.1	[TEE PP-D]
GPT_SPE_141	TEE Protection Profile with Time and Rollback PP-Module v1.2.1	[TEE PP-T]
ECP	Enhanced Content Protection, v1.1, MovieLabs	[ECP]
HDCP	High-bandwidth Digital Content Protection 2.2 (or better), Intel Corporation https://www.digital-cp.com/hdcp-specifications	[HDCP]
HDMI	High Definition Multimedia Interface 2.1, HDMI Forum http://hdmiforum.org/specifications/	[HDMI]

Table 1-2: Informative References

Standard / Specification	Description	Ref

1.4 Terminology and Definitions

Selected terms used in this document are included in Table 1-3.

Table 1-3: Terminology and Definitions

Term	Definition
Conditional Access	System for allowing consumers access only to content streams to which they have subscribed. Typically used to protect broadcast media content.
Enhanced Content	Valuable digital media content as per [ECP], including UHD.
Graphics Processor Unit	Programmable hardware block capable of performing advanced graphics processing.
Protected Media Manager	The software which controls access to protected media assets.

1.5 Abbreviations and Notations

Table 1-4 defines the abbreviations used within this PP-Module.

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
ACPU	Application CPU
CA	Conditional Access (In DRM context) Client Application (in TEE context)
CC	Common Criteria
CPU	Central Processing Unit
DRAM	Dynamic Random Access Memory
DRM	Digital Rights Management
EAL	Evaluation Assurance Level
FLASH	Non-volatile, rewritable memory
GPU	Graphics Processor Unit
HDCP	High-bandwidth Digital Content Protection
HDMI	High Definition Multimedia Interface
HW	Hardware
LCD	Liquid-Crystal Display
NT-REE	Non-Trusted Regular Execution Environment
OEM	Original Equipment Manufacturer
PMM	Protected Media Manager
PP	Protection Profile
P-REE	Protected Regular Execution Environment
REE	Regular Execution Environment
RNG	Random Number Generator
SAR	Security Assurance Requirement
SMP	Secure Media Platform / Secure Media Path
SMS	Secure Media System
SoC	System-on-Chip
ST	Security Target
SW	Software
TA	Trusted Application
TEE	Trusted Execution Environment
TOE	Target Of Evaluation

Abbreviation / Notation	Meaning
UHD	Ultra High Definition
UI	User Interface
USB	Universal Serial Bus
WiFi	Wireless networking technology (IEEE 802.11x)

1.6 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 precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-5 lists the revision history for this PP-Module.

Table 1-5: Revision History

Date	Version	Description
Nov 2014 – March 2015	0.0.0.1 – 0.0.0.4	Initial and intermediate versions containing TOE definition, assets, security problem definition and security objectives
April 2015	0.0.0.5	Intermediate version for distribution to interested parties
May – Dec 2015	0.0.0.6 – 0.0.0.7	Intermediate version containing security requirements
Dec 2015	0.0.0.8	Complete version
January 2016	0.0.0.9	Integration of comments
	1.0.0.0	Version change for distribution to GlobalPlatform Premium Content Task Force No content change since January 2016
June 2017	1.0.0.1	Member Review
November 2017	0.0.0.2	Integration of Member Review feedback (Trustonic, Dolby) Addition of chapter 8 with requirements in CC language (incomplete) Version number update
November 2017	0.0.0.3	Minor changes following PCTF and TEE SW meetings in Vienna (Nov 8th 2017)
April 2018	0.0.0.4	Integration of GP review outcome (MovieLabs, Verimatrix) Minor update of some explanations and document structure

Date	Version	Description
March 2020	0.0.0.5	Template update Definition of SFRs using CC language Use of PP-Modules for Debug and Rollback protection Software update replaced by Application update Elimination of redundancy in objectives that were linked to the same CC SFRs Remark: chapter 6 is no longer needed (although some of the statements can be used to introduce the CC SFRs)
April 2020	0.0.0.6	Proof-reading and update wrt updated TEE PP (not certified yet) Candidate for Committee Review
TBD	TBD	Public Review
TBD	TBD	Public Release

2 Overview

2.1 SMP PP-Module identification

Title	Secure Media Path Protection Profile Module (SMP PP-Module)
Base PP	Trusted Execution Environment Protection Profile (TEE PP)
Base PP-Module	Time and Rollback PP-Module, and optionally Debug PP-Module
Editor	Internet of Trust
Date	April 2020
Version	0.0.0.6
Sponsor	ARM
CC Version	3.1 Revision 5

Note:

1. The TEE either does not implement debug interfaces or these are disabled in the end-user phase (also called production mode). Otherwise debug interfaces require the use of the Debug PP-Module.

2.2 SMP PP-Module overview

The SMP PP-Module has been designed for the evaluation and certification of TEE-enabled media devices that enforce market requirements for Enhanced Content protection.

The devices addressed by the SMP PP-Module include, but are not limited to, internet-connected systems such as smartphones, tablets and set-top boxes. These devices typically have the following characteristics:

- Implement a feature-rich user-facing operating system, which may have the capability to execute user-downloaded third-party applications, and to support online firmware updating;
- Can be used to access financial services in order to make payments for services including
  - playback authorization for downloaded media content and;
  - subscription to broadcast media services such as Pay TV;
- Can be used to play back premium media content, with video being displayed either on an attached screen, or on a remote display to which the system is connected either via wires or a wireless interface.

The SMP PP-Module supplements the GlobalPlatform TEE PP. The PP-Configuration obtained using the TEE PP and this SMP PP-Module together complies with MovieLabs Enhanced Content Protection [ECP] specification, excluding forensic video watermarking and Cinavia audio watermark detection. Watermarking features are optional and not covered by the requirements of the SMP PP-Module.

2.3 TOE overview

2.3.1 TOE type

The TOE type is the *Secure Media Platform* (SMP) for the protection of Enhanced Content.

The SMP is an execution environment for *Digital Rights Management* (DRM) and media content playback. It consists of:

- A TEE that provides the secure boot, the cryptographic functionality to protect the media content and the configuration of the media pipeline;
- A Protected Regular Execution Environment (P-REE), which handles compressed and decompressed plaintext media content.

The SMP cohabits with and is isolated from the *Non-Trusted Regular Execution Environment* (NT-REE) that typically consists of a general-purpose OS and user applications.

The P-REE implements the media content pipeline. It may optionally provide the capability to execute arbitrary code in a sandbox. This may be required in order to allow the NT-REE to customize or extend the functionality of the media content pipeline. For example, GPU shader programs may be generated at runtime by the NT-REE and then imported into the P-REE. Such usage of GPU shader is allowed. The sandbox functionality is part of the TOE, however the code that executes in the sandbox is not.

The TEE initializes the P-REE.

The *Secure Media System* (SMS) is the SMP plus any arbitrary code used to process the media content at a given time.

The TOE comprises:

- Any hardware, firmware and software used to provide the SMP security functionality;
- The guidance for the secure usage of the SMP after delivery.

The TOE does not comprise:

- The Trusted Applications running on top of the TEE;
- The arbitrary code executed by the P-REE;
- The NT-REE, which hosts the Client Applications that use the TEE.

In the following, TOE and SMP are used interchangeably.

Notes:

1. Although the TEE within the SMP is expected to implement GlobalPlatform specifications ([TEE Arch], [TEE Core API], [TEE Client API]), the SMP PP-Module does not require functional compliance with GlobalPlatform specifications.
2. The TEE can use different privilege levels for implementing different functionalities, e.g. DRM functionality could execute at a lower privilege level than the Trusted OS.
3. Output Control TA and specific output control protection technology such as HDCP is out of scope as DRM and CA are.

2.3.2 TOE usage

An SMP-enabled device may execute any of a wide variety of use cases involving protected media content. For example,

- The use case may involve consumption of live broadcast / multicast media, an on-demand stream, or a piece of pre-recorded content.
- The content may be either streamed to the system, or read from internal storage. The system may also permit content received via streaming to be stored locally for later consumption.
- Access to the content may be controlled via a Conditional Access (CA) system, or a DRM system.
- Protection may need to be applied to audio content, video content, or both.
- Once decrypted and decoded, the protected content may undergo processing on the device prior to rendering. For example, protected content may be
  - post-processed to improve perceived quality (e.g. color gamut remapping to the target display),
  - transformed for UI effects, for example a media gallery may be rendered as a carousel showing live clips from the video library,
  - geometrically transformed for immersive displays or virtual reality headsets,
  - mixed with non-protected content (e.g. to display UI overlays on top of protected video content; overlay video on live capture for augmented reality applications, or to mix system audio alerts with protected audio content).
- Rendering may be via local sinks (display and / or audio output); or the system may transmit the protected content to a remote sink (e.g. via an HDMI or WiFi link). Re-encryption may be necessary before the content leaves the SMS (depending on what local means, e.g. an accessible bus, re-encryption may be necessary for ‘local sinks’).

Note:

1. The requirements of DRM and CA are, for the purposes of this document, equivalent. “DRM” is used to mean “DRM or CA”.

2.3.3 TOE architecture

2.3.3.1 Relationship with TEE

The SMP PP-Module extends the TOE defined in the TEE PP by introducing the P-REE in the scope of evaluation. This means that:

- From the SMP perspective, the REE defined in TEE PP is split into P-REE and NT-REE.
- From the TEE perspective, the P-REE is part of the REE.

The TEE provides a hierarchy of trust built on two worlds:

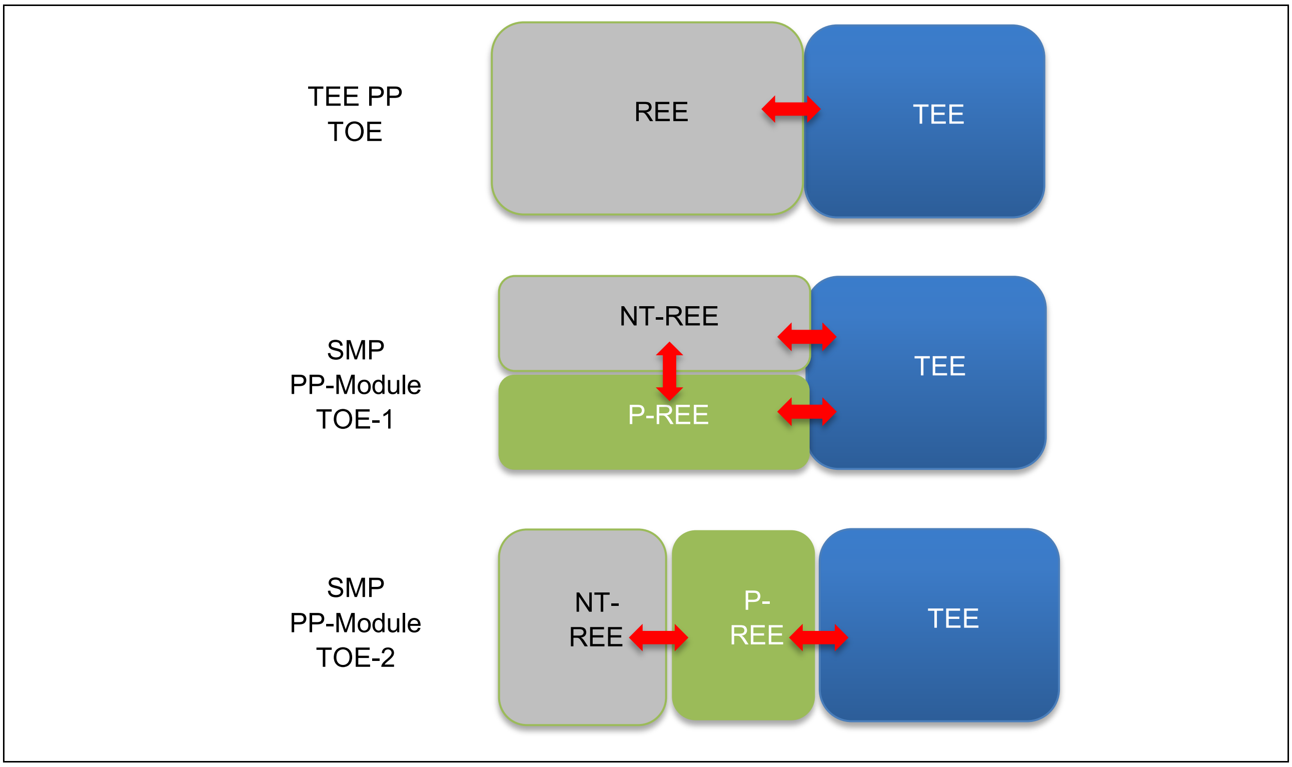
- (trusted) TEE < (non-trusted) REE.

The SMP refines this hierarchy by adding an intermediate world:

- (trusted) TEE < (protected) P-REE < (non-trusted) NT-REE.

The following figure is a simple representation of the TOEs in TEE PP and SMP PP-Module, where the TOEs are represented by blue and green boxes.

Figure 2-1: TOEs in TEE PP and SMP PP-Module



The SMP PP-Module addresses two kinds of TOE, which consists of TEE and P-REE:

- TOE-1: There exist direct communication means between the TEE, P-REE, and NT-REE.
- TOE-2: The P-REE provides the channel for the communication between the TEE and NT-REE.

2.3.3.2 Components and properties

A typical device for media content applications:

- Uses a SoC based on one or more *Application Central Processing Unit* (ACPU);
- Integrates one or more DRAM controllers;
- Has access to non-volatile storage (e.g. FLASH and / or hard drive);
- Implements a hardware or software audio decoder;
- Implements a hardware or software video decoder;
- Implements for instance
  - a dedicated HDMI transceiver with an HDCP encryption engine; or
  - a wireless display transceiver with an HDCP encryption engine.

Note:

1. The output list is informative:
   a. The player device could be inside a TV with another mechanism to ensure that decrypted content is not accessible (local sink).
   b. It is possible that other HW-based baseband video security systems will be developed for connecting player devices to displays.

2. The device may implement other interfaces, which are not related to media playback, for instance USB and user data entry. Such interfaces are part of the TOE but the SMP PP-Module does not introduce any requirement on their implementation.

The TOE architecture may vary from one device to another. The SMP PP-Module does not mandate any concrete HW or SW architecture but provides an abstract view of the TOE components, describes their roles and gives examples of realisations. Different SMP-compliant TOEs may use TEE and P-REE in different ways. However, there is a constant in the SMP architecture, namely that TEE provides the cryptographic functionality related to the media content protection and protects the cryptographic material from the REE and other TAs while the P-REE implements the plaintext media content pipeline.

The TOE components are of two kinds: *Resources* and *Functions*. Resources are mapped to on-chip/off-chip memory locations and store the assets such as the root(s) of trust, the different formats of media content, the code and the system state information. Functions are active entities that perform the media content playback and the management and control operations that support the protection of the media content pipeline. The Functions access the Resources to achieve their behavior.

The Functions can be implemented in HW, SW or a mix of both, for instance:

- Software executing on the ACPU, from on-chip memory or DRAM;
- Pure hardware component outside the ACPU;
- Component outside the ACPU that executes firmware, from on-chip memory or DRAM.

The protection of the media content pipeline is enforced by a P-REE hardware-filtering Function that controls access to the Resources and ensures the isolation of the P-REE from the NT-REE. The filtering relies on:

- a property of the access transaction which uniquely determines the Function that initiated the transaction – this is referred to as the *identifier;*
- the target Resource;
- the requested operation, for example, Read or Write.

The hardware-filtering Function may be runtime-programmable. The assignment of identifiers to Functions may either be fixed in hardware, or programmable.

Note:

1. A set of Functions may hold the same identifier provided there is no isolation requirement between them.

Table 2-1 shows the characteristics of Resources and Functions.

Table 2-1: SMS Resources and Functions

	Characteristics	Meaning
Resource	Trusted/Protected/Non-Trusted	Trusted Resources contain SMP assets belonging to the TEE (e.g. roots of trust, unique identifiers, keys and certificates, playback map). Protected Resources contain SMP assets belonging to the P-REE (e.g. compressed and decompressed plaintext media content). Non-Trusted Resources do not contain SMP assets.
	Interface	Non-Trusted Resource shared between SMP and NT-REE (e.g. communication buffers, registers or more generally any memory mapped entities which are used for communication purposes).
	Code	Resource that contains executable data.
Functions	SMS/Non-SMS (at a given time)	Functions within the SMS are used to deliver the protected content. Functions outside the SMS do not contribute to the delivery of the protected content. An SMS Function can be an SMP Function or a Non-SMP Function.
	SMP(Authenticated)/Non-SMP(Non-Authenticated)	SMP Functions can reside in the TEE or in the P-REE. SMP Functions are in the scope of the SMP evaluation. Non-SMP Functions belonging to the SMS stand for arbitrary code out of the scope of the SMP evaluation (e.g. usage of GPU shader programs generated at runtime by NT-REE is allowed).
	Control/Data	Control Functions are used for communication between execution environments through Interface Resources. Data Functions execute within one environment and cannot access Interface Resources.

The SMP design guarantees that the SMP is initialized through a secure boot process, which initializes the TEE first and then the P-REE. This process results in a well-defined system state in which the SMP assets belong either to the TEE or to the P-REE, i.e. they are stored in Trusted or Protected Resources:

- Roots of trust, keys and certificates belong to the TEE;
- Code that operates on SMP keys and certificates belongs to the TEE;
- Code that operates on plaintext media content belongs to the P-REE.

Most of the TEE Functions are described in the TEE PP: they provide trusted storage and cryptographic operations to the DRM TA, means to communicate with the REE (P-REE/NT-REE) as well as isolation mechanisms enforcing the sandboxing of the DRM TA, other TAs and the TEE itself. Isolation of the TEE and TAs from the REE can be hardware-enforced.

TEE Debug features are optional.

This SMP PP-Module introduces an application management functionality, controlled by the TEE.

Application Note: Indeed, the TEE must allow the update of the DRM application. Although the TEE may allow the update of TEE and/or P-REE firmware and software components, such functionality is out of the scope of this SMP PP-Module.

There is one fixed special Function called the *Protected Media Manager* (PMM) that resides within the TEE.

P-REE Functions (for instance, the video and audio decoders, the output management) may be:

- fixed such that they always exist inside the SMS, or
- moved into / out of the SMS at runtime.

The PMM manages the transitions of P-REE Functions into / out of the SMS:

- For instance, a video decoder engine may be used outside the SMS for playback of non-protected content or inside the SMS for playback of protected content.

While a Function is in the SMS, it may receive and respond to communication from the NT-REE:

- For example, when the video decoder is inside SMS, it may receive from the NT-REE “Fill this buffer”/”Empty this buffer” commands.

The SMP policy, enforced by the TEE and the P-REE, controls the access to Trusted, Protected and Interface Resources. The GPU can be a Protected Resource.

The TEE controls the access to the Trusted Resources: access to Trusted Resources is granted to Trusted (TEE) Functions only.

The P-REE policy specifies the following rules:

1. Non-SMS Functions cannot read from Protected Resources;
2. SMS Functions cannot write P-REE assets into Non-Trusted Non-Interface Resources;
3. Non-SMP Functions within SMS, which means arbitrary code, do not have write access to Interface Resources;
4. SMP Functions cannot write P-REE assets into Interface Resources.

Rules 1, 2 and 3 are enforced by hardware memory filter(s). Rule 4 has to be checked during SMP evaluation:

- For instance, to satisfy rule 2, a video decoder processing protected content must be constrained to prevent writing into any memory location that could be accessed by the NT-REE.

Within the P-REE, the Functions that operate on the compressed and decompressed forms of the plaintext media content may be isolated from one another. The interest of such isolation is that the compressed content is considered more valuable than the decompressed form: in order to practically redistribute the content, an attacker would need to have access to the compressed form; by stealing and then recompressing the decompressed content, quality may be lost.

The TEE may optionally provide debug functionality.

Note:

1. Security Targets conformant to the SMP PP-Module shall provide a description of how they implement the architecture defined above, including the SMP initialisation process and the isolation and debug mechanisms.

2.3.4 Available Non-TOE hardware/software/firmware

The TOE may require some non-TOE hardware, software or firmware components in order to operate. However, the TOE must be realized in such a way that TOE security functionalities do not rely on the proper behavior of non-TOE hardware, software or firmware.

Note:

1. For example, a Protected accelerator firmware may be loaded from FLASH by the NT-REE, then loaded to the relevant component and authenticated under TEE control. The FLASH storage and the

NT-REE software are outside the TOE. Without these components, the Protected accelerator firmware cannot be loaded. However, even if these components misbehave, they must not be allowed to subvert the TOE security functionality, which in this example include the authentication and load processes.

2. Security Targets conformant to the SMP PP-Module shall complete the descriptions of the available non-TOE hardware/software/firmware with the list of non-TOE Resources used by the TOE.

It is accepted that if the non-TOE is misbehaving, then the target meets its security functionalities by the withdrawal of services and functionality.

2.3.5 TOE security functionality

SMP devices host multiple execution environments, with access to sensitive data granted to trusted and protected environments (TEE and P-REE) only. Untrusted environments (NT-REE) are granted limited capabilities, such that untrusted software is unable to affect the protected media pipeline functionality or to access any SMP asset.

The SMP provides the TEE security functionality stated in the TEE PP and additional security functionality stated in the SMP PP-Module that is implemented either in the TEE or in the P-REE.

2.3.5.1 SMP TEE security functionality

The TEE protects highly valuable assets that have a relatively small footprint both at rest and at runtime, such as roots of trust, system identity and media licenses and cryptographic keys used to protect media data.

The TEE is in charge of the initialisation of the SMP and performs all the cryptographic operations on media content. The TEE starts the P-REE but the initialisation of the P-REE media pipeline Functions can be completed within the TEE or the P-REE.

The TEE provides application management functionality, including update.

The TEE provides the PMM Function.

The TEE provides full rollback protection of assets including TEE firmware, TEE persistent data, TA code and data and TA Trusted Storage.

Either debug functionality is disabled in production mode or the TEE provides controlled access to debug capabilities of the TEE itself, the DRM TA and the P-REE.

Note:

1. The TEE allows to mutually isolate content management (DRM) systems from different vendors by using different Trusted Applications (TA). This aspect is not developed further in the document; the TEE PP states all the properties of the TA from a platform perspective.
2. Unlike the TEE PP, this SMP PP-Module requires full rollback protection. Note that such protection can be achieved by integrating the Time and Rollback PP-Module.
3. The TEE debug functionality is also optional in the TEE PP. In the SMP PP-Module, the Digital Rights Manager assets are not accessible to the debug functionalities.

2.3.5.2 SMP P-REE security functionality

The P-REE, which performs the media playback, provides runtime protection of assets that may have a large footprint, for instance plaintext forms of protected media data. The compromise of such assets would have a less detrimental impact than the compromise of TEE assets.

If arbitrary code is permitted in the media pipeline, the P-REE ensures that it is executed in a sandbox, and grants Functions executing arbitrary code limited access rights to protected Resources. These access rights are enforced by hardware filters which are under the control of the P-REE.

The P-REE has no access to any asset belonging to the TEE.

The P-REE may be granted access to selected data belonging to the NT-REE.

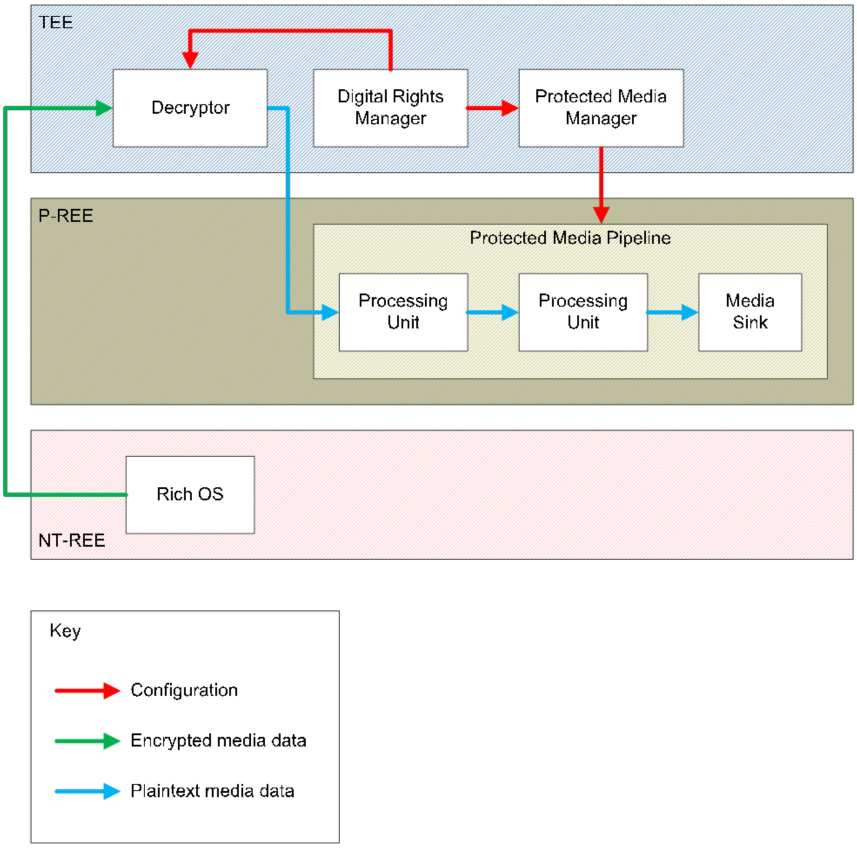
The P-REE provides an interface with the NT-REE.

2.3.6 Example system architecture

Figure 2-2 illustrates a possible architecture. The components that make up the SMS are as follows:

- TEE
    - The firmware which initializes the system upon boot and which manages ACPU switching between Secure and Non-secure states;
    - Optionally, a Trusted OS executing in the ACPU Secure state;
    - A DRM component (Trusted Application) which grants authorization to play protected media content. If the system supports multiple content protection schemes, separate Digital Rights Managers may implement each of them;
    - A PMM, responsible for configuring all agents in the system which process protected media content;
    - A Decryptor, which converts encrypted protected media content to its compressed plaintext form.
- P-REE
    - Processing Units such as video decoders, mixers and post-processors;
    - Memory filters;
    - One or more Media Sinks which render protected media data. These may include on-board components such as display panels and loudspeakers, or controllers such as HDMI, which transmit media content to be rendered remotely.

Figure 2-2: Example System Architecture



2.3.6.1 Video playback use case

This section describes an example of a simple protected video playback pipeline where:

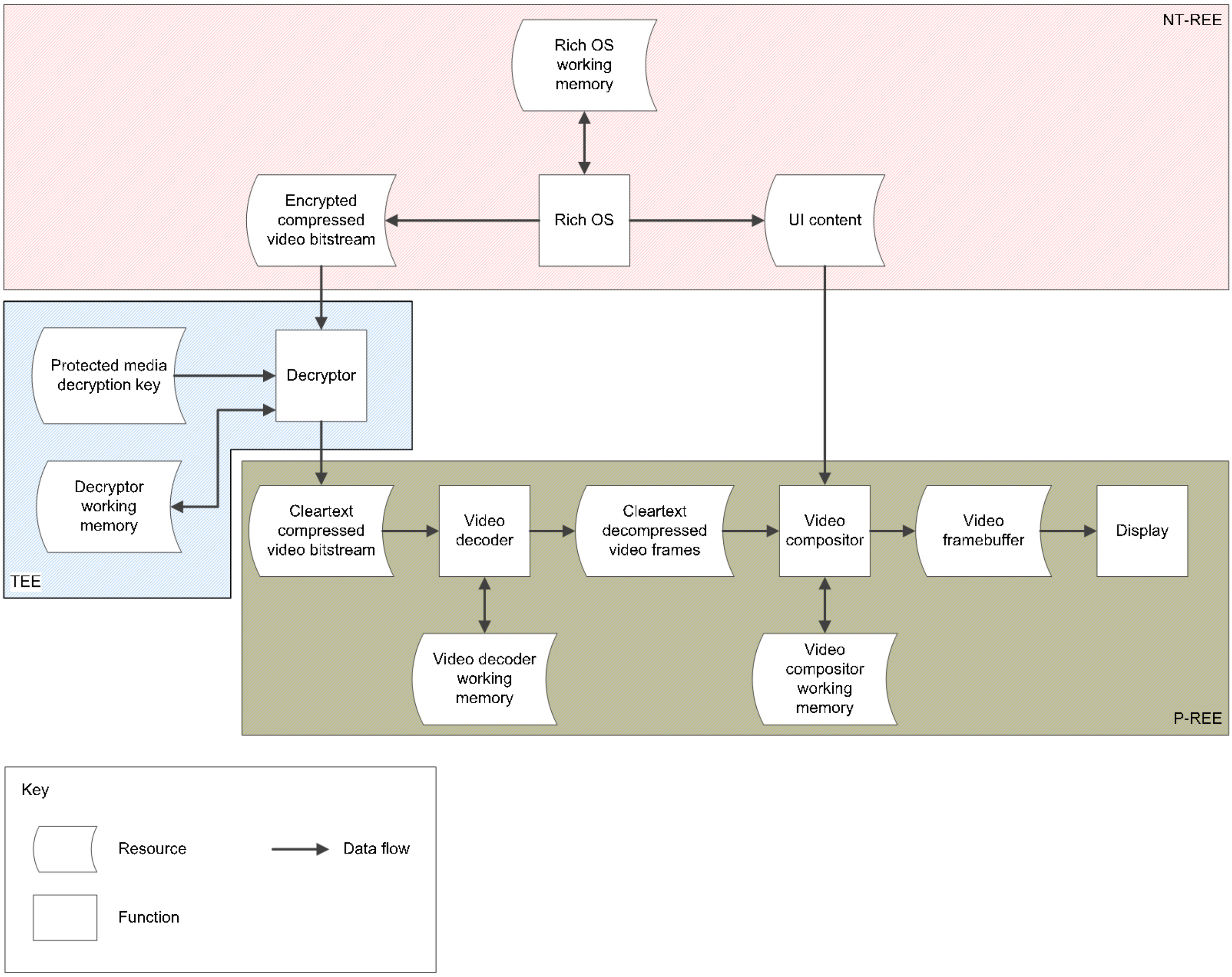
- DRM-protected content is stored encrypted on the local file system;
- Only video content is protected; the audio track(s) are not protected;
- UI overlay is composed with protected video content;
- Rendering is performed on a local display.

Figure 2-3 shows the data and Functions mapped into the device's components:

- The encrypted content is initially read from the file system by the NT-REE;
- Decryption of the protected video content occurs in the TEE. Any processing necessary to obtain the decryption key is also performed under TEE control. This may for example require a secure transaction with the content owner, via which a payment is made and a content key is returned to the client;
- The cleartext bitstream is passed from the TEE to the P-REE, where it is first decompressed, then mixed with the non-protected UI overlay, and finally sent to the local display for rendering.

All Functions that have access to the plaintext video data reside in the P-REE. By contrast, the Functions which control the protected media pipeline – for example sequencing the buffer flow, and providing parameters which describe where on the screen the video should appear – can operate without requiring access to the video data itself, and therefore can reside in the NT-REE.

Figure 2-3: Example Video Playback Use Case


NT-REE
Rich OS working memory
Encrypted compressed video bitstream
Rich OS
UI content
Protected media decryption key
Decryptor
Decryptor working memory
TEE
Cleartext compressed video bitstream
Video decoder
Cleartext decompressed video frames
Video compositor
Video framebuffer
Display
Video decoder working memory
Video compositor working memory
P-REE
Key
Resource
Data flow
Function

2.3.7 Reference Device Life Cycle

The reference device life cycle defined in the TEE PP applies to the SMP platform.

3 Conformance Claims

3.1 CC Conformance Claims

The SMP PP-Module is CC Part 2 [CC2] conformant.

3.2 Conformance Claim to a Package

The SMP PP-Module inherits the minimum assurance level defined in the TEE PP.

3.3 Conformance Claim to the PP-Module

The SMP PP-Module inherits from TEE PP the strict conformance as defined in [CC1] for all Security Targets and Protection Profiles claiming conformance to it.

3.4 Consistency rationale

The consistency rationale with the TEE PP is given along with the definition of the SMP elements (security problem, objectives and requirements).

4 Security Problem Definition

4.1 Assets

The assets of the SMP PP-Module are of two kinds: media assets belonging to the owner of the media content, and platform assets that are used to protect the media assets. These assets are stored in Trusted and/or Protected Resources and accessed by Functions under TEE or P-REE control, or they are stored in Non-Trusted Resources under control of TEE Trusted Storage functionality.

Section 4.1.1 presents a summary of the assets and their security properties. Sections 4.1.2 and 4.1.3 provide the definition of the assets that are added to the TEE PP or PP-Modules.

Note:

1. In the following, “Internal memory” means SoC-memory or any component memory protected at the same level.

4.1.1 Overview of SMP assets

Table 4-1 provides the list of SMP assets and the security properties that must be enforced on them. It shows the SMP assets defined in the TEE PP and the applicable PP-Modules, and, in red, the assets that are introduced or refined in this SMP PP-Module. Notice that the new assets are under the control of either the TEE or the P-REE.

For completeness all the assets defined in the TEE PP and the applicable PP-Modules are listed.

Table 4-1: SMP Assets

SMP Assets	Security properties	TEE PP and PP-Modules assets	SMP PP-Module new or refined assets	
		Under TEE control	Under TEE control	Under P-REE control
SMP Platform Assets				
TEE Storage Root of Trust (S-ROT) *(Defined in TEE PP)*	Integrity Confidentiality	✓		
TEE Identification *(Defined in TEE PP)*	Unique Non-modifiable	✓		
TEE Initialisation Code and Data *(Defined in TEE PP)*	Integrity	✓		
TEE Firmware *(Defined in TEE PP)*	Authenticity Integrity	✓		
TEE Runtime Data *(Defined in TEE PP)*	Integrity Confidentiality	✓		
TEE Persistent Data *(Defined in TEE PP)*	Authenticity Integrity Confidentiality Device binding	✓		
Random Number Generator (RNG) *(Defined in TEE PP)*	Unpredictability Sufficient entropy	✓		
TA Instance Time *(Defined in TEE PP)*	Monotonicity	✓		
TA Persistent Time *(Defined in Time & Rollback PP-Module)*	Monotonicity	✓		

SMP Assets	Security properties	TEE PP and PP-Modules assets	SMP PP-Module new or refined assets	
		Under TEE control	Under TEE control	Under P-REE control
TEE Rollback Detection Data[1] *(Defined in Time & Rollback PP-Module)*	Integrity	✓		
(Optional) TEE Debug Authentication Keys[2] *(Defined in Debug PP-Module)*	Integrity Confidentiality	✓		
TEE Platform Root of Trust (P-ROT) *(Defined below)*	Non-modifiable Confidentiality		✓	
P-REE Initialisation Code and Data *(Defined below)*	Integrity		✓	
P-REE Firmware *(Defined below)*	Integrity Authenticity		✓	✓
P-REE Runtime Data *(Defined below)*	Integrity Confidentiality			✓
SMP Application Management Data *(Defined below)*	Integrity Confidentiality		✓	

SMP Assets	Security properties	Core TEE PP assets	SMP PP-Module new assets	
		Under TEE control	Under TEE control	Under P-REE control
SMP Media Assets				
Digital Rights Manager *(Defined in TEE PP and Time & Rollback PP-Module, refined below)*	Authenticity Integrity	✓		
Media Keys and Certificates *(Defined in TEE PP and Time & Rollback PP-Module, refined below; it includes the assets below)*	Integrity Confidentiality	✓		
DRM Scheme Public Keys	Integrity Non-modifiable	✓		
Player Certificates	Integrity	✓		
Player Private Keys	Integrity Non-modifiable Confidentiality	✓		
Playback Map	Integrity Confidentiality	✓		
(optional) Output Protection Keys	Integrity Confidentiality	✓		
Compressed Plaintext Media Content *(Defined below)*	Confidentiality			✓

[1] The TEE data that is used to detect rollback of previous versions of TEE firmware and persistent data and Digital Rights Manager code, data, and keys.

[2] The cryptographic keys used to authenticate the Debug Administrator prior to granting access to debug functionality (TEE and P-REE). Here the requirements associated with the debug functionalities will be reinforced regarding the inaccessibility of Digital Rights Manager assets. As in the TEE PP, either the TEE debug functionality is disabled or authentication is mandatory.

SMP Assets	Security properties	Core TEE PP assets	SMP PP-Module new assets	
		Under TEE control	Under TEE control	Under P-REE control
Decompressed Plaintext Media Content *(Defined below)*	Confidentiality			✓

Application Note:

- *The Security Target shall specify the cryptographic strength of S-ROT and P-ROT, which should meet the requirements of the target DRM scheme(s);*
- *The PMM is part of the TEE Firmware.*

4.1.2 SMP platform assets

The SMP contains the following platform assets on top of the assets defined in the Core TEE PP, which are not reproduced here (see TEE PP).

TEE Platform Root of Trust (P-ROT)

The root of trust that is used to perform software authentication during secure boot or application update. This data is either a secret symmetric key or a public key.

Application Note:

- *For instance, immutability can be achieved by hardware means, e.g. using write-once memory such as OTP or ROM. Confidentiality can be ensured by the fact that the asset remains inside the SoC part of the TEE.*
- *This asset could be seen as part of the TEE Persistent Data in the TEE PP. It is introduced in this SMP PP-Module for two reasons: there is no immutability requirement on the TEE Persistent Data and the TEE PP does not address application update, which is the reason for introducing the P-ROT asset.*

P-REE Initialisation Code and Data

Initialisation code and data used at any stage from device power-on up to the complete activation of the P-REE initial secure state. The data includes P-REE software keys, certificates or signatures required for the authentication of the P-REE firmware before loading.

P-REE Firmware

The firmware and the static data that are part of the media path. This includes firmware that executes on an accelerator with the single purpose of transforming decompressed plaintext media content for composition and/or rendering.

Application Note:

- *Accelerators note: Firmware that executes on an accelerator for the single purpose of transforming decompressed plaintext video content is not evaluated and not authenticated. It executes in a sandbox, isolated from P-REE firmware and data. The P-REE ensures that such accelerators' firmware does not leak media content.*
- *The integrity of P-REE firmware must be checked during boot/loading and could be checked on demand (implementation choice).*

P-REE Runtime Data

The runtime data generated and used during the execution of P-REE firmware. This data is stored in volatile memory (RAM, DRAM).

Application Note: The integrity and confidentiality of P-REE runtime data is necessary to prevent the leakage of video buffers contents. The (de)compressed plaintext media content is a separate confidential asset.

SMP Application Management Data

The keys and certificates used for the realization of the application management operations.

Application Note: The ST author shall define the precise set of keys and certificates used for the application management operations.

4.1.3 SMP media assets

The SMP contains the following media assets, which are instantiations of the TA assets defined in the Time and Rollback PP-Module holding “integrity” security properties[3].

Digital Rights Manager (DRM)

The code of the CA/DRM application installed in the SMP platform and running under TEE control.

Application Note:

- *The DRM is a Trusted Application. This asset corresponds to “TA code_module” defined in the TEE Time and Rollback PP-Module.*
- *The DRM application manages the handshake protocol between the client device and the remote DRM sever and the results of the verification processes. It executes in (internal) integrity protected memory under TEE control. The TEE shall process the application’s session keys in internal confidential memory.*
- *The DRM code is typically stored in external non-volatile memory that is accessible from the NT-REE.*

Media Keys and Certificates

The keys and certificates necessary for decrypting the media content. It includes:

- DRM Scheme Public Keys: The RSA public key originating from a trusted authority and stored at manufacture. This is the root of trust of the DRM handshake protocol.
- Player Certificates: The certificates for the device signed by authorities trusted by the content owner.
- Player Private Keys: The private keys of the player stored at manufacture or via secure key provisioning. They are stored in internal confidentiality protected non-volatile memory.
- Playback Map: Data structure containing the keys and other information derived from the protocols necessary to decrypt the media content;
- (Optional) Output Protection Keys: The keys to enforce output protection control to local or remote sinks.

[3] In the TEE PP, the TA assets hold authenticity and consistency security properties, not integrity.

Application Note:

- *The Media Keys and Certificates are DRM assets that should meet the target DRM scheme requirements. The Security Target shall provide the characteristics of such material, including their life cycle. Note that some DRM schemes may require to store such material in the manufacturing phase.*
- *This asset corresponds to “TA data and keys_module” in TEE Time and Rollback PP-Module.*
- *Immutability of DRM Scheme Public Keys can be achieved by hardware means e.g. using write-once memory such as OTP or ROM.*
- *There is no rollback protection required for player certificates since rollback would simply cause the license file to stop working. This means integrity is not strictly necessary. However, the Media Keys and Certificates assets are seen as a whole in this SMP PP-Module, hence the rollback detection mechanism that enforces the memory integrity applies to the player certificates too.*
- *The Resources holding the playback map shall be overwritten or zeroed out once the player is stopped or exited.*
- *The decryption keys for the audio path must be independent from the decryption keys for the video path.*

Compressed Plaintext Media Content

The media content decrypted by the TEE and processed by the P-REE in compressed format.

This asset is stored in memory which is internal to the device, but which may reside off-SoC.

Application Note:

- *The P-REE shall protect the confidentiality of this asset from the NT-REE and from composition or rendering Functions.*
- *The SMP access policy will grant access to this asset to the video decoder not to composition or rendering Functions. The video decoder is a Function within the scope of evaluation. The evaluation must check that the video decoder does not simply copy the compressed content to the composition and rendering Functions.*

Decompressed Plaintext Media Content

The plaintext media content, which has been decompressed by the P-REE and is rendered through video/audio devices.

This asset is stored in memory which is internal to the device, but which may reside off-SoC.

Application Note:

- *The P-REE shall protect the confidentiality of this asset from the NT-REE.*
- *Two cases arise: 1) local display rendering (e.g. no HDCP) and 2) external device rendering (e.g. via HDCP). In case 2, SMP must provide re-encryption functionality, e.g. the Output Control TA running in the TEE needs to communicate with the DRM and must provide the required level of control compliant with the Output Control technology, e.g. HDCP, which requires checking the state, controlling version number (HDCP 2.2) and setting appropriate configuration (Type 1 Flag).*

4.2 Users and subjects

The users of the TOE (SMP) are

- the Trusted Applications and the NT-REE.
- (optional) The TEE Debug Administrator if the TEE implements debug functionality.

The subjects of the SMP are the Functions within the SMS.

4.3 Threats

The threat model defined in the TEE PP applies to the SMP PP-Module. The threats defined in the TEE PP that target the SMP assets are all relevant and there are new threats directed to the P-REE assets and to the new TEE assets.

Section 4.3.1 presents a summary of all the threats and the impacted assets. Section 4.3.2 provides the definition of the threats that are added to the TEE PP.

Note:

1. The threat T.TA_PERSISTENT_TIME_ROLLBACK defined in [TEE PP-T] is not in the scope of the SMP PP-Module since the persistent time functionality does not belong to the TOE. Nevertheless, it is possible to address it in any SMP evaluation: the introduction of this threat and the corresponding asset "TA Persistent Time" does not lead to contradiction.

4.3.1 Overview of SMP threats

Table 4-2 shows the direct threats to the SMP assets. Most of the threats may indirectly impact other assets.

The SMP assets defined or refined in this PP-Module are written in red in the table. They reside either in the TEE or in P-REE (defined in the second and third columns).

The threats defined in the TEE PP apply to all the SMP assets that are managed by the TEE. In the context of the SMP PP-Module, this means that there are threats that extend their scope to the new (red) assets, which are linked to the additional functionalities of the TEE[4].

The threats written in black are defined in the TEE PP or applicable PP-Modules; the threats written in red are introduced in the SMP PP-Module.

For completeness all the assets defined in the TEE PP and the applicable PP-Modules are listed.

[4] For instance, T.ABUSE_DEBUG extends to P-REE Runtime Data.

Table 4-2: SMP Assets and Threats Relationship

SMP Assets / Threats	In TEE	In P-REE	T.ABUSE_FUNC	T.CLONE	T.FLASH_DUMP	T.IMPERSONATION	T.ROGUE_CODE_EXECUTION	T.PERTURBATION	T.RAM	T.RNG	T.SPY	T.TEE_FIRMWARE_DOWNGRADE	T.STORAGE_CORRUPTION	T.ABUSE_DEBUG	T.ROLLBACK	T.TA_PERSISTENT_TIME_ROLLBACK	T.P-REE_ABUSE_FUNC	T.P-REE_ROGUE_CODE_EXECUTION	T.P-REE_MODIFICATION	T.P-REE_DISCLOSURE	T.P-REE_FIRMWARE_DOWNGRADE	T.P-REE_STORAGE_CORRUPTION
SMP platform assets																						
TEE Storage Root of Trust (S-ROT)	x			x				x	x		x		x									
TEE Identification	x			x																		
TEE Initialisation Code and Data	x		x	x				x	x					x								
TEE Firmware	x											x	x									
TEE Runtime Data	x		x			x	x	x	x	x	x			x								
TEE Persistent Data	x			x	x						x		x		x							
Random Number Generator (RNG)	x		x			x	x	x	x	x				x								
TA Instance Time	x							x					x									
TA Persistent Time	x															x						
TEE Rollback Detection Data	x			x																		
(Optional) TEE Debug Authentication Keys	x			x	x																	
TEE Platform Root of Trust (P-ROT)	x			x	x			x	x		x	x	x									
P-REE Initialisation Code and Data	x		x	x				x	x					x	x							
P-REE Firmware		x																	x		x	x
P-REE Runtime data		x												x			x	x	x	x		
SMP Application Management Data	x			x	x						x		x									
SMP media assets																						
Digital Rights Manager	x		x										x	x	x							
Media Keys and Certificates	x			x	x				x	x	x		x	x	x							
Compressed Plaintext Media Content		x																x		x		
Decompressed Plaintext Media Content		x																x		x		

4.3.2 Threats to P-REE assets

The SMP PP-Module contains the following threats in addition to those defined in the TEE PP. The threats defined in the TEE PP are not reproduced here.

T.P-REE_ABUSE_FUNCT

An attacker accesses P-REE functionalities outside of their expected availability range.

An attacker manages to instantiate an illegal P-REE or to start-up the P-REE in an insecure state or to enter an insecure state, allowing the attacker to obtain sensitive data or compromise the TSF (bypass, deactivate or change security services).

Assets threatened directly: P-REE Runtime Data (confidentiality, integrity).

T.P-REE_ROGUE_CODE_EXECUTION

An attacker imports malicious code into the P-REE, for instance into media pipeline accelerators, to disclose or modify sensitive data.

Assets threatened directly: P-REE Runtime data (confidentiality, integrity), Compressed and Decompressed Plaintext Media Content (confidentiality).

T.P-REE_DISCLOSURE

An attacker discloses confidential media content by means of runtime read attacks to the volatile Resources used by the P-REE, e.g. the RAM, the memory buses or the video buffers.

Assets threatened directly: P-REE Runtime data and Compressed and Decompressed Plaintext Media Content (confidentiality).

Application Note:

- *When the NT-REE and the P-REE share memory, an attack path consists in the (partial) memory dump by the NT-REE.*

T.P-REE_MODIFICATION

An attacker modifies (the behavior of) the P-REE in order to gain unauthorized access to media content or to force the execution of unauthorized Functions.

Assets threatened directly: P-REE Firmware and Runtime Data (integrity).

T.P-REE_FIRMWARE_DOWNGRADE

An attacker backs up part of or all the P-REE firmware and restores it later in order to use obsolete P-REE functionalities.

Assets threatened directly: P-REE Firmware (integrity).

Application Note: This threat concerns the TEE as well, which is responsible for detecting P-REE firmware downgrade.

T.P-REE_STORAGE_CORRUPTION

An attacker corrupts the non-volatile memory that stores the P-REE firmware. The goal is to trigger misbehavior of the storage security mechanisms that would allow compromising the media pipeline and disclosing plaintext media content.

Assets threatened directly: P-REE Firmware (integrity).

Application Note: The attack can rely, for instance, on the NT-REE file system or the Flash driver.

4.4 Organisational security policies

The two organisational security policies defined in TEE PP apply to the SMP PP-Module:

- OSP.INTEGRATION_CONFIGURATION;
- OSP.SECRETS.

The SMP PP-Module introduces the following additional OSP:

OSP.P-REE_INTEGRATION_CONFIGURATION

Integration and configuration of the P-REE by the device manufacturer shall rely on guidelines defined by the SMP provider, which state all the P-REE related security requirements for the device manufacturer issued from the SMP evaluation.

4.5 Assumptions

The assumptions A.PROTECTION_AFTER_DELIVERY, A.TA_MANAGEMENT and A.TA_DEVELOPMENT defined in the TEE PP apply to the SMP PP-Module.

The SMP PP-Module adds the following assumptions:

A.SMP_DRM_DEVELOPMENT

The DRM application is assumed to:

- use the cryptographic key management and operations provided by the TEE to implement all the cryptographic DRM functionality, including handshake protocols and content decryption;
- delete the Playback Map when playback is finished, i.e. when the user stops playback by hitting the stop button or the player application is exited. Deletion means removing the information by overwriting it with all zeroes or by overwriting it with random or unrelated data.

A.P-REE_PROTECTION_AFTER_DELIVERY

It is assumed that the environment protects the TOE (SMP) after delivery and before entering the final usage phase. It is assumed that the persons manipulating the TOE in the operational environment apply the P-REE guidelines (e.g. user and administrator guidance, installation documentation, personalisation guide). It is also assumed that the persons responsible for the application of the procedures contained in the guides, and the persons involved in delivery and protection of the product have the required skills and are aware of the security issues.

Application Note: The certificate is valid only when the guidelines are applied. For instance, for installation, pre-personalisation or personalisation guides, the certificate covers the described set-up configurations or personalisation profiles only.

5 Security Objectives

The security objectives contain the objectives for the TOE, i.e. the SMP, and the objectives for the TOE operational environment, defined in sections 5.2 and 5.4, respectively.

Section 5.1 presents an overview of all the objectives and the coverage of the threats.

5.1 Overview of SMP objectives

5.1.1 Coverage of threats

Table 5-1 lists the SMP security objectives. The objectives written in black come from the TEE PP; they apply to the SMP assets that are managed by the TEE and either counter or mitigate the threats to such assets. The objectives written in red are defined in the SMP PP-Module.

Application Note: O.INSTANCE_TIME from TEE PP is included for completeness although it does not play a role in the SMP.

Table 5-1: SMP Objectives and Threats Coverage

SMP Objectives / Threats	Applies to TEE	Applies to P-REE	T.ABUSE_FUNC	T.CLONE	T.FLASH_DUMP	T.IMPERSONATION	T.ROGUE_CODE_EXECUTION	T.PERTURBATION	T.RAM	T.RNG	T.SPY	T.TEE_FIRMWARE_DOWNGRADE	T.STORAGE_CORRUPTION	T.TA_PERSISTENT_TIME_ROLLBACK	T. ROLLBACK	T.ABUSE_DEBUG	T.P-REE_ABUSE_FUNC	T.P-REE_ROGUE_CODE_EXECUTION	T.P-REE_MODIFICATION	T.P-REE_DISCLOSURE	T.P-REE_FIRMWARE_DOWNGRADE	T.P-REE_STORAGE_CORRUPTION
O.CA_TA_IDENTIFICATION	x					x																
O.KEYS_USAGE	x		x																			
O.TEE_ID	x			x																		
O.INITIALISATION	x		x	x			x	x	x	x		x	x				x	x	x	x	x	x
O.INSTANCE_TIME	x							x														
O.OPERATION	x		x			x	x	x					x									
O.RNG	x			x						x												
O.RUNTIME_CONFIDENTIALITY	x		x	x			x	x	x	x	x											
O.RUNTIME_INTEGRITY	x		x	x		x	x	x	x	x												
O.TA_AUTHENTICITY	x		x				x	x					x									
O.TA_ISOLATION	x							x	x		x											
O.TEE_DATA_PROTECTION	x		x	x			x	x					x									

SMP Objectives / Threats	Applies to TEE	Applies to P-REE	T.ABUSE_FUNC	T.CLONE	T.FLASH_DUMP	T.IMPERSONATION	T.ROGUE_CODE_EXECUTION	T.PERTURBATION	T.RAM	T.RNG	T.SPY	T.TEE_FIRMWARE_DOWNGRADE	T.STORAGE_CORRUPTION	T.TA_PERSISTENT_TIME_ROLLBACK	T. ROLLBACK	T.ABUSE_DEBUG	T.P-REE_ABUSE_FUNC	T.P-REE_ROGUE_CODE_EXECUTION	T.P-REE_MODIFICATION	T.P-REE_DISCLOSURE	T.P-REE_FIRMWARE_DOWNGRADE	T.P-REE_STORAGE_CORRUPTION
O.TEE_ISOLATION	x		x					x	x		x											
O.TRUSTED_STORAGE	x			x	x		x				x		x									
O.ROLLBACK_PROTECTION[5]	x														x							
O.TA_PERSISTENT_TIME								x						x								
O.SMP_TEE_INITIALISATION	x	x					x		x		x						x	x	x	x	x	x
O.P-REE_OPERATION		x															x	x	x			x
O.P-REE_ RUNTIME_CONFIDENTIALITY		x															x	x		x		
(Optional) O.P-REE_FUNCTION_ ISOLATION		x															x		x	x		
O.SMP_TEE_PMM	x																x	x	x	x		
O.SMP_TEE_DRM_CRYPTO	x								x		x											
O.SMP_TEE_ZEROIZATION	x								x		x											
O.SMP_TEE_APPLICATION_MGT	x						x															
(Optional) O.SMP_TEE_DEBUG[6]	x														x	x						
OE.INTEGRATION_ CONFIGURATION							x					x										
OE.SECRETS																						
OE.PROTECTION_ AFTER_DELIVERY							x					x										
OE.TA_MANAGEMENT	x																					
OE.TA_DEVELOPMENT	x		x																			
OE.DISABLED_DEBUG	x															x						
OE.SMP_DRM_DEVELOPMENT																						

[5] In the SMP context this means that the TEE shall prevent unauthorized rollback by:

- Monitoring integrity of TEE Persistent Data as well as DRM code, keys and certificates;
- Reacting so that the SMP remains in a secure state and the access to SMP services, in particular playback, is not allowed upon detection of integrity violation.

[6] Refines and replaces the objective O.DEBUG that is defined in the Debug PP-Module.

SMP Objectives / Threats	Applies to TEE	Applies to P-REE	T.ABUSE_FUNC	T.CLONE	T.FLASH_DUMP	T.IMPERSONATION	T.ROGUE_CODE_EXECUTION	T.PERTURBATION	T.RAM	T.RNG	T.SPY	T.TEE_FIRMWARE_DOWNGRADE	T.STORAGE_CORRUPTION	T.TA_PERSISTENT_TIME_ROLLBACK	T. ROLLBACK	T.ABUSE_DEBUG	T.P-REE_ABUSE_FUNC	T.P-REE_ROGUE_CODE_EXECUTION	T.P-REE_MODIFICATION	T.P-REE_DISCLOSURE	T.P-REE_FIRMWARE_DOWNGRADE	T.P-REE_STORAGE_CORRUPTION
OE.P-REE_NTEGRATION_ CONFIGURATION																		x			x	
OE.P-REE_PROTECTION_ AFTER_DELIVERY																		x			x	

5.1.2 Coverage of assumptions and organisational security policies

Table 5-2 shows the security objectives for the SMP operational environment and the assumptions and organisational security policies they cover.

Table 5-2: SMP Objectives for the Environment and Coverage of OSP and Assumptions

SMP Objectives for the environment / Assumptions and OSP	Applies to TEE	Applies to P-REE	OSP.INTEGRATION_CONFIGURATION	OSP.SECRETS	OSP.P-REE_INTEGRATION_CONFIGURATION	A.PROTECTION_AFTER_DELIVERY	A.TA_MANAGEMENT	A.TA_DEVEOPMENT	A.SMP_DRM_DEVELOPMENT	A.P-REE_PROTECTION_AFTER_DELIVERY
OE.INTEGRATION_CONFIGURATION	x		x							
OE.SECRETS	x			x						
OE.PROTECTION_AFTER_DELIVERY	x					x				
OE.TA_MANAGEMENT	x						x			
OE.TA_DEVELOPMENT	x							x		
OE.DISABLED_DEBUG	x									
OE.SMP_DRM_DEVELOPMENT	x								x	
OE.P-REE_INTEGRATION_CONFIGURATION		x			x					
OE.P-REE_PROTECTION_AFTER_DELIVERY		x								x

5.2 Security objectives for the P-REE

The SMP PP-Module contains the following objectives for the P-REE.

O.P-REE_OPERATION

The P-REE shall ensure the correct operation of its security functionality and shall enter a secure state upon failure detection, without exposure of P-REE confidential assets, especially the plaintext media content.

O.P-REE_RUNTIME_CONFIDENTIALITY

The P-REE shall ensure that compressed and decompressed plaintext media content is protected against unauthorized disclosure. In particular,

- The P-REE shall not export plaintext media content to the NT-REE or any storage location accessible from the NT-REE;
- The P-REE shall grant access to plaintext media content only to Functions authorized by the PMM;
- The P-REE shall clean up Resources containing plaintext media content as soon as it can determine that their values are no longer needed.

Application Note:

- *Memory filters provide access control to plaintext media content. Isolation or obfuscation techniques may be used as well to protect confidentiality.*

(Optional) O.P-REE_FUNCTION_ISOLATION

The P-REE shall isolate the Functions executing arbitrary code: such Functions shall execute from and access only the Resources granted by the PMM.

In particular, the P-REE shall prevent Functions executing arbitrary code to write to resources accessible to the NT-REE.

Application Note:

- *This objective applies only if the P-REE allows to execute arbitrary code, otherwise the SMS is fixed.*
- *This objective contributes to the enforcement of the confidentiality of the P-REE media path.*
- *Moreover, a particular implementation may isolate all Functions from each other so that each Function accesses the Resources it has been granted access to and only to perform the allowed operations (read/write/execute).*

5.3 Security objectives for the TEE

The SMP PP-Module contains the following additional objectives for the TEE. The objectives defined in the TEE PP are not reproduced here.

Note:

- O.TEE_ISOLATION (from TEE PP): this objective can be achieved through hardware-enforced isolation mechanism. Such mechanism may become a requirement in some DRM schemes.
- O.INITIALISATION (from TEE PP): the initialisation can rely on code executed from ROM at boot time. Some DRM schemes may impose restrictive cryptographic strength for the authentication mechanism based on P-ROT.

O.SMP_TEE_INITIALISATION

The TEE shall start the P-REE through a secure initialisation process that ensures:

a. the integrity of the P-REE initialisation code and data used to load the P-REE firmware;

b. the authenticity and integrity of the P-REE firmware;

c. the binding of P-REE initialisation to the SoC of the device.

In particular, the TEE shall protect against P-REE firmware downgrade attacks.

The SMP initialisation process shall initialise the P-REE fixed pipeline Functions.

O.SMP_TEE_PMM

The TEE shall provide the PMM Function that configures the media pipeline and controls the Functions that enter and exit the SMS.

If the P-REE does not provide means to isolate the execution of arbitrary code, then the SMS is fixed. That is, the PMM shall not authorize non-SMP Functions to enter the SMS.

Application Note:

- *The PMM is initialised during TEE initialisation.*
- *This objective contributes to prevent the NT-*REE *from accessing the* P-REE media pipeline *and in the end the plaintext media content.*

O.SMP_TEE_DRM_CRYPTO

The TEE shall provide the cryptographic key management and operations that are required to implement the target DRM schemes.

Application Note:

- *This means that the TEE shall support the cryptographic algorithms required by the DRM applications to implement handshake protocols, content decryption or any other cryptographic functionality (see objective OE.SMP_DRM_DEVELOPMENT).*

O.SMP_TEE_ZEROIZATION

The TEE shall provide a zeroization mechanism for permanently erasing confidential information upon request of a Trusted Application.

Application Note: The DRM application should use this mechanism to erase Playback Map when it is no longer needed (see objective OE.SMP_DRM_DEVELOPMENT).

O.SMP_TEE_APPLICATION_MGT

The TEE shall provide application management functionality including application update.

The TEE shall ensure the authenticity and integrity of the application management requests and related data prior to the realization of the operation, e.g. the installation of an updated application.

Application Note: The ST author shall define the properties of the application management policy.

(Optional) O.SMP_TEE_DEBUG

The TEE shall authenticate the TEE Debug Administrator before granting access to the TEE debug features.

The TEE debug features shall not allow access to any SMP media asset, including the DRM code, keys and certificates as well as media content managed by the P-REE.

Application Note:

- *This objective applies only if TEE Debug features are available in production mode.*
- *This objective is a refinement of O.DEBUG defined in Debug PP-Module.*

5.4 Security objectives for the SMP operational environment

The following objectives for the operational environment defined in TEE PP apply to the SMP PP-Module:

- OE.INTEGRATION_CONFIGURATION;
- OE.SECRETS;
- OE.PROTECTION_AFTER_DELIVERY;
- OE.TA_MANAGEMENT;
- OE.TA_DEVELOPMENT;
- OE.DISABLED_DEBUG.

This module introduces the following additional objectives for the SMP environment:

OE.SMP_DRM_DEVELOPMENT

The DRM application shall:

- use the cryptographic key management and operations provided by the TEE to implement all the cryptographic DRM functionality, including handshake protocols and content decryption;
- delete the Playback Map using TEE services when playback is finished, i.e. when the user stops playback by hitting the stop button or the player application is exited. Deletion means removing the information by overwriting it with all zeroes or by overwriting it with random or unrelated data.

OE.P-REE_INTEGRATION_CONFIGURATION

Integration and configuration of the P-REE by the device manufacturer shall rely on guidelines defined by the P-REE provider. The guidelines shall include all the P-REE related security requirements for the device manufacturer issued from the SMP evaluation.

OE.P-REE_PROTECTION_AFTER_DELIVERY

The environment shall protect the TOE (SMP) after delivery and before entering the end-user phase. The persons manipulating the TOE in the operational environment shall apply the P-REE guidelines (e.g. user and administrator guidance, installation documentation, personalisation guide). The persons responsible for the application of the procedures contained in the guides, and the persons involved in delivery and protection of the product shall have the required skills and be aware of the security impact.

5.5 Security objectives rationale

The rationale of the coverage of threats, OSPs and assumptions that are not defined in the TEE PP apply. This section contains the rationales of the elements introduced in this SMP PP-Module.

T.RAM and T.SPY (from TEE PP)

The following additional objectives contribute to cover these threats provided the underlying mechanisms are used by the DRM Trusted Application(s):

- O.SMP_TEE_INITIALISATION completes O.INITIALISATION and ensures that the P-REE security functionality is correctly initialized and that the initialisation process is protected from the NT-REE;
- O.SMP_TEE_DRM_CRYPTO ensures a secure implementation of cryptographic operations and key management functionality;
- O.SMP_TEE_ZEROIZATION ensures a secure implementation of the data erasure functionality.

T.ROGUE_CODE_EXECUTION (from TEE PP)

The following additional objective contributes to cover this threat:

- O.SMP_TEE_INITIALISATION completes O.INITIALISATION and ensures that the P-REE security functionality is correctly initialized and the integrity of P-REE firmware
- O.SMP_TEE_APPLICATION_MGT ensures the authenticity of the updated application before it enters into the device and can be executed.

T.P-REE_ABUSE_FUNCT

The combination of the following objectives ensures protection against abuse of functionality:

- O.INITIALISATION ensures that the TEE security functionality is correctly initialized;
- O.SMP_TEE_INITIALISATION ensures that the P-REE security functionality is correctly initialized;
- O.P-REE_OPERATION ensures correct operation of the P-REE security functionality and proper management of failures;
- O.P-REE_RUNTIME_CONFIDENTIALITY prevents exposure of P-REE confidential data;
- (Optional) O.P-REE_FUNCTION_ISOLATION enforces the separation between Functions executing arbitrary code;
- O.SMP_TEE_PMM ensures that the SMS contains authorized Functions only.

T.P-REE_ROGUE_CODE_EXECUTION

The combination of the following objectives ensures protection against import of malicious code:

- O.INITIALISATION ensures that the TEE security functionality is correctly initialised and the integrity of the TEE firmware;
- O.SMP_TEE_INITIALISATION ensures that the P-REE security functionality is correctly initialised and the integrity of the P-REE firmware;
- O.P-REE_OPERATION ensures correct operation of the P-REE security functionality and proper management of failures;
- O.P-REE_RUNTIME_CONFIDENTIALITY prevents exposure of P-REE confidential data;
- O.SMP_TEE_PMM ensures that the SMS contains authorized Functions;
- OE.P-REE_INTEGRATION_CONFIGURATION ensures that import of code prior the end-user phase follows P-REE guidelines;
- OE.P-REE_PROTECTION_AFTER_DELIVERY ensures that the import of code prior the end-user phase is performed in an environment that complies with the P-REE guidelines by authorized persons only.

T.P-REE_MODIFICATION

The combination of the following objectives ensures protection against modification attacks:

- O.INITIALISATION ensures that the TEE security functionality is correctly initialised and that the initialisation process is protected from the REE;
- O.SMP_TEE_INITIALISATION ensures that the P-REE security functionality is correctly initialised and that the initialisation process is protected from the NT-REE;
- O.P-REE_OPERATION ensures correct operation of the P-REE security functionality and proper management of failures;
- (Optional) O.P-REE_FUNCTION_ISOLATION enforces the separation of arbitrary code from P-REE SMP Functions;
- O.SMP_TEE_PMM ensures the correct initialisation of the media pipeline and the control of Functions that enter and exit the SMS.

T.P-REE_DISCLOSURE

The combination of the following objectives ensures protection against disclosure of media content:

- O.INITIALISATION ensures that the TEE security functionality is correctly initialised and that the initialisation process is protected from the REE;
- O.SMP_TEE_INITIALISATION ensures that the P-REE security functionality is correctly initialised and that the initialisation process is protected from the NT-REE;
- O.P-REE_RUNTIME_CONFIDENTIALITY prevents exposure of P-REE confidential data;
- (Optional) O.P-REE_FUNCTION_ISOLATION enforces the separation of arbitrary code from P-REE SMP Functions;
- O.SMP_TEE_PMM ensures the correct initialisation of the media pipeline and the control of Functions that enter and exit the SMS.

T.P-REE_FIRMWARE_DOWNGRADE

The combination of the following objectives ensures protection against TEE firmware downgrade:

- O.INITIALISATION ensures that the TEE firmware that is executed is the version that was intended;

- O.SMP_TEE_INITIALISATION ensures that the P-REE firmware that is executed is the version that was intended;
- OE.P-REE_INTEGRATION_CONFIGURATION ensures that the P-REE firmware installed in the device is the version intended for that device;
- OE.P-REE_PROTECTION_AFTER_DELIVERY ensures the integrity protection of the P-REE firmware after delivery.

T.P-REE_STORAGE_CORRUPTION

The following objective ensures protection against corruption of P-REE firmware non-volatile storage:

- O.INITIALISATION ensures that the TEE firmware that is executed is the version that was intended;
- O.SMP_TEE_INITIALISATION ensures the integrity of the P-REE firmware that is executed;
- O.P-REE_OPERATION ensures the correct operation of the P-REE security functionality, including storage.

T. ABUSE_DEBUG

The protection against abuse of debug functionality is ensures by:

- the objective OE.DISABLED_DEBUG for the TOE environment when the Debug PP-Module is not used,
- the objective O.SMP_TEE_DEBUG for the TOE when the Debug PP-Module is used,

A.P-REE_PROTECTION_AFTER_DELIVERY

The objective OE.P-REE_PROTECTION_AFTER_DELIVERY covers this assumption.

OSP.P-REE_INTEGRATION_CONFIGURATION

The objective OE.P-REE_INTEGRATION_CONFIGURATION covers this organisational security policy.

6 Security Requirements

6.1 Security functional requirements

The set of SMP Security Functional Requirements contains requirements for the TEE and requirements for the P-REE, defined in sections 6.1.1 and 6.1.2, respectively.

6.1.1 TEE security functional requirements

The SMP security functional requirements for the TEE consists of the TEE PP requirements that cover the following security objectives for the TEE:

- O.CA_TA_IDENTIFICATION
- O.KEYS_USAGE
- O.TEE_ID
- O.INITIALISATION
- O.OPERATION
- O.RNG
- O.RUNTIME_CONFIDENTIALITY
- O.RUNTIME_INTEGRITY
- O.TA_AUTHENTICITY
- O.TA_ISOLATION
- O.TEE_DATA_PROTECTION
- O.TEE_ISOLATION
- O.TRUSTED_STORAGE
- O.TA_PERSISTENT_TIME
- O. ROLLBACK_PROTECTION

and the additional SMP_TEE requirements defined in this section, which cover the following SMP security objectives:

- O.SMP_TEE_INITIALISATION
- O.SMP_TEE_PMM
- O.SMP_TEE_DRM_CRYPTO
- O.SMP_TEE_ZEROIZATION
- O.SMP_TEE_APPLICATION_MGT
- (Optional) O.SMP_TEE_DEBUG

Table 6-1 shows the correspondence between the security functional requirements defined in this section and the security objectives.

6.1.1.1 SMP_TEE_COP - Cryptographic operation

SMP_TEE_COP.1

The TEE shall perform the authenticity and integrity checks required during SMP initialisation in accordance with well-defined cryptographic algorithms and cryptographic key sizes that meet the appropriate standards.

The developer shall fill in the following table:

SMP initialisation crypto operation	Cryptographic algorithm	Key size	Standard

SMP_TEE_COP.2

The TEE shall provide the cryptographic operations required by the DRM scheme in accordance with well-defined cryptographic algorithms and cryptographic key sizes that meet the appropriate standards.

The developer shall fill in the following table:

DRM crypto operation	Cryptographic algorithm	Key size	Standard

Note: This requirement shall be iterated for all the applicable DRM schemes.

6.1.1.2 SMP_TEE_FLS - Failure with preservation of secure state

SMP_TEE_FLS.1

The TEE shall preserve a secure state when the SMP initialisation fails to complete, in particular upon:

a) SoC binding failure;
b) P-REE firmware authenticity or integrity failure;
c) P-REE firmware downgrade.

Application Note: The developer shall identify all the failure conditions and describe the SMP secure state reached upon each of them.

SMP_TEE_FLS.2

The TEE shall ensure that the secure state reached upon SMP initialisation failure does not allow access to the media playback services of the SMP.

6.1.1.3 SMP_TEE_INI - SMP initialisation

SMP_TEE_INI.1

The SMP initialisation shall consist of a 2-step process that performs P-REE initialisation after TEE initialisation is completed according to the rules stated in the TEE PP.

Application Note: The developer shall describe the P-REE secure initial state.

Application Note: P-REE firmware downgrade verification has to rely on data stored on One Time Programmable (OTP) memories or EEPROM.O

SMP_TEE_INI.2

The SMP initialisation function shall detect and respond to errors and failures during SMP initialisation such that the TOE either successfully completes the initialisation or is halted.

SMP_TEE_INI.3

The SMP initialisation function shall not be able to arbitrarily interact with the TSF after the TOE initialisation completes.

6.1.1.4 SMP_TEE_RIP - Residual information protection

SMP_TEE_RIP.1

The TEE shall provide a zeroization mechanism for permanently erasing (confidential) information upon request of a Trusted Application.

Application Note: The DRM application must use the zeroization mechanism to erase the playback map as soon as the information is no longer needed.

SMP_TEE_RIP.2

The TEE shall ensure that any previous information content of a Resource is unavailable immediately following zeroization.

6.1.1.5 SMP_TEE_SMS - Secure Media System

SMP_TEE_SMS.1

The initial set of SMS Functions upon successful SMP initialisation shall contain exactly the SMP Functions.

SMP_TEE_SMS.2

The TEE shall provide the PMM Function that manages the transitions of non-SMP Functions into/out of the SMS.

If the P-REE does not provide means to isolate the execution of arbitrary code, then the PMM shall not authorize non-SMP Functions to enter the SMS.

Application Note: Such non-SMP Functions stand for arbitrary code that has to execute in a sandbox (cf. SMP_PREE_MCA.2b).

6.1.1.6 SMP_TEE_APM – Application management

SMP_TEE_APM.1

The TEE shall provide application management functionality including application update.

SMP_TEE_APM.2

The TEE shall ensure the authenticity and integrity of the application management requests and related data prior to the realization of the operation, e.g. the installation of an updated application.

6.1.1.7 (Optional) SMP_TEE_TSD - TEE secure debug

SMP_TEE_TSD.1

The TEE shall authenticate the TEE Debug Administrator before granting access to the TEE debug functionality.

SMP_TEE_TSD.2

The TEE debug functionality shall not allow access to any SMP media asset, including the DRM code, keys and certificates as well as media content managed by the P-REE.

6.1.2 P-REE security functional requirements

The SMP security functional requirements for the P-REE consists of new requirements, additional to the TEE PP requirements, which cover the following security objectives:

- O.P-REE_OPERATION
- O.P-REE_RUNTIME_CONFIDENTIALITY
- (Optional) O.P-REE_FUNCTION_ISOLATION

Table 6-2 shows the correspondence between the security functional requirements defined in this section and the security objectives.

6.1.2.1 SMP_PREE_FLS - Failure with preservation of secure state

SMP_PREE_FLS.1

The P-REE shall preserve a secure state when the following types of failures occur:

- Invalid operation (invalid access attempt to Protected or Interface Resource), denied by the Media Content Access Policy.

Application Note: The developer shall describe the P-REE secure state reached upon violation of the Media Content Access Policy.

SMP_PREE_FLS.2

The P-REE shall ensure that the state reached upon Media Content Access Policy violation does not allow access to compressed or decompressed plaintext media content or any other P-REE confidential asset.

6.1.2.2 SMP_PREE_MCA - Media Content Access Policy

This section states the minimal set of access restrictions which must be enforced by the P-REE. Additional restrictions, for example granting different access permissions to Resources containing compressed and decompressed forms of plaintext media data, may optionally be applied.

SMP_PREE_MCA.1

The P-REE, through its hardware filters, shall deny read access to the Resource R by the Function F if the following condition is met:

a) F is not an SMS Function and R is a Protected Resource.

SMP_PREE_MCA.2

The P-REE, through its hardware filters, shall deny write access to the Resource R by the Function F if one of the following conditions is met:

a) F is an SMS Function, R is a Non-Trusted Non-Interface Resource and F requests to write a P-REE asset (media content) to R;
b) F is an SMS Function that is not an SMP Function (F is arbitrary code) and R is an Interface Resource.

SMP_PREE_MCA.3

The SMP Functions shall not write SMP assets into Interface Resources.

6.1.2.3 SMP_PREE_RIP - Residual information protection

SMP_PREE_RIP.1

The P-REE shall clean up Resources containing compressed and decompressed plaintext media content as soon as it can determine that such data is no longer needed.

6.1.3 Security functional requirements rationale

The following tables show the mapping between the security objectives for the TEE and the P-REE and the security functional requirements introduced in this SMP PP-Module.

Table 6-1: SMP Objectives and Requirements Coverage (TEE Additional Part)

TEE additional security objectives	TEE additional security requirements
O.SMP_TEE_INITIALISATION	SMP_TEE_COP.1 SMP_TEE_FLS.1 to 2 SMP_TEE_INI.1 to 3 SMP_TEE_SMS.1
O.SMP_TEE_PMM	SMP_TEE_SMS.2
O.SMP_TEE_DRM_CRYPTO	SMP_TEE_COP.2
O.SMP_TEE_ZEROIZATION	SMP_TEE_RIP.1 to 2
O.SMP_TEE_APPLICATION_MGT	SMP_TEE_APM.1 to 2
(Optional) O.SMP_TEE_DEBUG	SMP_TEE_TSD.1 to 2

Table 6-2: SMP Objectives and Requirements Coverage (P-REE Part)

P-REE security objectives	P-REE security requirements
O.P-REE_OPERATION	SMP_PREE_FLS.1 to 2
O.P-REE_RUNTIME_CONFIDENTIALITY	SMS_PREE_MCA.1 to 2 SMP_PREE_RIP.1
(Optional) O.P-REE_FUNCTION_ISOLATION	SMS_PREE_MCA.2b

7 CC Security Functional Requirements

This chapter contains the Security Functional Requirements (SFR) for the SMP in Common Criteria (CC) language.

7.1 Security requirements rationale

Table 7-1: SMP Objectives and CC SFRs Coverage (TEE Additional Part)

TEE additional security objectives	TEE additional security requirements	CC SFR
O.SMP_TEE_INITIALISATION	SMP_TEE_COP.1	FCS_COP.1/SMP_INI
	SMP_TEE_FLS.1 to 2	FPT_FLS.1/SMP_INI
	SMP_TEE_INI.1 to 3	FPT_INI.1/SMP
	SMP_TEE_SMS.1	FPT_INI.1/SMP, FMT_SMF.1/SMS
O.SMP_TEE_PMM	SMP_TEE_SMS.2	FMT_MTD.1/SMS, FMT_SMF.1/SMS
O.SMP_TEE_DRM_CRYPTO	SMP_TEE_COP.2	FCS_COP.1/SMP_DRM
O.SMP_TEE_ZEROIZATION	SMP_TEE_RIP.1 to 2	FDP_RIP.1/ZERO
O.SMP_TEE_APPLICATION_MGT	SMP_TEE_APM.1 to 2	FTP_TRP.1/APM, FDP_ACC.1/APM, FDP_ACF.1/APM, FDP_ITC.2/APM, FMT_MSA.3/APM, FMT_SMR.1/APM FCS_COP.1/APM FPT_FLS.1/APM
(Optional) O.SMP_TEE_DEBUG	SMP_TEE_TSD.1	SFRs defined in Debug PP-Module
	SMP_TEE_TSD.2	FMT_SMF.1/DEBUG

Table 7-2: SMP Objectives and CC SFRs Coverage (P-REE Part)

P-REE security objectives	P-REE security requirements	CC SFR
O.P-REE_OPERATION	SMP_PREE_FLS.1 to 2	FPT_FLS.1/P-REE
O.P-REE_RUNTIME_CONFIDENTIALITY	SMS_PREE_MCA.1 to 3	FDP_ACC.1/MCA, FDP_ACF.1/MCA, FMT_MSA.3/MCA
	SMP_PREE_RIP.1	FDP_RIP.1/ P-REE
(Optional) O.P-REE_FUNCTION_ISOLATION	SMS_PREE_MCA.2b	FDP_ACC.1/MCA, FDP_ACF.1/MCA, FMT_MSA.3/MCA

7.2 Additional TEE security functional requirements

7.2.1 SMP_TEE_COP: Cryptographic operation

FCS_COP.1/SMP_INI Cryptographic operation

FCS_COP.1.1/SMP_INI The TSF shall perform [assignment: **list of authenticity and integrity cryptographic operations required during SMP initialisation**] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

FCS_COP.1/SMP_DRM Cryptographic operation

FCS_COP.1.1/SMP_DRM The TSF shall perform [assignment**: list of cryptographic operations required by the DRM scheme**] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

FCS_COP.1/APM Cryptographic operation

FCS_COP.1.1/APM The TSF shall perform **[assignment: list of cryptographic operations related with the application management operations defined in FDP_ACC.1]** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

7.2.2 SMP_TEE_RIP: Residual information protection

FDP_RIP.1/ZERO Subset residual information protection

FDP_RIP.1.1/ZERO The TSF shall ensure that any previous information content of a resource is made unavailable upon **the zeroisation of the resource by a Trusted Application** from the following objects: **any**.

7.2.3 SMP_TEE_FLS: Failure with preservation of secure state

FPT_FLS.1/SMP_INI Failure with preservation of secure state

FPT_FLS.1.1/SMP_INI The TSF shall preserve a secure state when the following types of failures occur:

- **Device binding failure**
- **P-REE firmware authenticity or integrity failure**
- **P-REE firmware downgrade**
- [assignment: **list of types of failures during SMP initialisation]**.

Refinement:

The TEE shall ensure that the secure state reached upon SMP initialisation failure or integrity checking failure does not allow access to the media playback services of the SMP.

FPT_FLS.1/APM Failure with preservation of secure state

FPT_FLS.1.1/APM The TSF shall preserve a secure state when the following types of failures occur: **interruption or incident which prevents the completion of an application management operation as defined in FDP_ACC.1/APM.**

7.2.4 SMP_TEE_INI: SMP initialisation

FPT_INI.1/SMP TSF initialisation

FPT_INI.1.1/SMP The TOE initialisation function shall verify

- **the binding of P-REE initialisation to the SoC of the device,**
- **the integrity of the P-REE initialisation code and data used to load the P-REE firmware,**
- **the authenticity and integrity of P-REE firmware,**
- **the version of the P-REE firmware to prevent downgrade to previous versions**
- [assignment: **list of implementation-dependent verifications**]

prior to establishing the TSF in a secure initial state.

Refinement:

- TSF stands for SMP including the P-REE
- In the secure initial state the SMS contains exactly the SMP-Functions, as specified in FMT_MTD.1/SMS.

FPT_INI.1.2/SMP The TOE initialisation function shall detect and respond to errors and failures during initialisation such that the TOE either successfully completes initialisation or is halted.

FPT_INI.1.3/SMP The TOE initialisation function shall not be able to arbitrarily interact with the TSF after TOE initialisation completes.

Application Note:

P-REE firmware downgrade verification has to rely on data residing on the TOE, for instance on One Time Programmable (OTP) memories or EEPROM.

7.2.5 SMP_TEE_SMS: SMS initialization and update

FMT_MTD.1/SMS Management of TSF data

Dependencies:

- FMT_SMR.1 Security roles –discarded (PMM is part of the TSF, user identification is not required)
- FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SMS The TSF shall restrict the ability to **define (initialize, add, configure)** the **set of SMS Functions** to **the PMM Function**.

FMT_SMF.1/SMS Specification of Management Functions

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

- **Initialize the set of SMS Functions with the SMP Functions**

- **Add non-SMP Functions to the SMS, provided the P-REE provides means to isolate the execurion of arbitrary code**
- **Configure the SMS Functions**

7.2.5.1 (Optional) SMP_TEE_TSD: TEE secure debug

If the TEE implements debug features in production mode then the Debug PP-Module applies and

- the SFRs defined in that PP-Module cover the requirement SMS_TEE_TSD.1.
- the following FSRs cover the requirement SMS_TEE_TSD.2.

FMT_SMF.1/DEBUG Specification of Management Functions

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

- Disallowing the access to any SMP media asset including the DRM code, keys and certificates as well as media content managed by the P-REE by debug functionality (OP.DEBUG in FDP_ACC.1)

7.2.5.2 SMP_TEE_APM: Application management

FTP_TRP.1/APM Trusted Path

FTP_TRP.1.1/APM The TSF shall provide a communication path between itself and [selection: remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [assignment: modification, disclosure, other types of integrity or confidentiality violation]**.**

FTP_TRP.1.2/APM The TSF shall permit [selection: the TSF, local users, remote users] to initiate communication via the trusted path.

FTP_TRP.1.3/APM The TSF shall require the use of the trusted path for **application management operations**.

FDP_ACC.1/APM Subset access control

FDP_ACC.1.1/APM The TSF shall enforce the **Application Management (APM) Access Control Policy** on **the following:**

- **Subjects: Application Manager**
- **Objects:**
  - **for TA_update: current TA, new TA [assignment: list of other objects covered by the SFP]**
  - **[assignment: For other application management operations, list of objects covered by the SFP]**
- **Operations:**

- **TA_update**
- **[assignment: list of other application management operations covered by the SFP]**

Application Note:

- Subjects: Application Manager stands for the entity that is responsible for authorizing and performing the application management operation. The ST author may refine the definition of this subject.
- The ST author shall define the application management operations and the related objects.

FDP_ACF.1/ APM **Security attribute based access control**

FDP_ACF.1.1/ APM The TSF shall enforce the **APM Access Control Policy** to objects based on the following:

- **Application Manager's security attributes: [assignment: SFP-relevant security attributes, or named groups of SFP-relevant security attributes]**
- **Objects' security attributes:**
  - **For TA_update: [assignment: (named groups of) SFP-relevant objects's security attributes]**
  - **[assignment: For any other application management operation, (named groups of) SFP-relevant objects' security attributes]**

FDP_ACF.1.2/APM 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].

FDP_ACF.1.3/APM 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/APM 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].

Application Note:

- FDP_ACF.1.1/APM: The ST author shall define the security attributes that are used to authorize or deny an application management operation. For instance, for TA_update, the security attributes of the "current TA" may include identification data and life-cycle state, and the security attributes of the "new TA" may include identification data, signature, checksum, etc.

- FDP_ACF.1.2/APM: The ST author shall define the rules for authorizing each of the application management operations. For instance, TA_update should require that the “new TA” is authentic, integer and does not lead to TA downgrade.

- The ST author may decide to discard any of the SFRs FMT_MSA.3, FMT_SMR.1 and FMT_SMF.1 when they are not necessary for specifying the APM Access Control SFP.

FDP_ITC.2/APM Import of user data with security attributes

FDP_ITC.2.1/APM The TSF shall enforce the **APM Access Control Policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/APM The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/APM The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/APM The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/APM The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules]

Application Note:
This SFR applies to data (objects) that are imported into the TOE with their security attributes. For instance, the “new TA” involved in a TA_update operation.

FMT_MSA.3/APM Security attribute initialisation

FMT_MSA.3.1/APM The TSF shall enforce the **APM Access Control Policy** to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/APM 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.

FMT_SMR.1/APM Security roles

FMT_SMR.1.1/APM The TSF shall maintain the roles [assignment: the authorised identified roles].

FMT_SMR.1.2/APM The TSF shall be able to associate users with roles.

FMT_SMF.1/APM Specification of Management Functions

FMT_SMF.1.1/APM The TSF shall be capable of performing the following management functions: **[assignment: list of operations related to the application management]**.

7.3 P-REE security functional requirements

7.3.1 SMP_PREE_RIP: Residual information protection

FDP_RIP.1/P-REE Runtime Subset residual information protection

FDP_RIP.1.1/P-REE 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] the following objects: [assignment: list of objects].

Refinement:
The TSF shall ensure that compressed and decompressed plaintext media content is made unavailable as soon as it can determine that such data is no longer needed.

7.3.2 SMP_PREE_FLS: Failure with preservation of secure state

FPT_FLS.1/P-REE Failure with preservation of secure state

FPT_FLS.1.1/P-REE The TSF shall preserve a secure state when the following types of failures occur:

- **Invalid operation: access to Protected or Interface Resource rejected by the security policy**
- [assignment: list of types of failures in the TSF].

Refinement:
The P-REE shall ensure that the secure state reached upon security policy violation does not allow access to compressed or decompressed plaintext media content.

7.3.3 SMS_PREE_MCA: Media Content Access Policy

FDP_ACC.1/MCA Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/MCA The TSF shall enforce the **Media Content Access Control SFP** on

- **Subjects: SMS Functions**
- **Objects: Resources**
- **Operations: read and write compressed or uncompressed plaintext media content.**

Application Note: non-SMP Functions are in scope only in the case where P-REE supports sandboxing of arbitrary code (non-SMP Functions).

FDP_ACF.1/MCA Security attribute based access control

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/MCA The TSF shall enforce the **Media Content Access Control SFP** to objects based on the following:

- **Subjects' security attributes: 'Function.type' (values : SMP or non-SMP)**
- **Objects' security attributes: 'Resource.type' (values: Trusted, Protected or Non-Trusted Resource) and boolean 'Resource.isInterface'.**

FDP_ACF.1.2/MCA The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Function		Protected Resource		Non-Trusted Resource	
		Interface	Non-Interface	Interface	Non-Interface
SMS	**SMP**	Read / ~~Write~~ (MCA.3)	Read / Write	Read / ~~Write~~ (MCA.3)	Read / ~~Write~~ (MCA.2a)
SMS	**Non-SMP**	Read / ~~Write~~ (MCA.2b)	Read / Write	Read / ~~Write~~ (MCA.2b)	Read / ~~Write~~ (MCA.2a)
Non-SMS		~~Read~~ / Write (MCA.1)	~~Read~~ / Write (MCA.1)	Read / Write	Read / Write

Application Note:

The MCA.2b rule for non-SMP Functions are in scope only in the case where P-REE supports sandboxing of arbitrary code.

FDP_ACF.1.3/MCA 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/MCA 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].

Refinement FDP_ACF.1/MCA:
The TSF stands for the P-REE through its hardware filters.

FMT_MSA.3/MCA Static attribute initialisation

Dependencies:

- FMT_MSA.1 Management of security attributes – discarded (the P-REE cannot change the attributes of the Functions or Resources)
- FMT_SMR.1 Security roles – discarded (no role required)

FMT_MSA.3.1/MCA The TSF shall enforce the **Media Content Access Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/MCA The TSF shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.