TRUSTED CONNECTIVITY ALLIANCE

Open Firmware Loader (OFL) Ecosystem

Version 1.0.3

Published by simalliance now Trusted Connectivity Alliance

May 2019

Intellectual Property Rights (IPR) Disclaimer

Attention is drawn to the possibility that some of the elements of any material available for download from the specification pages on Trusted Connectivity Alliance's website may be the subject of Intellectual Property Rights (IPR) of third parties, some, but not all, of which are identified below.

Trusted Connectivity Alliance shall not be held responsible for identifying any or all such IPR, and has made no inquiry into the possible existence of any such IPR. TRUSTED CONNECTIVITY ALLIANCE SPECIFICATIONS ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER TRUSTED CONNECTIVITY ALLIANCE, 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 ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION.

Table of Contents

Figures

Tables

1 Introduction

1.1 Normative References

Selected normative references used in this document are included in Table 1-1.

Table 1-1: Normative References

Standard / Specification	Description	Ref
GPC_FST_134	GlobalPlatform Open Firmware Loader for Tamper Resistant Element Version 1.3 and later[1].	[OFL]
GPC_FST_140	GlobalPlatform Technology VPP - Network Protocol v1.0.1	[VNP]
GPC_FST_141	GlobalPlatform Technology VPP - OFL VNP Extension	[OFLE]
GPC_FST_142	GlobalPlatform Technology VPP - Concepts and Interfaces 1.0.1	[VCI]
GPC_FST_143	GlobalPlatform Technology VPP - Firmware Format v1.0.1	[VFF]
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]
SA_INT2	SIMalliance IDS to Image Owner Interface-v1.0	[INT2]
SA_INT4	SIMalliance IDS to OFL Agent Interface-v1.0	[INT4]
SA_INT7	SIMalliance Image Maker/Image Owner Interface-v1.0	[INT7]
SA_INT8	SIMalliance IDS/TRE Maker Interface-v1.0	[INT8]
SA_INT10	SIMalliance IDS/OEM device Maker Interface-v1.0	[INT10]

1.2 Informative References

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

Table 1-2: Informative References

Standard / Specification	Description	Ref
GSMA iUICC PoC PP	GSMA iUICC PoC Group Primary Platform Requirements	[IUICC Req]
GSMA SGP 2.2	GSMA RSP Technical Specification Version 2.2 01 September 2017	[SGP22]
GSMA SGP 0.2	GSMA Remote Provisioning Architecture for Embedded UICC Technical Specification Version 2.1 02 November 2015	[SGP02]

1.3 Abbreviations

Selected abbreviations and notations used in this document are included in Table 1-3.

[1] PBL Working Group is anticipating the approval of the GlobalPlatform OFL 2.0.0 specification release.

Table 1-3: Abbreviations

Abbreviation	Meaning
ARP	Access Rights Pattern defined in [OFL]
CI	Certificate Issuer (e.g. CI_{OFL} and CI_{IDS})
MMI	Man Machine Interface
M2M	Machine to Machine
NA	Not Applicable
OFB	Other Functional Block
OFL	Open Firmware Loader
RFU	Reserved for Future Use
RO	Read-Only
RW	Read / Write
SDO	Standard Development Organization.
VCI	VPP Concepts and Interfaces
VFF	VPP Firmware Format
VNP	VPP Network Protocol defined in [VNP].
VPP	Virtual Primary Platform defined in [VCI]
WO	Write-Only

1.4 Definitions

1.4.1 Key Words

The following meanings apply to SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY in this document as defined in the RFC 2119 [RFC 2119]:

- **SHALL** indicates an absolute requirement, as does **MUST**.
- **SHALL NOT** indicates an absolute prohibition, as does **MUST NOT**.
    - **SHOULD** and **SHOULD NOT** indicate recommendations: the “SHOULD NOT” part is new in this structure
    - **MAY** indicates an option.

The names starting with a Capital letter refers to terms having a definition in the Table 1-4 or a description in a section of this document or both.

1.4.2 Other Terminology

Selected terms used in this document are included in Table 1-4.

Table 1-4: Terminology and Definitions

Term	Definition
Actor	Legal entity involved in the OFL ecosystem due either to a process in the OFL data flow or as a provider of assets (e.g. keys, certificates…).

Term	Definition
Authentication Token	Defined in [OFL].
ARP Certificate	Defined in [OFL].
End-User	Physical person interacting with the device MMI.
Firmware	Defined in [OFL].
Firmware Loading	Defined in [OFL].
Firmware Update	Defined in [OFL].
IMF	Image Maker Facility.
IMF Agent	Agent in the IMF interfacing the IDS.
IMF Server	Server operating in the IMF on behalf of the Image Maker and interfacing the IOF.
IOF Agent	Agent in the IOF interfacing with the IDS or the IMF Server.
IOF	Image Owner Facility. Place where the Image Owner operate.
Image	Generic data format encapsulating an encrypted Firmware supporting a format defined in [VFF], cryptographic material and directives able to be processed by the OFL in [OFL].
Image Owner	Defined in [OFL].
Industry Organization	Consortium of companies that are representative of an industry or sharing common interests in the development of specific technology.
Multicast Bound Image	Image bound to a given group of Firmware identified by their Group Identifier. This Image is used for a multicast Image Loading as defined in [OFL].
OFL Agent	Defined in [OFL].
OMF Agent	Agent in the OMF interfacing the IDS.
OFB	Other Functional Block. This block may contain functionalities contributing to the Firmware management (e.g. user's interface) see Table 5-1.
OFL Authority	Defined in [OFL].
OMF	OEM device Manufacturer Facilities manufactures their devices.
Open Firmware Loader	Defined in [OFL].
Subscriber	Logical (M2M) or Physical entity (i.e. End-User) subscribing a Service on the TRE.
TMF Agent	Agent in the TMF interfacing the IDS.
TMF	TRE Maker Facility of the TRE maker where the TRE are manufactured.
TRE	Defined in [OFL].
TRE Instance	Identified instance of a TRE.
TRE Credentials	Defined in [OFL]

Term	Definition
Unbound Image	Image able to be installed into any authorized TRE exposing a given PART_NUMBER (defined in [OFL]; the Firmware conveyed in this Image can only be installed in a TRE publishing this PART_NUMBER.
Unicast Bound Image	Image tied to a unique TRE Instance; This Image is used for unicast Image Loading as defined in [OFL].
VPP Application	Defined in [VCI].

2 Overview

This document aims at providing an overview of the ecosystem surrounding the OFL technology. This includes the Actors, as well as, the Functions and the interfaces between all of them. This document does not detail the Actors, Functions and interfaces, but provides the reference of the documents in which the details are consolidated.

This ecosystem is independent of the technology of the TRE and the use case supported by the Firmware which is installed in the TRE.

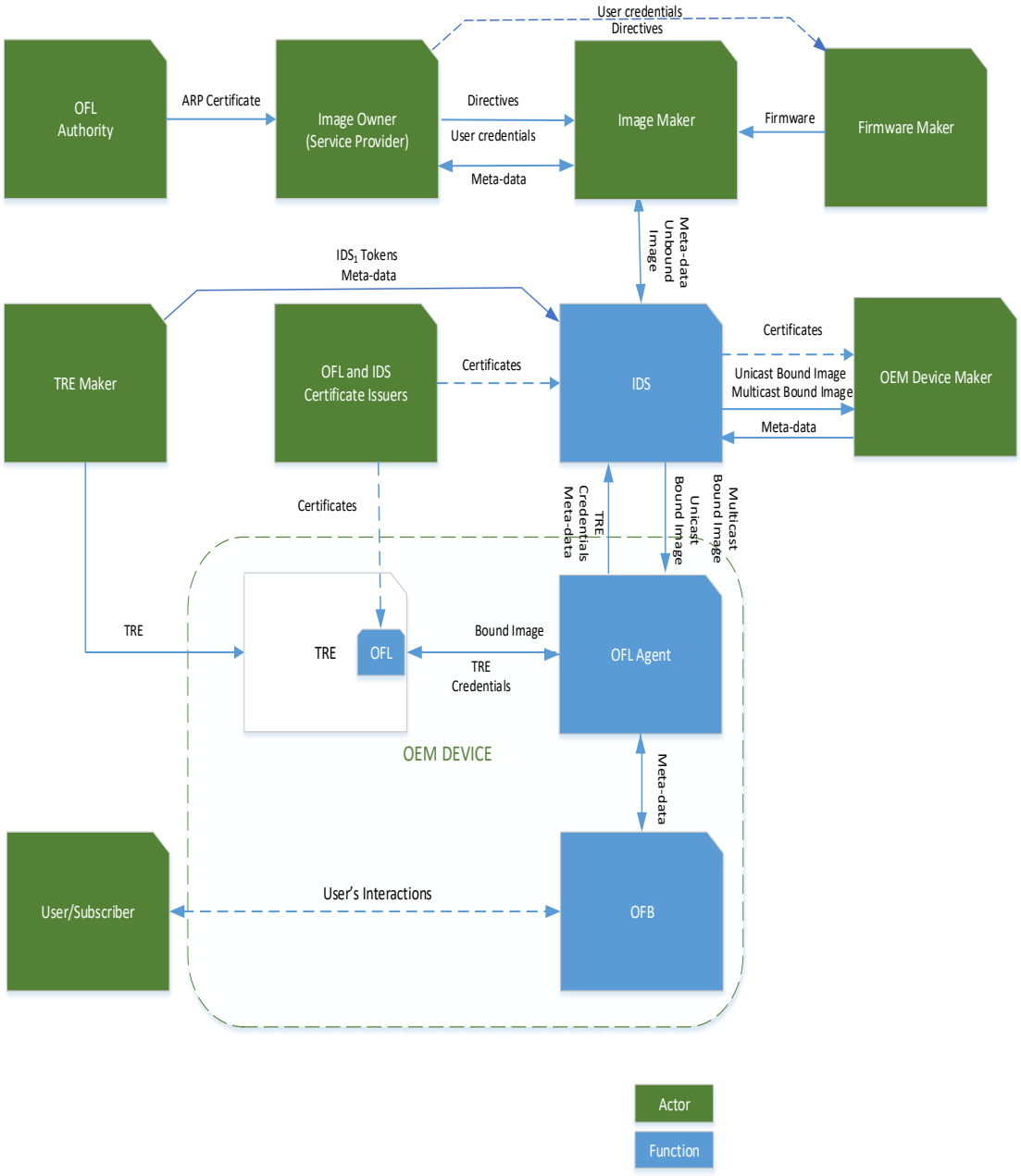
As a consequence, the TRE may be:

- Integrated in a SoC as defined in [VCI] and appears as an integrated TRE (iTRE). The Firmware loaded into the TRE follow the requirements and specifications from a SDO such as ETSI or an Industry Organisation such as GSMA and host at least one application defined by 3GPP. The iTRE may support specifications as defined in TS 102.221 in [TS102.221] or SGP 2.2 in [SGP22] or SGP 0.2 in [SGP02]. The resulting combination is called iUICC (integrated UICC).
- Integrated in a discrete chip which is embedded in a device then appears as an embedded TRE (eTRE). The Firmware loaded into the TRE may follow the requirements and specifications from a SDO such as ETSI or an Industry Organization such as GSMA and host at least one application defined by 3GPP. The eTRE may support specifications as defined in TS 102.221 in [TS102.221] or SGP 2.2 in [SGP22] or SGP 0.2 in [SGP02]. The resulting combination is called eUICC (embedded UICC).
- Integrated in a discrete chip which is inserted in a device then appears as a removable TRE (rTRE). The Firmware loaded into the TRE may follow the requirements and specifications from a SDO such as the ETSI or an Industry Organization such as GSMA and hosting at least one application defined by 3GPP. The rTRE may support specifications as defined in TS 102.221 in [TS102.221] or SGP 2.2 in [SGP22] or SGP 0.2 in [SGP02]. The resulting combination is called UICC.

3 The OFL ecosystem

The OFL ecosystem is represented in Figure 3-1.

Figure 3-1: The OFL Ecosystem



For sake of simplicity, the term Bound Image denotes either a Unicast Bound Image or Multicast Bound Image.

The OFL ecosystem relies on 7 different Actors:

- The OFL Authority generates an ARP Certificate granting access rights to a TRE in counterpart of an agreement with the Image Owner.

- The Image Owner (a.k.a. Service Provider) defining requirements and directives for End-User/Subscriber services to the Image Maker. The Image Owner provides the End-User/Subscriber credentials to the Firmware Maker via the Image Maker or directly with an interface out of the scope of this specification.
- The Image Maker gets a Firmware from a Firmware Maker supporting the requirements and the input data from an Image Owner. The Image Maker encapsulates the Firmware within a secure container called the Unbound Image. The Unbound Image is provisioned to the IDS under control and agreement with the Image Owner.
- The OFL Certificate Issuers (CI_{OFL}) and IDS Certificate Issuers (CI_{IDS}) may manage multiple Public Key Infrastructures (PKI) ensuring trusted exchanges between the Actors and the Functions. The OFL CI_{OFL} issues all certificates to the OFL and the Certificates ensuring a trustable collaboration with other Functions depending to IDS Certificate Issuers. The IDS CI_{IDS} issues all certificates to the IDS.
- The TRE Maker manufactures the TRE according to specifications from Industry Organizations and/or a SDO.
- The OEM Device Maker manufactures an OEM device embedding the OFL Agent and the TRE provisioned from the TRE Maker. The OEM Device Maker implements the OFL Agent and the OFB, which bridges the IDS and OFL running in the TRE.
- The End-User/Subscriber interacts with the OFB. Indeed, the End-User may be prompted for giving his explicit consent validating some OFL operations or retrieves specific credentials required for initiating the OFL operations from the Service Provider.

The OFL ecosystem defines 5 Functions:

- The IDS (Image Delivery Server) is the Function in charge to deliver Bound Images to the OFL Agent or to the OEM Device Maker.
- The OFL Agent is the Function in charge of supporting the procedure defined in [OFLE] from a data flow as defined in [INT4]. This Function manages a certificate used for authentication with the IDS and gets/forwards meta-data between the IDS and the OFB or between the OFL Agent and the OFB.
- The Open Firmware Loader as defined in [OFL].
- The TRE is a secure environment able to run the instance of the Firmware. The TRE may be compliant with the VPP specifications as defined in [VCI], [OFLE], [VFF] and [VNP].
- The OFB implements the requirements from Industry Organizations and/or SDO. The OFB is usually use case dependent and may interact with the End-User through a MMI. The OFB collaborates with the OFL Agent.

Section 6 defines all interfaces between the Actors and the Functions.

The OFL and IDS certificates issuance is out of the scope of this document.

4 The Actors

Each actor (in green boxes on the Figure 3-1) of the OFL ecosystem exposes a role and endorses a responsibility defined in Table 4-1).

Table 4-1: Actors, Roles and Responsibilities

Actor	Roles and Responsibilities	Input	Output
Image Owner / Service Provider	• Provides Services • Defines directives and orders the corresponding Images • Provides profile information, input data	• ARP Certificate from the OFL Authority managing the TRE • Report from the Image Maker • Report from the IDS	• Directives to the Image and Firmware Makers • User's credentials to the Image Maker • ARP Certificate from the OFL Authority to the IDS • Directives to the IDS
Image Maker	• Design the Image template from Image Owner directives • Create diversified data from Image Owner input data. • Get a Firmware from a Firmware Maker that includes the High Level Operating System and the diversified data • Create an Unbound Image containing the Firmware and possibly user's credentials • Sends the Unbound Image to the IDS	• TRE specification from the TRE Maker • User's credentials from the Image Owner • IDS_1 Authentication Tokens[2] to the Image Maker	• Unbound Image • Reports to the Image Owner •
Firmware Maker	• Design a Firmware that includes the High Level Operating System and its application(s)	• TRE specification from the TRE Maker Directives from the Image Owner • Diversified data	• The Firmware
TRE Maker	• This actor manufactures a TRE integrating a loader to implement OFL	• TRE specification from Industry Organization and/or a SDO • PN Certificate from the Certificate Issuer	• TRE to the OEM device maker • OFL certificate • IDS_1 Authentication Tokens[2] to the Image Maker
OEM Device Maker	• This actor implements a TRE and the OFL agent during the manufacturing of the device	• Certificate for the OFL Agent • TRE	• OEM device

[2] Authentication Tokens as defined in [OFL].

Actor	Roles and Responsibilities	Input	Output
OFL Authority	• This actor grants the rights for Image Owners to create an Image accepted by a TRE implementing OFL	• Business agreement from the Image Owner	• ARP Certificate
OFL CI_{OFL} and IDS CI_{IDS}	• Issues Certificates for Actors of the OFL ecosystem and acts as a trusted third parties for the purpose of authenticating the Actors of the ecosystem	• Agreements • Evidences about certification conformances	• PN certificate to the TRE maker • IDS certificates • IMO certificate (option) • OFL Agent certificate (TLS) (optional)

5 The Functions

Each Function (in blue boxes on the Figure 3-1) of the OFL ecosystem is described in Table 5-1.

Table 5-1: Functions

Function	Description	Input	Output
IDS	• IDS_1 Tokens repository: storage of IDS_1 Authentication Tokens • Bound Image repository: temporary storage of Bound Images • Unbound Image repository: storage of Unbound Images • Binding of an Unbound Image (on demand) on a specific TRE • Provisioning the Bound Image to the OEM device via the OFL Agent • Report of the loading operation to the Image Maker and/or the Image Owner	• Unbound Image • IDS_1 Authentication Tokens • TRE Credentials	• Bound Images • Reporting to Image Maker and Image Owner
Open Firmware Loader	• Extracting the Firmware from the Bound Image the loading of the Firmware into the TRE • Administrative operations on the Firmware (enabling, disabling, deletion, update) • Administrative operations on the TRE (OFL authority changes, policy update…)	• Bound Image	• Status information
OFL Agent	• Responsible for transferring Bound Images from IDS to OFL • Responsible for forwarding meta-data from IDS to OFB • Collaborate with the OFB for supporting Industry Organization requirements	• Bound Image • Meta-data from the OFB • Status information from the OFL	• Bound Image to OFL • Meta-data to OFB • Notification to IDS • Meta-data to IDS

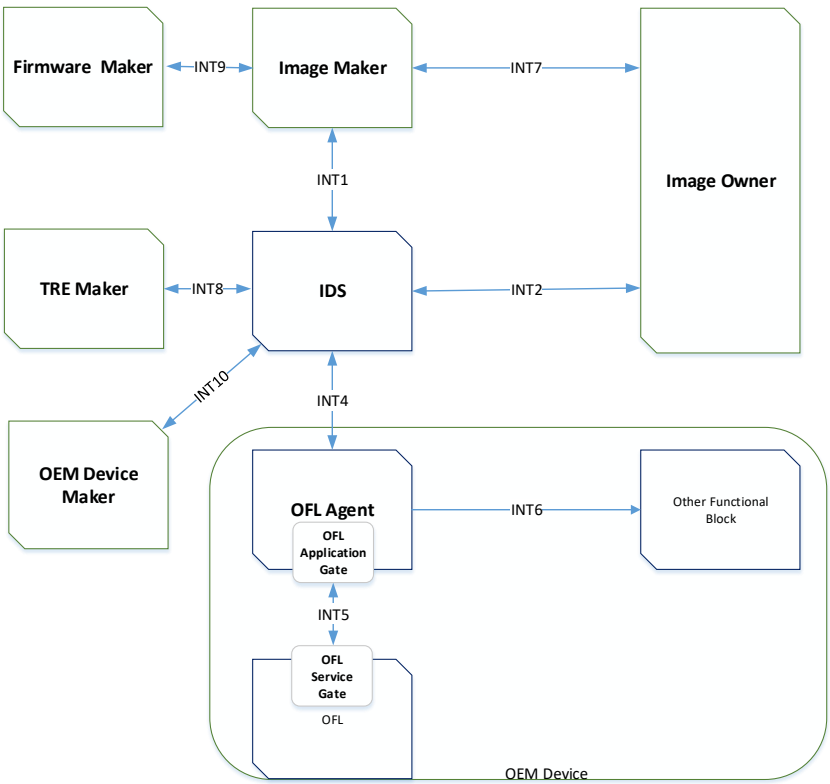
Function	Description	Input	Output
TRE	• Run the instance of Firmware • Run OFL	• VNP Packet as defined in [VNP]	• VNP Packet
OFB	• Implement the Industry Organization requirements • May interact with the End-End-User/Subscriber	• Meta-data • End-User's interaction (MMI)	• Meta-data • MMI

6 The interfaces

6.1 Overview

Figure 6-1 illustrates the interfaces between the Actors and the Functions.

Figure 6-1: Interfaces between Actors and Functions



6.2 The Function Interfaces

6.2.1 IDS Function Interfaces

The IDS Function may be assigned to different actors (i.e. TRE Maker, OEM Device Maker, Image Maker and Image Owner) and depending on the selected actor supporting the IDS Function then some interfaces shall be defined or may be proprietary.

Table 6-1 defines the standard interfaces required according to the assignment of the IDS Function to an Actor exposing the optimal configuration.

Table 6-1: Standard interfaces vs Actors

Actor supporting the IDS Function	Standard interface	Optional proprietary interface
Image Maker	INT2,INT4, INT8, INT10	INT1, INT7, INT9

The interfaces to the IDS are the following:

- The INT4 is defined in [INT4] and is used by the OFL Agent to retrieve a Bound Image from the IDS for a specific TRE Instance. The INT4 is used for notifying the IDS about the status of the operations performed by the OFL. The INT2 interface defined in [INT2] allows the Image Owner to manage the Firmware and to control the Images flow from the Image Maker to the OFL Agent. The INT2 interface may be tunneled via the INT1 and INT7 interfaces. INT2 interface connect the IDS and the IOF Agent within an IOF of the Image Owner.
- The INT8 defined in [INT8] interface may be used for credentials as Authentication Token defined in [OFL] for binding Unbound Images to a TRE before or during the manufacturing of the OEM device. INT8 interface connect the IDS and the TMF Agent within a TMF of the TRE Maker.
- The INT10 defined in [INT10] interface may be used for downloading the Bound Images from the IDS before or during the Manufacturing of the OEM device. INT10 interface connect the IDS and the OMF Agent within an OMF of the OEM device Maker.

6.2.2 The OFL Agent Function Interface

The interfaces of the OFL Agent Function include the following:

- The INT5 interface is defined in [OFLE].
- The INT6 interface is use case dependent but the conveyor of meta-data is defined in [INT4].

6.3 The Actor Interfaces

The interfaces between Actors include the following:

- The INT1 interface is used by the IDS and the Image Maker to provision the components for Unbound Images and exchange meta-data for their management. The INT1 interface connects the IDS and the IMF Agent acting on behalf of the Image Maker.
- The INT7 interface may be used by the Image Owner for ordering Unbound Images to the Image Maker and managing the credentials to insert in the Firmware within the Unbound Images. The INT7 interface connects the IMF server acting on behalf of the Image Maker and the IOF Agent acting on behalf of the Image Owner.
- The INT9 interface may be used by the Firmware Maker for providing the Firmware to the Image Maker. The way the transfer is done (authentication, authorization, size, format of transfer...) is out of scope of this document.

6.4 OFL Security Protocol Interfaces

The Figure 6-2 details the interfaces supporting the OFL Security Protocol defined in [OFL].

Figure 6-2: OFL Security Protocol interfaces

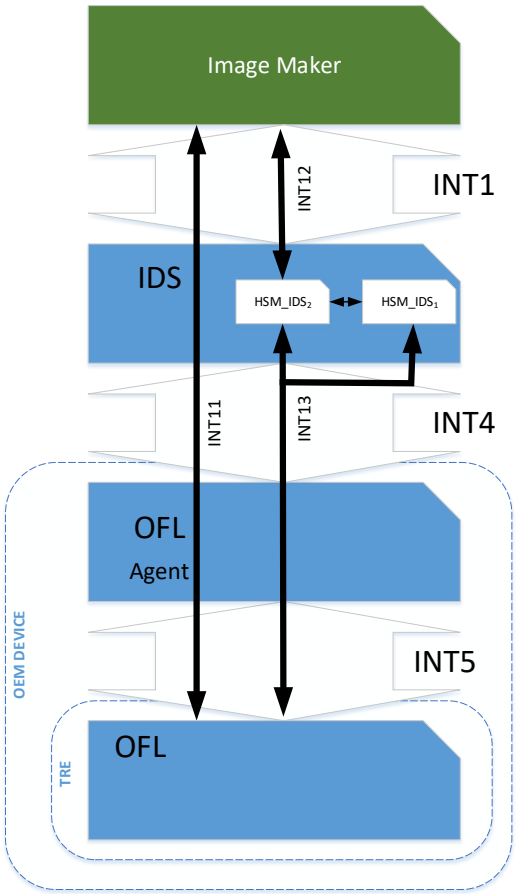


Figure 6-2 maps to Figure 5-2 defined in [OFL].

The INT12 interface shall be defined in a standard or in a specification if the INT1 is defined as a standard or a specification issued respectively from a SDO or from an Industry Organization. INT1 is a tunnel for INT12 and INT11.

The INT11 interface allows the transport of the encrypted Firmware tunneled within INT1, INT4 and INT5 interfaces and is defined in the section 5.5 in [OFL].

The INT13 interface allows the binding of the Image and is defined in section 4 in [OFL].

7 Annex A (Informative): Document history

The table below indicates changes that have been incorporated into the present document since it was created by SIMalliance.

Version	Date	Brief Description of Changes
V1.0.0	28/01/2019	1st Release of Document
V1.0.1	29/03/2019	Updated version with comment resolution before Publication
V1.0.2	08/04/2019	Updated version with sanity check and late comments resolution introduction
V1.0.3	22/04/2019	Publication after Board approval