TRUSTED CONNECTIVITY ALLIANCE

Image Deliver Server (IDS) to Open Firmware Loader (OFL) Agent Interfaces

Version 1.0.3

Published by simalliance now Trusted Connectivity Alliance

May 2019

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 v1.1	[VNP]
GPC_FST_141	GlobalPlatform Technology VPP - OFL VNP Extension	[OFLE]
GPC_FST_143	GlobalPlatform Technology VPP - Firmware Format v1.1	[VFF]
IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels, S. Bradner.	[RFC 2119]
ITU-T X.680 (11/2008)	Abstract Syntax Notation One (ASN.1): Specification of basic notation including Corrigendum 1 and 2	[X.680]
ITU-T X.690 (11/2008)	ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) including Corrigendum 1 and 2	[X.690]
RFC 1738	Uniform Resource Locators (URL)	[RFC 1738]
RFC 2818	HTTP Over TLS	[RFC 2818]
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace	[RFC 4122]
RFC 8446	The TLS Protocol – Version 1.3	[RFC 8446]
RFC 5280	Internet X.509 PKI Certificate and CRL Profile	[RFC 5280]
RFC 5758	RFC 5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA	[RFC 5758]
RFC 7027	Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)	[RFC 7027]
RFC 7159	IETF - The JavaScript Object Notation (JSON) Data Interchange Format	[RFC 7159]
RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2)	[RFC 7540]
SA OFL Ecosystem	SIMalliance OFL ecosystem V1.0.1	[OFL_ECO]

1.2 Informative References

No informative references are used in this document.

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

1.3 Abbreviations

Selected abbreviations and notations used in this document are included in Table 1-2.

Table 1-2: Abbreviations

Abbreviation	Meaning
ATK.IDS$_1$.ECKA	Defined in [OFL]
CERT.CI$_{AUTH}$.ECDSA	Certificate of the CI (Root) for the TLS server authentication.
CA	Certification Authority as defined in [RFC 5280].
CI	Certificate Issuer
MMI	Man Machine Interface
NA	Not Applicable
OFB	Other Functional Block
OFL	Open Firmware Loader
RFU	Reserved for Future Use
RO	Read-Only
RW	Read / Write
URI	Uniform Resource Identifier
URL	Uniform Resource locator
UUID	Universal Unique IDentifier version 5 or version 3 as defined in [RFC 4122]
VNP	VPP Network Protocol
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 (refer to [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 1-3 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 1-3.

Table 1-3: Terminology and Definitions

Term	Definition
Actor	Defined in [OFL_ECO].
Certification Path	Defined in [RFC 5280] in section 3.2.
Firmware	Defined in [OFL].
Firmware Loading	Defined in [OFL].
Firmware Update	Defined in [OFL].
Function	Defined in [OFL_ECO].
Gate	Defined in [VNP].
Image	Defined in [OFL_ECO].
Image Owner	Defined in [OFL].
Industry Organization	Defined in [OFL_ECO].
Multicast Bound Image	Defined in [OFL_ECO].
OFB	Defined in [OFL_ECO].
OFL Agent	Defined in [OFL].
Open Firmware Loader	Defined in [OFL].
Subscriber	Defined in [OFL_ECO].
TRE	Defined in [OFL].
TRE Instance	Instance of a TRE duly identified.
Unbound Image	Defined in [OFL_ECO].
Unicast Bound Image	Defined in [OFL_ECO].

2 Overview

2.1 Objectives

This specification details the interface between the IDS and the OFL Agent called INT4 in the Figure 2-1. The INT4 interface is part of the OFL ecosystem defined in [OFL_ECO].

This specification details the procedure for the OFL Agent to forward the Image components to the OFL service hosted in the Tamper Resistant Element (i.e. TRE) via an interface called INT5.

The Figure 2-1 illustrates an OFL ecosystem defining multiple interfaces between Actors and Functions and defines the scope of this specification.

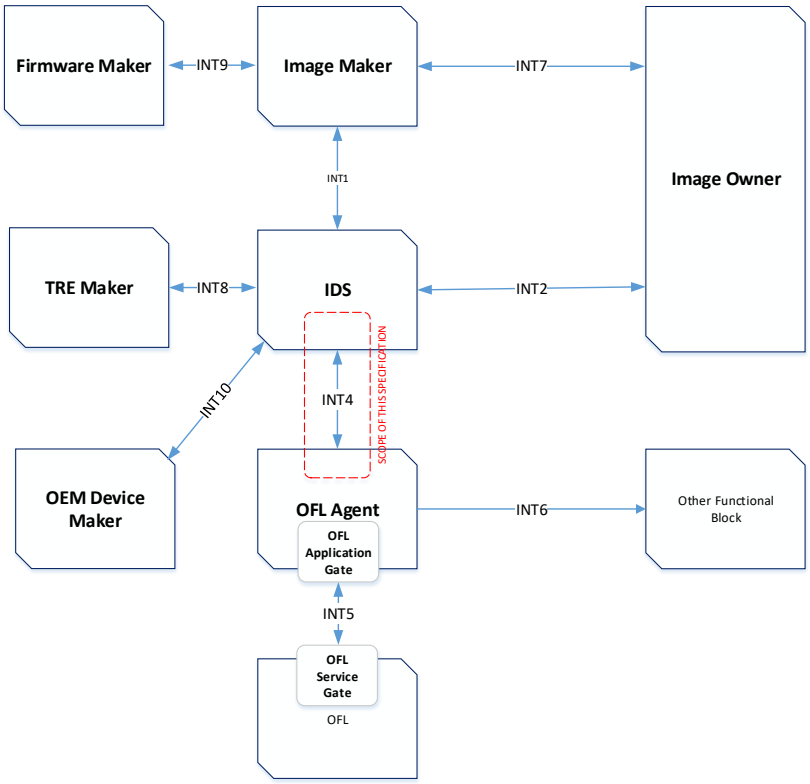
The INT4 interface provides the facilities for the OFL Agent to negotiate parameters with the IDS (e.g. multiple IDS Certificate Issuer [i.e. CI_{IDS}]). The negotiation of parameters is performed by the IDS:

- By getting the PART_NUMBER from OFL as defined in [OFL] and by deducing the capabilities of the OFL and the TRE. And/or;
- By getting this information through the INT4 interface from the metadata.

This specification is, thus, intended to be encapsulated or referenced in a document dedicated to a given context (e.g. mobile phone terminal).

The specification of the Functions are out of the scope for this document.

Figure 2-1: OFL communication ecosystem



As this specification is agnostic to the use case, additional metadata may be conveyed over the INT4 interface and routed to the other functional block via the INT6 interface.

The INT5 interface is defined in [OFLE].

The Other Functional Block (OFB) entity is use case dependent and is out of the scope of this document. The INT6 interface may perform the following actions, through the OFL Agent:

- Receive and send metadata from/to the IDS.
- Send metadata to the IDS.

INT1, INT2, INT6, INT7, INT8, INT9 and INT10 interfaces are out of the scope for this document.

3 INT4 Interface

3.1 Overview

The present section specifies the interface between the IDS and the OFL Agent. This interface is used by the OFL Agent to retrieve a Unicast Bound Image or a Multicast Bound Image from the IDS for a specific TRE. It is also used to notify the IDS about different steps of the life cycle of the Image or the Firmware it contains.

3.2 Transport Layer

3.2.1 Definition

The binding of the INT4 interface shall be performed over HTTP/2 as defined in RFC 7540 [RFC 7540] and TLS v1.3 as defined in RFC 8446 [RFC 8446]. The OFL Agent act as an HTTPS client and the IDS as an HTTPS server.

3.2.2 Requirements

The communication between the OFL Agent and the IDS shall be managed using messages and a HTTPS (Server Authentication is required) communication according to the below specification.

The Transport Layer mandates use of TLS v1.3 as defined in RFC 8446 [RFC 8446] as the minimal version for TLS connection.

The OFL Agent and the IDS shall use the TLS key exchange algorithm as defined in RFC 8446 [RFC 8446].

The following requirements shall be supported:

- Minimum Key Length Symmetric (AES) 128 bits, block size of 128 bits.
- Minimum Elliptic curve 256 bits length.
- Hashing for Digital signatures and hash-only applications SHA-256.

3.2.3 HTTP Header

3.2.3.1 HTTP Request

The HTTP request header shall have the following format:

```
<http-method> <URL> HTTP/<version>
Accept: <format>
User-Agent: <user-agent>
X-Admin-Protocol: sa/ofla/v<xx.yy>
Content-Type: <content Type>
Content-Length: <XXX>
CRLF
<content>
```

Where:

- **<version>**: shall be set to 2 as defined in [RFC 7540].
- **<http-method>**: shall be POST.
- **<URL>:** is the URL of the request.
- **<user-agent>**: shall contain at least sa-ofla.
- **<xx.yy>:** indicates the highest version of INT4 interface supported by the User-Agent. Where xx (two digits) is the major version and yy (two digits) is the minor version.
- **<format>:** shall be set to:
    - “application/json” when JSON message format is used.

  - “application/sa-ofla-asn1” when ASN.1 DER message format is used.
- **<content type>** shall be set to:
  - “application/json” when JSON message is used.
  - “application/sa-ofla-asn1” when ASN.1 DER message is used.
- **<XXX>:** The length of the HTTP request content (i.e. <content>) is defined in bytes (8-bit bytes) and shall be present if required.

The request <URL> is compliant with RFC 1738 and is defined as follows:

https://<host>:<port>/<url-path>?< searchpart>

Where:

- **https**: http scheme as defined in the section 3 in [RFC 1738] with TLS support.
- **<host>**: as defined in the section 3.1 in [RFC 1738].
- **<port>**: as defined in the section 3.1 in [RFC 1738].
- **<url-path>**: as defined in the section 3.1 in [RFC 1738].
- **<searchpart>**: the searchpart contains the PART_NUMBER defined in [OFL]. This <searchpart> is mandatory.

The <host>, <port> and <url-path> parameters are out of the scope for this specification. It shall be retrieved by OFL Agent from any means, for example:

  - From a dynamic external source like the QR code used for the Image generation,
  - Hard-coded in the Agent if the agent is dedicated to a specific IDS,
  - Retrieved from a device setting or menu,
  - Any other means.

3.2.3.2 HTTP Response

The HTTP response header shall have the following format:

```
HTTP/<version> <error-code>
Content-Type: <content type>
Content-Length: <XXX>
CRLF
<content>
```

Where:

- **<version>**: shall be set to 2 as defined in [RFC 7540].
- **<error-code>:** as defined in the section 3.2.3.1.
- **<content type>** shall be set to:
  - “application/json” when JSON message is conveyed in the HTPP request content (i.e. <content>).
  - “application/sa-ofla-asn1” when ASN.1 DER message is conveyed in the HTPP request content <content>.
- **<XXX>:** The length of the HTTP message content (i.e. <content>) is defined in bytes (8-bit bytes).
- **<content>**: contains the OFL message according to a format defined in <content type>.

3.2.3.3 HTTP response codes

The following response codes <error-code> from the IDS are defined hereunder.

Table 3-1: HTTP response codes

Code	Comment
200	OK **regardless whether the IDS Function response is an error or a success**
204	“No content” – Success. Other status codes '2xx' SHALL not be used by the IDS
1xx	Information may be used by the IDS
3xx	Redirection may be used by the IDS
4xx	HTTP client error may be used by the IDS
5xx	HTTP server error may be used by the IDS

3.2.4 Identification/Authentication/Authorization

The authentication of the sending entity of a JSON or ASN.1 DER message shall rely on the Transport Layer Security (using TLS Certificate of the sender). The authentication procedure is defined in [RFC 8446].

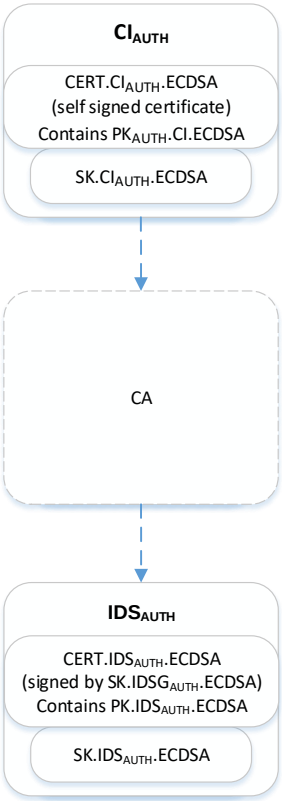
3.2.4.1 Certificate

The X509 Certificate shall follow the RFC 5280 version 3.

3.2.4.2 Certification Path

The Figure 3-1 illustrates the Certification Path supporting the server authentication related to the INT4 interface. The number of CA is context dependent.

Figure 3-1: Certification Path for the INT4 interface



The PK Infrastructure shall be based on the RFC 5758 requires the following long term keys:

Table 3-2: Long term authentication keys

PK Node	Name of Key	Description
CI$_{AUTH}$	PK.CI$_{AUTH}$.ECDSA	Public key of the CI$_{AUTH}$ in CERT.CI$_{AUTH}$.ECDSA for the server authentication
	SK.CI$_{AUTH}$.ECDSA	Private Key of the CI$_{AUTH}$ for the server authentication
CA		Any number of CA
IDS$_{AUTH}$	PK.IDS$_{AUTH}$.ECDSA	Public key of the IDS in CERT.IDS$_{AUTH}$.ECDSA.
	SK.IDS$_{AUTH}$.ECDSA	Private Key of the IDS$_{AUTH}$

3.2.5 Integrity

The integrity of the message shall exclusively rely on the Transport Layer Security (TLS) as defined in [RFC 8446] section 9.1.

3.2.6 Confidentiality

The confidentiality of the message shall exclusively rely on the Transport Layer Security (TLS) as defined in [RFC 8446] section 9.1.

3.3 Presentation Layer

Two formats of messages shall be defined for this interface:

- JSON: this format, as defined in [RFC 7159], aims at facilitating the implementation of OFL Agents in advanced devices for which interpretation of JSON is natural and native.
- ASN.1 DER: this binary format as defined in [X.690] is generated from an ASN.1 description defined in [X.680]. This format minimises the volume of data exchanged, as such, it can be used by devices that have constraint memory.

Thus, the choice is left to the device maker to support one format or the other, however the same format shall be used for all the messages of a given implementation. More specifically, when a format is used by the OFL Agent in a request, the same format shall be used by IDS in the corresponding response.

3.4 Application Layer

3.4.1 Overview

This API shall provide the following methods:

- **GetCertificate**: This method can be used by the OFL Agent to retrieve from the IDS the Certificates to be used to get the session materials generated by the TRE through INT5. This method is useless if the OFL Agent gets the IDS certificates by other means.
- **GetImage**: This method can be used by the OFL Agent to request the binding of an Unbound Image with the TRE Credentials and the delivery of the Unicast Bound Image, therefore generated for the corresponding TRE. The Unicast Bound Image is delivered in the response to this method.
- **GetImageFromRef**: This method can be used by the OFL Agent to request the unicast delivery of Bound Image(s) for the corresponding TRE. The Unicast Bound Image(s) is/are retrieved from its reference ID_TRANSAC[2] as defined in [OFL]. The Bound Image(s) is/are delivered in the response to this method.
- **GetMulticastImage**: This method can be used by the OFL Agent to request the multicast delivery of a Multicast Bound Image for the corresponding TRE. The Multicast Bound Image is retrieved from its group identifier GROUP_ID. The Multicast Bound Image(s) is/are delivered in the response to this method.
- **NotifyLoadStatus**: This method is used to notify the IDS that a Unicast or a Multicast Bound Image was successfully loaded.
- **NotifyDeleteStatus**: This method is used to notify the IDS that a Firmware was deleted.

3.4.2 Elements of Information

The following elements of information definitions are used in the INT4 interface.

```
-- ASN1START
INT4Interface {joint-iso-itu-t(2) international-organizations(23) simalliance(143) ofl(2) int4(4)}
DEFINITIONS
AUTOMATIC TAGS
EXTENSIBILITY IMPLIED
::= BEGIN
EXPORTS ALL; --

Version                                ::= [PRIVATE 1]INTEGER  {  v1(0)   }
                                       --Version of the interface
Status                                 ::= INTEGER  (1..255)
                                       --Status of an operation
```

[2] ID_TRANSAC should be renamed as ISID (Image Session Identifier) in the future release of the OFL specification.

```
ok Status                               ::= 0
                                        --Operation successfully executed
nok Status                              ::= 1
                                        -- Request badly formated
unknownCI Status                        ::= 2
                                        -- The requested OFL Certification Path is not supported
unknownPN Status                        ::= 3
                                        -- The requested Part Number is not supported
max-metadata                            INTEGER                             ::= 64
max-size-metadata INTEGER               ::= 8196
UUID                                    ::= OCTET STRING  (SIZE(16))
ChangeSegmentParameter                  ::= OCTET STRING
LoadSegmentParameter                    ::= OCTET STRING

VersionOFL                              ::= [PRIVATE 2]OCTET STRING  (SIZE(2))
                                        --Major and Minor version of the OFL implementation
FirmwareID                              ::= [PRIVATE 3]UUID
                                        --Firmware Identifier (see Public UUID of the Firmware)
ImageMakerID                            ::= [PRIVATE 4]UUID
                                        --Image Maker Identifier
ImageOwnerID                            ::= [PRIVATE 5]UUID
                                        --Image Owner Identifier
FirmwareFamilyID                        ::= [PRIVATE 6]UUID
                                        --Firmware Family Identifier
NumberSegment                           ::= [PRIVATE 7]INTEGER (0..65535)
DoOperateParameter                      ::= [PRIVATE 8]OCTET STRING
                                        --Parameter for the OFL_DO_OPERATE command
ChangeSegmentParameters                 ::= [PRIVATE 9]SEQUENCE OF ChangeSegmentParameter
                                        -- Parameters for the OFL_CHANGE_SEGMENT command
LoadSegmentParameters                   ::= [PRIVATE 10]SEQUENCE OF LoadSegmentParameter
                                        -- Parameters for the OFL_LOAD_SEGMENT command
Metadata                                ::= [PRIVATE 11]SEQUENCE (SIZE(1..max-metadata))OF MetaDatum  -
                                        -Any metadata
ImageSessionID                          ::= [PRIVATE 12]OCTET STRING (SIZE(16))
                                        --ID_TRANSAC as defined in OFL
ImageSessionIDList                      ::= [PRIVATE 13]OCTET STRING
                                        --Content of the LIST_TRANSAC register as defined in OFL
GroupIDList                             ::= [PRIVATE 14]OCTET STRING
                                        --Content of the GROUP_ID_LIST register as defined in OFL

MetaDatum                               ::=  SEQUENCE
{
aTypeDatum         OBJECT IDENTIFIER,
aData              OCTET STRING (SIZE(0..max-size-metadata)) OPTIONAL
}

TreCredentialsParameter                 ::= OCTET STRING
                                        --TRE credentials from the OFL interface
Certificate                             ::= [PRIVATE 15]OCTET STRING
                                        --Represents the X509v3 Certificate
Certificates                            ::=SET OF Certificate
-- ASN1STOP
```

The following data definition shall apply to the INT4 interface.

```
-- ASN1START

id-int4 OBJECT IDENTIFIER               ::=    {joint-iso-itu-t(2)    international-organizations(23)
simalliance(143) ofl(2) int4(4)}
AtkOFLDoOperate                        ::= [PRIVATE 16]OCTET STRING (SIZE(32)) --Token for proofing the
successfull OFL_DO_OPERATE command execution
AtkOFLDeleteSession            ::=  [PRIVATE  17]OCTET  STRING  (SIZE(32))  --Token  for  proofing  the
successfull Firmware session deletion
GroupID                                 ::=[PRIVATE 18] UUID
                                        -- Group Identifier as defined in [OFL]
-- ASN1STOP
```

3.4.3 Unicast/Multicast Bound Image structure

The structure of the Unicast/Multicast Bound Image is defined as below for the ASN.1 format:

```
-- ASN1START
BoundImage                              ::= [PRIVATE 19] SEQUENCE
{
```

```
aFirmwareID                             FirmwareID,
                                        --Public Firmware Identifier
aImageOwnerID                            ImageOwnerID,
                                        --Image Owner Identifier
aFirmwareFamilyID                       FirmwareFamilyID,
                                        --Fimware Familly Identifier
aNumberSegment                          NumberSegment,
                                        --Number of segments in the image
aFirmwareSize                           INTEGER,
                                        --Sum of all data segment size containing non-volatile data/size
of the Memory Partition
aDoOperateParameter                     DoOperateParameter,
                                        --Parameter for the OFL_DO_OPERATE command

aImageSessionID                         ImageSessionID OPTIONAL,
                                        --Image Session identifier as defined in [OFL].
aGroupID                                GroupID OPTIONAL,
                                        --Fimware Familly Identifier

aImageMakerID                           ImageMakerID OPTIONAL,
                                        --Image Maker Identifier
aMetaDataImage                          Metadata OPTIONAL,
                                        -- metadata of the image from the Image Maker
aChangeSegmentParameters                ChangeSegmentParameters OPTIONAL,
                                        --List of parameter for the OFL_CHANGE_SEGMENT
aLoadSegmentParameters                  LoadSegmentParameters OPTIONAL
                                        --List of parameter for the OFL_LOAD_SEGMENT
}
-- ASN1STOP
```

And as follows for the JSON format:

```
{
"aFirmwareID":"00000000000000000000000000000000",
"aImageOwnerID":"00000000000000000000000000000000",
"aFirmwareFamilyID":"00000000000000000000000000000000",
"aNumberSegment":0,
"aFirmwareSize":0,
"aDoOperateParameter":"00",
"aImageSessionID":"00000000000000000000000000000000",
"aGroupID": "00000000000000000000000000000000",
"aImageMakerID":"00000000000000000000000000000000",
"aMetaData":[
    {
    "aTypeDatum":"0.0",
    "aData": "0"
    }
    ],
"aChangeSegmentParameters":[
    "00"
    ],
"aLoadSegmentParameters":[
    "00"
    ]
}
```

The structure of the Unicast Bound Image and the Multicast Bound Image differs by two fields: aImageSessionID and aGroupID.

Where:

- **aFirmwareID** : The Public Firmware Identifier. UUID[I] as defined in [OFL].
- **aImageOwnerID** : The Image Owner Identifier (UUID) as defined in [OFL].
- **aFirmwareFamilyID** : The Firmware Family Identifier as defined in [OFL].
- **aNumberSegment** : The Number of segments in the Image as defined in [OFL].
- **aFirmwareSize**: The Sum of all NVM data segment size/size of the Memory Partition as defined in [VCI].
- **aDoOperateParameter**: The Parameter for the OFL_DO_OPERATE command. For the JSON interface this parameter is encoded in base64.

- **aImageMakerID**: The Image Maker Identifier (UUID).
- **aImageSessionID**: The Image Session Identifier (ID_TRANSAC) as defined in [OFL). Absent for Multicast Bound Image.
- **aGroupID**: The Group Identifier (GROUP_ID) as defined in [OFL). Absent for Unicast Bound Image.

- **aMetaData**: The metadata of the Image.
- **aChangeSegmentParameters**: The List of parameters for the OFL_CHANGE_SEGMENT command defined in [OFL]. The number of elements in this list is equal to aNumberSegment. The parameters in this list for JSON are encoded in base64.
- **aLoadSegmentParameters**: The List of parameters for the OFL_LOAD_SEGMENT commands defined in [OFL]. The number of elements in this list is equal to aNumberSegment. The parameters in this list for JSON are encoded in base64.

3.4.4 GetCertificate

3.4.4.1 Overview

This function allows the OFL Agent to retrieve the Certification Path ended by the CERT.IDS$_1$.ECKA Certificate from the IDS.

3.4.4.2 Request

3.4.4.2.1 JSON Interface

The JSON body schema of the GetCertificateRequest is described hereunder.

```
{
        "i4:getCertificateRequest": {
                "i4:aMetaDataRequest": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aVersion": "v1",
                "i4:aVersionOFL": "aa"
        }
}
```

3.4.4.2.2 ASN.1 Interface

The binary body schema of the GetCertificateRequest command is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetCertificateRequest   ::= [APPLICATION 1] SEQUENCE
{
aVersion                                Version DEFAULT v1,
aVersionOFL                             VersionOFL,
                                        --Version OFL implemented
aMetaDataRequest                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.4.2.3 Parameters

The parameters used in the application layer element defined in the section 3.4.4.2.1 and 3.4.4.2.2 are as follows:

- **aVersion**: The Version of the interface.
- **aVersionOFL**: The Major and Minor version of the OFL as defined in [OFL]. This information can be retrieved from the INT5 interface.
- **aMetaDataRequest**: Any metadata from the OFL Agent to the IDS.
    - **aTypeDatum**: The Identifier of the metadata.
    - **aData**: The metadata.

3.4.4.3 Response

3.4.4.3.1 JSON Interface

In case of successful GetCertificateRequest command, the JSON body schema of the response shall return the CERT.IDS$_1$.ECKA certificate as described below:

```
{
        "i4:getCertificateResponse": {
                "i4:aCertificates": [
                        "a"
                ],
                "i4:aMetaDataReponse": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aStatus": 1
        }
}
```

3.4.4.3.2 ASN.1 Interface

In case of successful GetCertificateRequest command, the binary body schema of the response is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetCertificateResponse ::= [APPLICATION 2] SEQUENCE
{
aStatus                                 Status,
                                        --Status
aCertificates                           Certificates,
                                        --  X.509  Certification  Path  ended  by  the  CERT.IDS1.ECKA
Certificate
aMetaDataReponse                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.4.3.3 Parameters

The parameters used in the application layer element defined in the section 3.4.4.3.1 and 3.4.4.3.2 are as follows:

- **aStatus:** The Status of the response. The IDS shall answer with a status according to section 3.4.2.
- **aCertificates**: The Certification Path ended by the CERT.IDS$_1$.ECKA Certificate as defined in [OFL]. This binary format is encoded in base64.
- **aMetaDataResponse**: Any metadata from the IDS to the OFL Agent:
    - **aTypeDatum**: The Identifier of the metadata.

- **aData**: The metadata.

3.4.5 GetImage

3.4.5.1 Overview

This function allows the OFL Agent to retrieve the Unicast Bound Image from the IDS. The TRE credentials shall be retrieved from the INT5 interface. Prior to getting the TRE credentials, the IDS credentials shall be provided to the TRE via the INT5 interface. The IDS credentials (IDS_CREDENTIAL_PARAMETER parameters) are defined in [OFL] and shall be built by the OFL Agent:The IDS Credentials may be retrieved by any means (e.g. NFC NDEF, QR-CODE, Push…) from the OFB or the OFL Agent.

- Certification Path ended by the CERT.IDS$_1$.ECKA Certificate which may be retrieved by any means (e.g. NFC NDEF, QR-CODE, Push…) by the OFB or the OFL Agent or from the IDS by using the GetCertificateRequest command defined in section 3.4.4.

3.4.5.2 Request

3.4.5.2.1 JSON interface

The JSON body schema of the GetImageRequest command is described below:

```
{
        "i4:getImageRequest": {
                "i4:aMetaDataRequest": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aTreCredentialsParameter": "a",
                "i4:aVersion": "v1",
                "i4:aVersionOFL": "aa"
        }
}
```

3.4.5.2.2 ASN.1 Interface

The binary body schema of the GetImageRequest command is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetImageRequest   ::= [APPLICATION 3] SEQUENCE
{
aVersion                                Version DEFAULT v1,
aVersionOFL                             VersionOFL,
                                        --Version OFL implemented
aTreCredentialsParameter                TreCredentialsParameter,
                                        --TRE credentials from the OFL interface
aMetaDataRequest                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.5.2.3 Parameters

The parameters used in the application layer element defined in the section 3.4.5.2.1 and 3.4.5.2.2 are as follows:

- **aVersion**: The Version of the interface.

- **aVersionOFL**: The Major and Minor version of the OFL as defined in [OFL]. This information can be retrieved from the INT5 interface.
- **aTreCredentialsParameter**: The TRE credentials retrieved from the OFL interface.
- **aMetaDataRequest**: Any metadata from the OFL Agent to the IDS.

3.4.5.3 Response

3.4.5.3.1 JSON Interface

In case of successful GetImageRequest command, the JSON body schema of the response is described below:

```
{
"i4:getImageResponse": {
                "i4:aMetaDataReponse": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aResult": {
                        "i4:aBoundImage": {
                                "i4:aChangeSegmentParameters": [
                                        "a"
                                ],
                                "i4:aDoOperateParameter": "a",
                                "i4:aFirmwareFamilyID": "aaaaaaaaaaaaaaaa",
                                "i4:aFirmwareID": "aaaaaaaaaaaaaaaa",
                                "i4:aFirmwareSize": 1,
                                "i4:aImageMakerID": "aaaaaaaaaaaaaaaa",
                                "i4:aImageOwnerID": "aaaaaaaaaaaaaaaa",
                                "i4:aLoadSegmentParameters": [
                                        "a"
                                ],
                                "i4:aMetaDataImage": {
                                        "i4:MetaDatum": [
                                                {
                                                        "i4:aData": "a",
                                                        "i4:aTypeDatum": "0.0.0"
                                                }
                                        ]
                                },
                                "i4:aNumberSegment": 0,
                                "i4:aImageSessionID": "aaaaaaaaaaaaaaaa"
                        },
                        "i4:aImageSessionID": "aaaaaaaaaaaaaaaa"
                },
                "i4:aStatus": 1
        }
}
```

3.4.5.3.2 ASN.1 Interface

In case of successful GetImageRequest command, the binary body schema of the response is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetImageResponse ::= [APPLICATION 4] SEQUENCE
{
aStatus                                 Status,
                                        --Status
aResult                                 CHOICE
{
aBoundImage                             BoundImage ,
                                        --Unicast Bound image
```

```
aImageSessionID                         ImageSessionID
                                        --Image SessionID
} OPTIONAL,
aMetaDataReponse                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.5.3.3 Parameters

The parameters used in the application layer element defined in the section 3.4.5.3.1 and 3.4.5.3.2 are as follows:

- **aStatus:** The Status of the response. The IDS shall answer with a status according to section 3.4.2.
- **aResult :** a Unicast Bound Image:
  - **aFirmwareID**: The Public Firmware Identifier.
  - **aImageSessionID**: The Image Session Identifier (ID_TRANSAC).
  - **aImageOwnerID**: The Image Owner Identifier.
  - **aFirmwareFamilyID**: The Firmware Family Identifier.
  - **aNumberSegment**: The Number of segments in the Image.
  - **aFirmwareSize**: The Sum of all NVM data segment size/size of the Memory Partition.
  - **aDoOperateParameter**: The Parameter for the OFL_DO_OPERATE command.
  - **aImageMakerID**: The Image Maker Identifier.
  - **aChangeSegmentParameters**: The List of parameters for the OFL_CHANGE_SEGMENT.
  - **aLoadSegmentParameters**: The List of parameters for the OFL_LOAD_SEGMENT.
  - **aMetaDataImage**: Any metadata of the Unicast Bound Image from the Image Maker to the OFL Agent:
    - **aTypeDatum**: The Identifier of the metadata.
    - **aData**: The metadata.
- **aMetaDataResponse**: Any metadata from the IDS to the OFL Agent.
  - **aTypeDatum**: The Identifier of the metadata.
  - **aData**: The metadata.

3.4.6 GetImageFromRef

3.4.6.1 Overview

The function allows the OFL Agent to retrieve one or more Images from the IDS referenced by their Image Session identifier (ID_TRANSAC) as defined in [OFL].

3.4.6.2 Request

3.4.6.2.1 JSON Interface

The JSON body schema of the GetImageFromRefRequest command is described below:

```
{
        "i4:getImageFromRefRequest": {
                "i4:aMetaDataRequest": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
```

```
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aImageSessionIDList": "a",
                "i4:aVersion": "v1",
                "i4:aVersionOFL": "aa"
        }
}
```


3.4.6.2.2 ASN.1 Interface

The binary body schema of the GetImageFromRefRequest command is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetImageFromRefRequest   ::= [APPLICATION 5] SEQUENCE
{
aVersion                                Version DEFAULT v1,
aVersionOFL                             VersionOFL ,
                                         --Version OFL implemented
aImageSessionIDList                     ImageSessionIDList,
aMetaDataRequest                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.6.2.3 Parameters

The parameters used in the application layer element defined in the section 3.4.6.2.1 and 3.4.6.2.2 are as follows:

- **aVersion**: The Version of the interface.
- **aVersionOFL**: The Major and Minor version of the OFL as defined in [OFL]. This information can be retrieved from the INT5 interface.
- **aIdImageSessionIDList**: The content of LIST_TRANSAC as defined in [OFL] and retrieved thanks to the INT5 interface. For the JSON interface, this parameter is encoded in base64.
- **aMetaDataRequest**: Any metadata from the OFL Agent to the IDS:
    - **aTypeDatum**: The Identifier of the metadata.
    - **aData**: The metadata.

3.4.6.3 Response

3.4.6.3.1 JSON Interface

In case of successful GetImageFromRefRequest command, the JSON body schema of the response is described below:


```
{
"i4:getImageFromRefResponse": {
                "i4:aBoundImages": {
                        "i4:BoundImage": [
                                {
                                        "i4:aChangeSegmentParameters": [
                                                "a"
                                        ],
                                        "i4:aDoOperateParameter": "a",
                                        "i4:aFirmwareFamilyID": "aaaaaaaaaaaaaaaa",
                                        "i4:aFirmwareID": "aaaaaaaaaaaaaaaa",
                                        "i4:aFirmwareSize": 1,
                                        "i4:aImageMakerID": "aaaaaaaaaaaaaaaa",
                                        "i4:aImageOwnerID": "aaaaaaaaaaaaaaaa",
                                        "i4:aLoadSegmentParameters": [
                                                "a"
```

```
                                        ],
                                        "i4:aMetaDataImage": {
                                                "i4:MetaDatum": [
                                                        {
                                                                "i4:aData": "a",
                                                                "i4:aTypeDatum": "0.0.0"
                                                        }
                                                ]
                                        },
                                        "i4:aNumberSegment": 0,
                                        "i4:aImageSessionID": "aaaaaaaaaaaaaaaa"
                                }
                        ]
                },
                "i4:aMetaDataReponse": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aData": "a",
                                        "i4:aTypeDatum": "0.0.0"
                                }
                        ]
                },
                "i4:aStatus": 1
        }
}
```


3.4.6.3.2 ASN.1 Interface

In case of successful GetImageFromRefRequest command, the binary body schema of the response is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetImageFromRefResponse ::= [APPLICATION 6] SEQUENCE
{
aStatus                                 Status,
                                        --Status
aBoundImages                            SEQUENCE OF                     BoundImage OPTIONAL,
                                        --Array of Unicast Bound image
aMetaDataReponse                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.6.3.3 Parameters

The parameters used in the application layer element defined in the section 3.4.6.3.1 and 3.4.6.3.2 are as follows:

- **aStatus:** The Status of the response. The IDS shall answer with a status according to section 3.4.2.
- **aBoundImages**: The array of Unicast Bound Images according to section 3.4.2.
- **aMetaDataResponse**: Any metadata from the IDS to the OFL Agent:
  - **aTypeDatum**: The Identifier of the metadata.
  - **aData**: The metadata.

3.4.7 GetMulticastImage

3.4.7.1 Overview

The function allows the OFL Agent to retrieve one or more Multicast Bound Images from the IDS referenced by their group identifier (GROUP_ID) as defined in [OFL].

The GetMulticastImageRequest command is supported according to the procedure defined in section 4.3.5 in [OFL]. This command may be used by the OFL Agent.

3.4.7.2 Request

3.4.7.2.1 JSON Interface

The JSON body schema of the GetMulticastImageRequest is described below:

```
{
        "i4:getMulticastImageRequest": {
                "i4:aGroupIDList": "a",
                "i4:aMetaDataRequest": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aVersion": "v1",
                "i4:aVersionOFL": "aa"
        }
}
```

3.4.7.2.2 ASN.1 Interface

The binary body schema of the GetMulticastImageRequest command is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
 GetMulticastImageRequest              ::= [APPLICATION 7] SEQUENCE
{
aVersion                               Version DEFAULT v1,
aVersionOFL                            VersionOFL,
                                       --Version OFL implemented
aGroupIDList                           GroupIDList,
aMetaDataRequest                       Metadata OPTIONAL
                                       --Any metadata
}
-- ASN1STOP
```

3.4.7.2.3 Parameters

The parameters used in the application layer element defined in the section 3.4.7.2.1 and 3.4.7.2.2 are as follows:

- **aVersion**: The Version of the interface.
- **aVersionOFL**: The Major and Minor version of the OFL as defined in [OFL]. This information can be retrieved from the INT5 interface.
- **aGroupIDList**: The list of the Firmware Group Identifier as defined in [OFL] from INT5 interface. For the JSON interface this parameter is encoded in base64.
- **aMetaDataRequest**: Any metadata from the OFL Agent to the IDS:
    - **aTypeDatum**: The Identifier of the metadata.
    - **aData**: The metadata.

3.4.7.3 Response

3.4.7.3.1 JSON Interface

In case of successful GetMulticastImageRequest command, the JSON body schema of the response is described below:

```
{
        "i4:getMulticastImageResponse": {
                "i4:aBoundImages": {
                        "i4:BoundImage": [
                                {
                                        "i4:aChangeSegmentParameters": [
                                                "a"
                                        ],
                                        "i4:aDoOperateParameter": "a",
                                        "i4:aFirmwareFamilyID": "aaaaaaaaaaaaaaaa",
                                        "i4:aFirmwareID": "aaaaaaaaaaaaaaaa",
                                        "i4:aFirmwareSize": 1,
                                        "i4:aImageMakerID": "aaaaaaaaaaaaaaaa",
                                        "i4:aImageOwnerID": "aaaaaaaaaaaaaaaa",
                                        "i4:aLoadSegmentParameters": [
                                                "a"
                                        ],
                                        "i4:aMetaDataImage": {
                                                "i4:MetaDatum": [
                                                        {
                                                                "i4:aData": "a",
                                                                "i4:aTypeDatum": "0.0.0"
                                                        }
                                                ]
                                        },
                                        "i4:aNumberSegment": 0,
                                        "i4:aImageSessionID": "aaaaaaaaaaaaaaaa"
                                }
                        ]
                },
                "i4:aMetaDataReponse": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aData": "a",
                                        "i4:aTypeDatum": "0.0.0"
                                }
                        ]
                },
                "i4:aStatus": 1
        }
}
```


3.4.7.3.2 ASN.1 Interface

In case of successful GetMulticastImageRequest command, the binary body schema of the response is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
GetMulticastImageResponse ::= [APPLICATION 8] SEQUENCE
{
aStatus                                 Status,
                                        --Status
aBoundImages                            SEQUENCE OF BoundImage OPTIONAL,
                                        --Array of Multicast Bound images
aMetaDataReponse                        Metadata OPTIONAL
                                        --Any metadata
}
-- ASN1STOP
```

3.4.7.3.3 Parameters

The parameters used in the application layer element defined in the section 3.4.7.3.1 and 3.4.7.3.2 are as follows:

- **aStatus:** The Status of the response. The IDS shall answer with a status according to section 3.4.2.
- **aMetaDataResponse**: Any metadata from the IDS to the OFL Agent:
  - **aTypeDatum**: The Identifier of the metadata.
  - **aData**: The metadata.

3.4.8 NotifyLoadStatus

3.4.8.1 Overview

The function allows the OFL Agent to notify the IDS about an image loading status.

3.4.8.2 JSON Interface

The JSON body schema of the NotifyLoadStatus request is described below:

```
{
        "i4:notifyLoadStatus": {
                "i4:aAtkOFLDoOperate": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa",
                "i4:aFirmwareID": "aaaaaaaaaaaaaaaa",
                "i4:aImageMakerID": "aaaaaaaaaaaaaaaa",
                "i4:aMetaDataNotification": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aStatus": 1,
                "i4:aVersion": "v1",
                "i4:aVersionOFL": "aa"
        }
}
```

3.4.8.3 ASN.1 Interface

The binary body schema of the NotifyLoadStatus request is the result of DER of the ASN.1 description hereunder:

```
-- ASN1START
NotifyLoadStatus ::= [APPLICATION 9]SEQUENCE
{
aVersion                                Version DEFAULT v1,
aVersionOFL                             VersionOFL,
                                        --Version OFL implemented
aFirmwareID                             FirmwareID,
                                        --Public Firmware Identifier
aImageMakerID                           ImageMakerID,
                                        --Image Maker Identifier
aStatus                                 Status,
                                        --Status
...,
aAtkOFLDoOperate                        AtkOFLDoOperate OPTIONAL,
aMetaDataNotification                   Metadata OPTIONAL
                                        --Any metadata
                                        }
-- ASN1STOP
```

3.4.8.4 Parameters

The parameters used in the application layer element defined in the section 3.4.7.3.1 and 3.4.7.3.2 are :

- **aVersion**: The Version of the interface.
- **aVersionOFL**: The Major and Minor version of the OFL as defined in [OFL]. This information can be retrieved from the INT5 interface.
- **aFirmwareID**: The Public Firmware Identifier.
- **aImageMakerID**: The Image Maker Identifier.
- **aStatus**: The Status of the operation. The OFL Agent shall answer ok if the OFL operation is successful.

- **aAtkOFLDoOperate**: The Evidence, as defined in the section 4.3.3 in [OFL], that the loading operation is successful. This information can be retrieved from the INT5 interface.
- **aMetaDataNotification**: Any metadata from the OFL Agent to the IDS.

3.4.9 NotifyDeleteStatus

3.4.9.1 Overview

The function allows the OFL Agent to notify the IDS that a Firmware was deleted. This request can only be sent after a local deletion of the Firmware by using the INT5 interface.

3.4.9.2 JSON request

The JSON body schema of the request is described below:

```
{
        "i4:notifyDeleteStatus": {
                "i4:aAtkOFLDeleteSession": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa",
                "i4:aFirmwareID": "aaaaaaaaaaaaaaaa",
                "i4:aImageMakerID": "aaaaaaaaaaaaaaaa",
                "i4:aMetaDataNotification": {
                        "i4:MetaDatum": [
                                {
                                        "i4:aTypeDatum":"0.0",
                                        "i4:aData": "0"
                                }
                        ]
                },
                "i4:aStatus": 1,
                "i4:aVersion": "v1",
                "i4:aVersionOFL": "aa"
        }
}
```

3.4.9.3 ASN.1 Interface

The Binary body schema of the request is the result of DER of the ASN.1 description hereunder.

```
-- ASN1START
NotifyDeleteStatus ::= [APPLICATION 10] SEQUENCE
{
aVersion                                Version DEFAULT v1,
aVersionOFL                             VersionOFL,
                                         --Version OFL implemented
aFirmwareID                             FirmwareID,
                                        --Public Firmware Identifier
aImageMakerID                           ImageMakerID,
                                        --Image Maker Identifier
aStatus                                 Status,
                                        --Status
aAtkOFLDeleteSession                    AtkOFLDeleteSession OPTIONAL,
aMetaDataNotification                   Metadata OPTIONAL
                                        --Any metadata
}

-- ASN1STOP
```

3.4.9.4 Parameters

The parameters used in the application layer element defined in the section 3.4.7.3.1 and 3.4.7.3.2 are

- **aVersion**: The Version of the interface.
- **aVersionOFL**: The Major and Minor version of the OFL as defined in [OFL]. This information can be retrieved from the INT5 interface.
- **aFirmwareID**: The Public Firmware Identifier as defined in [OFL].

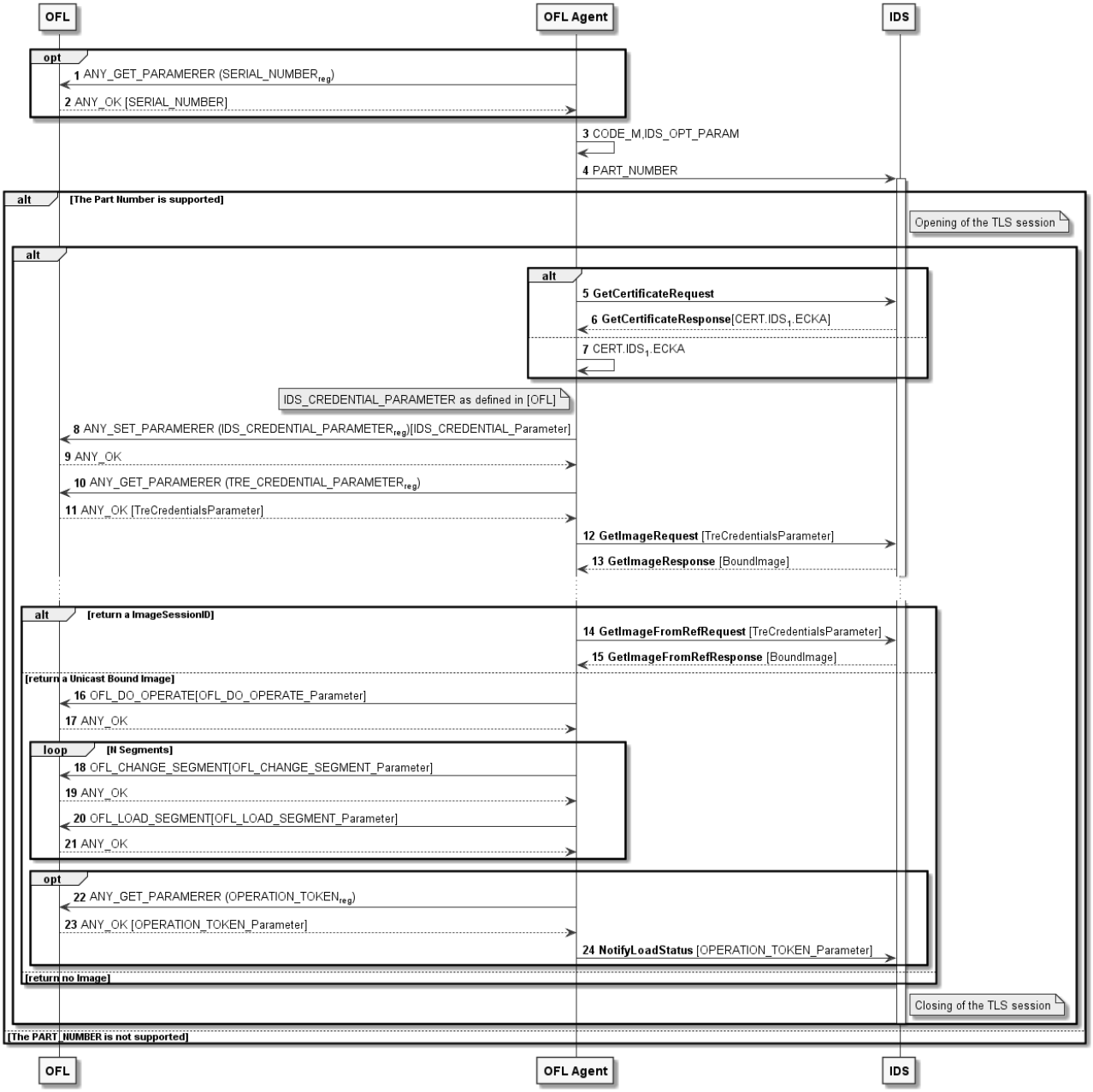
- **aImageMakerID**: The Image Maker Identifier as defined in [OFL].
- **aStatus**: The Status of the operation. The OFL Agent shall answer ok when the OFL operation is successful.
- **aAtkOFLDeleteSession**: The Evidence, as defined in the section 4.3.3 in [OFL], that the deletion of the Firmware is successful. This information can be retrieved from the INT5 interface.
- **aMetaDataNotification**: Any metadata.

4 ANNEX A (Informative): Procedures

4.1 Unicast Bound Image Loading procedure

The Figure 4-1 illustrates the procedure for a Unicast Bound Image Loading. This procedure occurs for any unicast delivery of the Unicast Bound Image to a given TRE.

Figure 4-1: Unicast Bound Image Loading procedure



The procedure has 24 steps:

1. The OFL Agent requires the OFL Service to return the value of the SERIAL_NUMBER register.

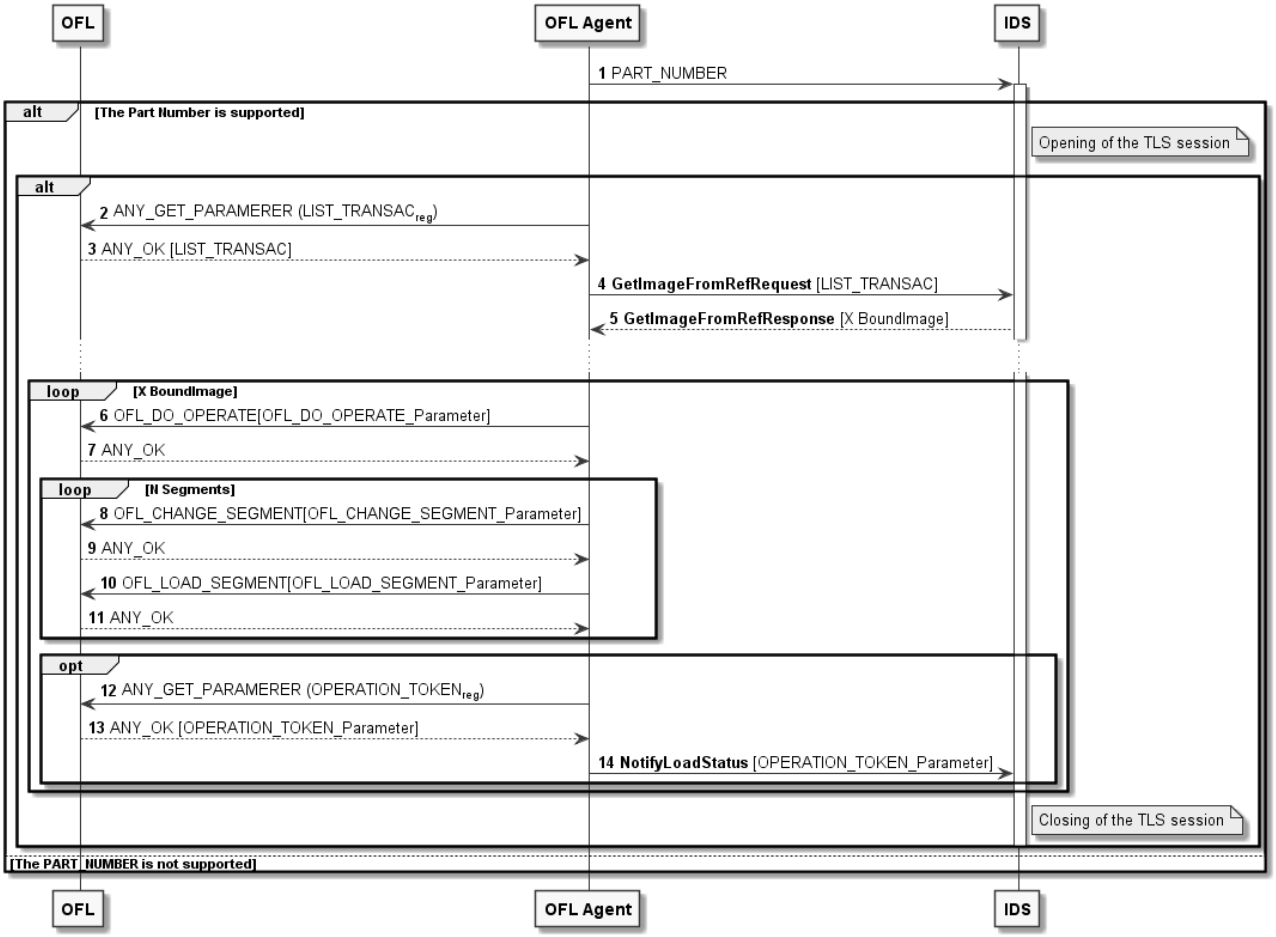
2. The OFL Service returns the SERIAL_NUMBER value to the OFL Agent.
3. The OFL Agent gets by any Out-Of-Band means (e.g. QR-Code, keyboard…) the parameters to request the IDS Credentials.
4. The OFL Agent requires the opening of a TLS session and provides the PART_NUMBER of the TRE. If the Part Number (PART_NUMBER) is not supported by the IDS then the procedure is aborted.
5. The OFL Agent may require from the IDS Certification Path, ended by the CERT.IDS$_1$.ECKA Certificate, by sending the GetCertificateRequest over the INT4 interface.
6. The IDS returns its certificate by sending the GetCertificateResponse over the INT4 interface.
7. Alternatively to steps 4 and 5, the OFL Agent gets by any Out-Of-Band means the IDS Certification Path.
8. The OFL Agent generates the IDS_CREDENTIAL_PARAMETER in concatenating CODE_M, CERT.IDS$_1$.ECKA and OPT_PARAM as defined in the section 6.2.1 in [OFL]. The OFL Agent sends over the INT5 interface, the ANY_SET_PARAMETER command containing the IDS_CREDENTIAL_PARAMETER for the IDS_CREDENTIAL_PARAMETER register as defined in the section 2.3.5 in [OFLE].
9. The OFL Service returns a successful execution over the INT5 interface.
10. The OFL Agent requests, over the INT5 interface, the OFL Service to return the TRE credentials (TRE_CREDENTIALS_PARAMETER) by sending the ANY_GET_PARAMETER command from the TRE_CREDENTIALS_PARAMETER register as defined in the section 2.3.5 in [OFLE].
11. The OFL Service returns the TRE_CREDENTIAL_PARAMETER value to the OFL Agent over the INT5 interface.
12. The OFL Agent copies the TRE_CREDENTIAL_PARAMETER value to the TreCredentialsParameter for the GetImageRequest. The OFL Agent may add metadata from the OFB over the INT6 interface and copies them into the aMetaData parameter of the GetImageRequest.
    The GetImageRequest is sent to the IDS over the INT4 interface.
13. The IDS returns the GetImageResponse containing the Unicast Bound Image over the INT4 interface or the Image Session identifier (ID_TRANSAC) related to the Unicast Bound Image. The communication session on the INT4 interface may be closed.
14. If the Image Session identifier has been returned then the OFL Agent may request the Unicast Bound Image by using the function GetImageFromRefRequest.
15. The IDS returns the Unicast Bound Image.
16. The OFL Agent may forward the metadata from the GetImageResponse to the OFB over the INT6 interface. The OFL Agent extracts from the Unicast Bound Image the OFL_DO_OPERATE_Parameter. The OFL Agent may forward the metadata of the Unicast Bound Image to the OFB over the INT6 interface. The OFL Agent prepares the OFL_DO_OPERATE command with the OFL_DO_OPERATE_Parameter, as defined in the section 2.3.2.1 in [OFLE]. The OFL Agent sends the OFL_DO_OPERATE command to the OFL Service over the INT5 interface.
17. If the OFL returns ANY_OK and if the aNumberSegment value extracted from the Unicast Bound Image is greater than 0 then the procedure goes to step 18, otherwise the procedure goes to step 22. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 24 in reporting a loading failure (aStatus sets to NOK) to the IDS.

18. The OFL Agent extracts from the Unicast Bound Image the OFL_CHANGE_SEGMENT_Parameter corresponding to the current segment to load. The OFL Agent prepares the OFL_CHANGE_SEGMENT command with the OFL_CHANGE_SEGMENT_Parameter, as defined in the section 2.3.2.3 in [OFLE]. The OFL Agent sends the OFL_CHANGE_SEGMENT command to the OFL Service over the INT5 interface.
19. The OFL Service returns ANY_OK informing a successful execution. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to the step 24 in reporting a loading failure (aStatus sets to NOK) to the IDS.
20. The OFL Agent extracts from the Unicast Bound Image the OFL_LOAD_SEGMENT_Parameter corresponding to the current segment to load. The OFL Agent prepares the OFL_LOAD_SEGMENT command with the OFL_LOAD_SEGMENT_Parameter, as defined in the section 2.3.2.2 in [OFLE]. The OFL Agent sends the OFL_LOAD_SEGMENT command to the OFL Service over the INT5 interface.
21. The OFL Service returns ANY_OK informing a successful execution and the procedure restarts from step 18 until all segments are not loaded. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 24 in reporting a loading failure (aStatus sets to NOK) to the IDS.
22. If the loading of all segments are successful then the OFL Agent requests, over the INT5 interface, the OFL Service to retrieve the operation token (OPERATION_TOKEN) by sending the ANY_GET_PARAMETER command from the OPERATION_TOKEN register as defined in section 2.3.5 in [OFLE].
23. The OFL Service returns ANY_OK with the OPERATION_TOKEN register value.
24. The OFL Agent prepares the NotifyLoadStatus request in filling the aStatus parameter and the aATK-OFL-DO-OPERATE with the OPERATION_TOKEN register value. The OFL Agent opens a communication session over the INT4 interface to the IDS. The OFL Agent sends the NotifyLoadStatus to the IDS.

4.2 Pre-Unicast Bound Image Loading operation procedure

The Figure 4-2 illustrates the procedure for a pre-Unicast Bound Image Loading. The IDS may receive from the INT8 interface tokens called ATK.IDS_1.ECDSA as defined in the Table 8-9 in [OFL]. These tokens allow the binding of the Unbound Image to a given TRE. The Unicast Bound Image is referenced by ID_TRANSAC defined in [OFL]..

Figure 4-2: Pre-Unicast Bound Image Loading procedure



The procedure has 14 steps:

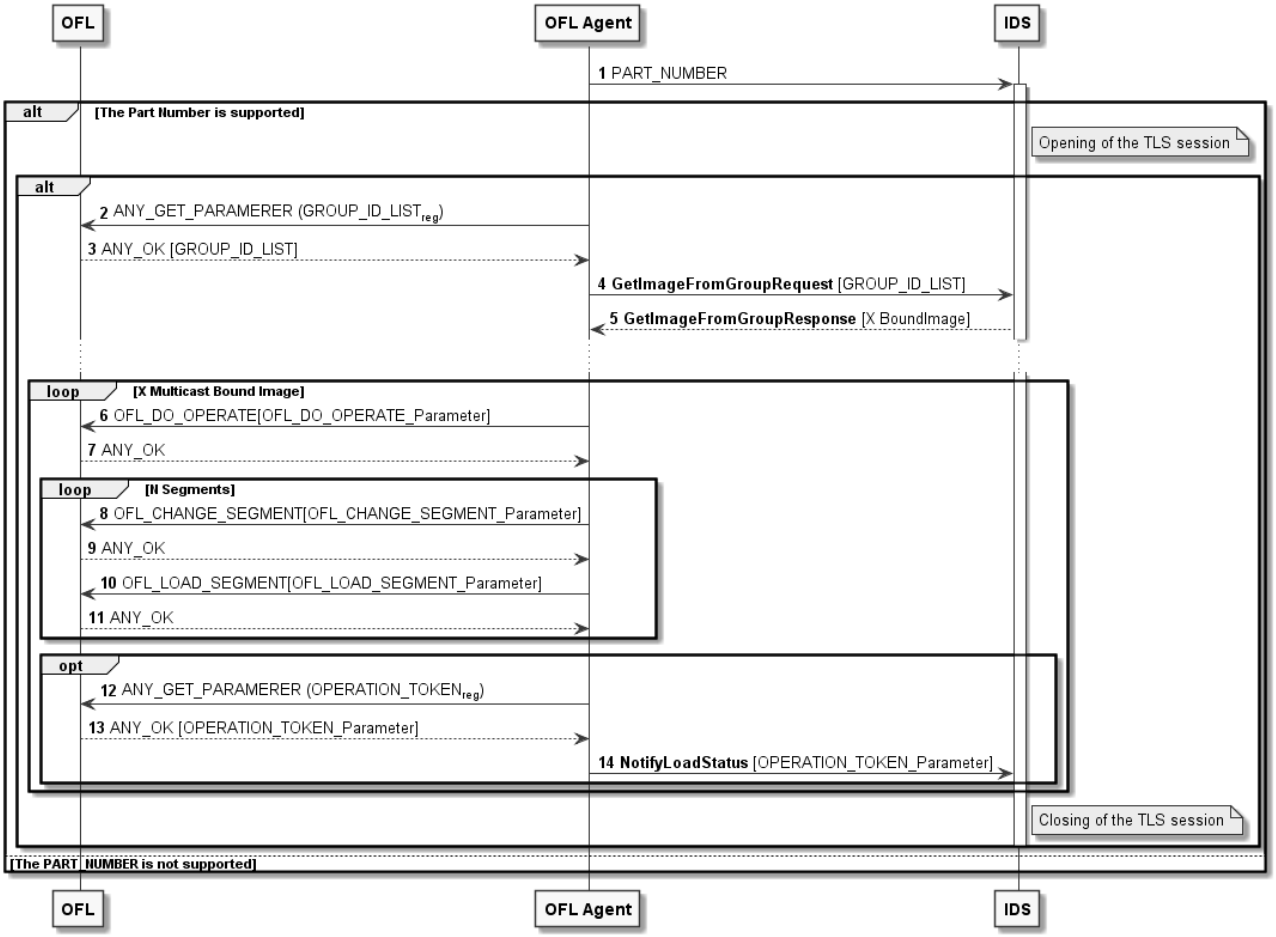
1. The OFL Agent requires the opening of a TLS session and provides the PART_NUMBER of the TRE. If the Part Number (PART_NUMBER) is not supported by the IDS then the procedure is aborted.
2. The OFL Agent requires the OFL Service to return the value of the LIST_TRANSAC register.
3. The OFL Service returns the LIST_TRANSAC value to the OFL Agent.
4. The OFL Agent copies the LIST_TRANSAC value to the aIdImageSessionList parameter for the GetImageFromRefRequest. The OFL Agent may add metadata from the OFB over the INT6 interface and copies them into the aMetaDataResquest parameter of the GetImageFromRefRequest. The GetImageFromRefRequest is sent to the IDS over the INT4 interface.
5. The IDS returns the GetImageFromRefResponse containing the Unicast Bound Images over the INT4 interface. The communication session on the INT4 interface may be closed.

6. The OFL Agent may forward the metadata of the GetImageFromRefResponse to the OFB over the INT6 interface. The OFL Agent extracts sequentially from the Unicast Bound Images a Unicast Bound Image. The OFL Agent extracts, from the Unicast Bound Image, the OFL_DO_OPERATE_Parameter. The OFL Agent may forward the metadata of the Unicast Bound Image to the OFB over the INT6 interface. The OFL Agent prepares the OFL_DO_OPERATE command with the OFL_DO_OPERATE_Parameter, as defined in section 2.3.2.1 in [OFLE]. The OFL Agent sends the OFL_DO_OPERATE command to the OFL Service over the INT5 interface.
7. If the OFL returns ANY_OK and if the aNumberSegment value extracted from the Unicast Bound Image is greater than 0 then the procedure goes to step 8 otherwise the procedure goes to step 12. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 14 in reporting a loading failure (aStatus sets to NOK) to the IDS.
8. The OFL Agent extracts from the Unicast Bound Image the OFL_CHANGE_SEGMENT_Parameter corresponding to the current segment to load. The OFL Agent prepares the OFL_CHANGE_SEGMENT command with the OFL_CHANGE_SEGMENT_Parameter, as defined in section 2.3.2.3 in [OFLE]. The OFL Agent sends the OFL_CHANGE_SEGMENT command to the OFL Service over the INT5 interface.
9. The OFL Service returns ANY_OK informing a successful execution. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 14 in reporting a loading failure (aStatus sets to NOK) to the IDS.
10. The OFL Agent extracts from the Unicast Bound Image the OFL_LOAD_SEGMENT_Parameter corresponding to the current segment to load. The OFL Agent prepares the OFL_LOAD_SEGMENT command with the OFL_LOAD_SEGMENT_Parameter, as defined in the section 2.3.2.2 in [OFLE]. The OFL Agent sends the OFL_LOAD_SEGMENT command to the OFL Service over the INT5 interface.
11. The OFL Service returns ANY_OK informing a successful execution and the procedure restarts from step 8 until all segments are not loaded. If the OFL Service does not return ANY_OK then the Image Loading has failed and the procedure goes to step 14 in reporting a Image Loading failure (aStatus sets to NOK) to the IDS.
12. If the loading of all segments is successful then the OFL Agent requests, over the INT5 interface, the OFL Service to retrieve the operation token (OPERATION_TOKEN) by sending the ANY_GET_PARAMETER command from the OPERATION_TOKEN register as defined in section 2.3.5 in [OFLE].
13. The OFL Service returns ANY_OK with the OPERATION_TOKEN register value.
14. The OFL Agent prepares the NotifyLoadStatus request in filling the aStatus parameter and the aATK-OFL-DO-OPERATE with the OPERATION_TOKEN register value. The OFL Agent opens a communication session over the INT4 interface to the IDS. The OFL Agent sends the NotifyLoadStatus to the IDS. The OFL Agent returns to step 6 until all Unicast Bound Images are extracted.

4.1 Multicast Bound Image Loading procedure

The Figure 4-3 illustrates the procedure for a Multicast Image Loading leading to multicast Firmware Update as defined in the section 4.3.5 in [OFL]. For performing a multicast Firmware Update, the TRE shall contain the Firmware publishing a Firmware Group Identifier as defined in [OFL]. The Multicast Bound Image is referenced by the Group Identifier as defined in [OFL].

Figure 4-3: Multicast Bound Image Loading procedure



The procedure has 14 steps:

1. The OFL Agent requires the opening of a TLS session and provides the PART_NUMBER of the TRE. If the Part Number (PART_NUMBER) is not supported by the IDS then the procedure is aborted.
2. The OFL Agent requires the OFL Service to return the value of the GROUP_ID_LIST register.
3. The OFL Service returns the GROUP_ID_LIST value to the OFL Agent.
4. The OFL Agent copies the GROUP_ID_LIST value to the aGroupIDList parameter for the GetMulticastImageRequest. The OFL Agent may add metadata from the OFB over the INT6 interface and copies them into the aMetaDataRequest parameter of the GetMulticastImageRequest. The GetMulticastImageRequest is sent to the IDS over the INT4 interface.
5. The IDS returns the GetMulticastImage response containing the Multicast Bound Images over the INT4 interface. The communication session on the INT4 interface may be closed.

6. The OFL Agent may forward the metadata of the GetImageFromRefResponse to the OFB over the INT6 interface. The OFL Agent extracts sequentially from the Multicast Bound Images a Multicast Bound Image. The OFL Agent extracts, from the Multicast Bound Image, the OFL_DO_OPERATE_Parameter. The OFL Agent may forward the metadata of the Multicast Bound Image to the OFB over the INT6 interface. The OFL Agent prepares the OFL_DO_OPERATE command with the OFL_DO_OPERATE_Parameter, as defined in section 2.3.2.1 in [OFLE]. The OFL Agent sends the OFL_DO_OPERATE command to the OFL Service over the INT5 interface.
7. If the OFL returns ANY_OK and if the aNumberSegment value extracted from the Multicast Bound Image is greater than 0 then the procedure goes to step 7, otherwise the procedure goes to step 11. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 14 in reporting a loading failure (aStatus sets to NOK) to the IDS.
8. The OFL Agent extracts from the Multicast Bound Image the OFL_CHANGE_SEGMENT_Parameter corresponding to the current segment to load. The OFL Agent prepares the OFL_CHANGE_SEGMENT command with the OFL_CHANGE_SEGMENT_Parameter, as defined in section 2.3.2.3 in [OFLE]. The OFL Agent sends the OFL_CHANGE_SEGMENT command to the OFL Service over the INT5 interface.
9. The OFL Service returns ANY_OK informing a successful execution. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 14 in reporting a loading failure (aStatus sets to NOK) to the IDS.
10. The OFL Agent extracts from the Multicast Bound Image the OFL_LOAD_SEGMENT_Parameter corresponding to the current segment to load. The OFL Agent prepares the OFL_LOAD_SEGMENT command with the OFL_LOAD_SEGMENT_Parameter, as defined in the section 2.3.2.2 in [OFLE]. The OFL Agent sends the OFL_LOAD_SEGMENT command to the OFL Service over the INT5 interface.
11. The OFL Service returns ANY_OK informing a successful execution and the procedure restarts from step 8 until all segments are not loaded. If the OFL Service does not return ANY_OK then the Image loading has failed and the procedure goes to step 14 in reporting a loading failure (aStatus sets to NOK) to the IDS.
12. If the loading of all segments are successful then the OFL Agent requests, over the INT5 interface, the OFL Service to retrieve the operation token (OPERATION_TOKEN) by sending the ANY_GET_PARAMETER command from the OPERATION_TOKEN register as defined in section 2.3.5 in [OFLE].
13. The OFL Service returns ANY_OK with the OPERATION_TOKEN register value.
14. The OFL Agent prepares the NotifyLoadStatus request in filling the aStatus parameter and the aATK-OFL-DO-OPERATE with the OPERATION_TOKEN register value. The OFL Agent opens a communication session over the INT4 interface to the IDS. The OFL Agent sends the NotifyLoadStatus to the IDS. The OFL Agent returns to step 6 until all Multicast Bound Images are extracted.

5 Annex B (Informative): ASN.1

```
-- ASN1START
END
-- ASN1STOP
```

6 Annex C (Informative): JSON Schema

The JSON schema for the INT4 interface is defined hereunder:

```
{
	"$schema": "http://json-schema.org/draft-04/schema#",
	"additionalProperties": false,
	"definitions": {
		".i4:getCertificateRequest": {
			"$ref": "#/definitions/i4:GetCertificateRequest"
		},
		".i4:getCertificateResponse": {
			"$ref": "#/definitions/i4:GetCertificateResponse"
		},
		".i4:getImageFromRefRequest": {
			"$ref": "#/definitions/i4:GetImageFromRefRequest"
		},
		".i4:getImageFromRefResponse": {
			"$ref": "#/definitions/i4:GetImageFromRefResponse"
		},
		".i4:getImageRequest": {
			"$ref": "#/definitions/i4:GetImageRequest"
		},
		".i4:getImageResponse": {
			"$ref": "#/definitions/i4:GetImageResponse"
		},
		".i4:getMulticastImageRequest": {
			"$ref": "#/definitions/i4:GetMulticastImageRequest"
		},
		".i4:getMulticastImageResponse": {
			"$ref": "#/definitions/i4:GetMulticastImageResponse"
		},
		".i4:notifyDeleteStatus": {
			"$ref": "#/definitions/i4:NotifyDeleteStatus"
		},
		".i4:notifyLoadStatus": {
			"$ref": "#/definitions/i4:NotifyLoadStatus"
		},
		"asn1:BMPString": {
			"type": "string"
		},
		"asn1:BOOLEAN": {
			"additionalProperties": false,
			"properties": {
				"false": {
					"additionalProperties": false,
					"type": "object"
				},
				"true": {
					"additionalProperties": false,
					"type": "object"
				}
			},
			"type": "object"
		},
		"asn1:BitString": {
			"pattern": "^([0-1]*)$",
			"type": "string"
		},
		"asn1:EXTERNAL": {
			"additionalProperties": false,
			"properties": {
				"data-value-descriptor": {
					"$ref": "#/definitions/asn1:ObjectDescriptor"
```

```
                                },
                                "direct-reference": {
                                        "$ref": "#/definitions/asn1:ObjectIdentifier"
                                },
                                "encoding": {
                                        "additionalProperties": false,
                                        "properties": {
                                                "arbitrary": {
                                                        "$ref": "#/definitions/asn1:BitString"
                                                },
                                                "octet-aligned": {
                                                        "$ref": "#/definitions/xsd:hexBinary"
                                                },
                                                "single-ASN1-type": {
                                                        "$ref": "#/definitions/asn1:ObjectIdentifier"
                                                }
                                        },
                                        "type": "object"
                                },
                                "indirect-reference": {
                                        "$ref": "#/definitions/asn1:ObjectIdentifier"
                                }
                        },
                        "required": [
                                "encoding"
                        ],
                        "type": "object"
                },
                "asn1:EmbeddedPDV": {
                        "additionalProperties": false,
                        "properties": {
                                "data-value": {
                                        "$ref": "#/definitions/xsd:hexBinary"
                                },
                                "identification": {
                                        "additionalProperties": false,
                                        "properties": {
                                                "context-negotiation": {
                                                        "additionalProperties": false,
                                                        "properties": {
                                                                "presentation-context-id": {
                                                                        "$ref":
"#/definitions/asn1:INTEGER"
                                                                },
                                                                "transfer-syntax": {
                                                                        "$ref":
"#/definitions/asn1:ObjectIdentifier"
                                                                }
                                                        },
                                                        "required": [
                                                                "presentation-context-id",
                                                                "transfer-syntax"
                                                        ],
                                                        "type": "object"
                                                },
                                                "fixed": {
                                                        "$ref": "#/definitions/asn1:NULL"
                                                },
                                                "presentation-context-id": {
                                                        "$ref": "#/definitions/asn1:INTEGER"
                                                },
                                                "syntax": {
                                                        "$ref": "#/definitions/asn1:ObjectIdentifier"
                                                },
```

```
                                                "syntaxes": {
                                                        "additionalProperties": false,
                                                        "properties": {
                                                                "abstract": {
                                                                        "$ref":
"#/definitions/asn1:ObjectIdentifier"
                                                                },
                                                                "transfer": {
                                                                        "$ref":
"#/definitions/asn1:ObjectIdentifier"
                                                                }
                                                        },
                                                        "required": [
                                                                "abstract",
                                                                "transfer"
                                                        ],
                                                        "type": "object"
                                                },
                                                "transfer-syntax": {
                                                        "$ref": "#/definitions/asn1:ObjectIdentifier"
                                                }
                                        },
                                        "type": "object"
                                }
                        },
                        "required": [
                                "data-value",
                                "identification"
                        ],
                        "type": "object"
                },
                "asn1:EnumInfo": {
                        "additionalProperties": false,
                        "properties": {
                                "EnumItem": {
                                        "items": {
                                                "additionalProperties": false,
                                                "properties": {
                                                        "@name": {
                                                                "$ref": "#/definitions/xsd:string"
                                                        },
                                                        "@value": {
                                                                "$ref": "#/definitions/xsd:integer"
                                                        }
                                                },
                                                "type": "object"
                                        },
                                        "type": "array"
                                }
                        },
                        "type": "object"
                },
                "asn1:GeneralString": {
                        "type": "string"
                },
                "asn1:GraphicString": {
                        "type": "string"
                },
                "asn1:IA5String": {
                        "type": "string"
                },
                "asn1:INTEGER": {
                        "type": "integer"
                },
```

```
            "asn1:ISO646String": {
                    "pattern": "^([ -z]*)$",
                    "type": "string"
            },
            "asn1:NULL": {
                    "additionalProperties": false,
                    "type": "object"
            },
            "asn1:NamedBitInfo": {
                    "additionalProperties": false,
                    "properties": {
                            "NamedBit": {
                                    "items": {
                                            "additionalProperties": false,
                                            "properties": {
                                                    "@name": {
                                                            "$ref": "#/definitions/xsd:string"
                                                    },
                                                    "@value": {
                                                            "$ref": "#/definitions/xsd:integer"
                                                    }
                                            },
                                            "type": "object"
                                    },
                                    "type": "array"
                            }
                    },
                    "type": "object"
            },
            "asn1:NumericString": {
                    "pattern": "^([ 0-9]*)$",
                    "type": "string"
            },
            "asn1:OIDIRI": {
                    "type": "string"
            },
            "asn1:ObjectDescriptor": {
                    "type": "string"
            },
            "asn1:ObjectIdentifier": {
                    "pattern": "^([0-2](\\.[1-3]?[0-9](\\.[\\d]+)*)?)$",
                    "type": "string"
            },
            "asn1:OctetString": {
                    "pattern": "^([0-9A-Fa-f]*)$",
                    "type": "string"
            },
            "asn1:OpenType": {
                    "additionalProperties": false,
                    "patternProperties": {
                            "^\\w+$": {
                            }
                    },
                    "type": "object"
            },
            "asn1:PrintableString": {
                    "pattern": "^([ '-\\)\\+-\\.0-\\:\\=\\?A-Za-z]*)$",
                    "type": "string"
            },
            "asn1:REAL": {
                    "additionalProperties": false,
                    "properties": {
                            "$": {
                                    "type": [
```

```
                                        "string",
                                        "number",
                                        "boolean"
                                ]
                        },
                        "MINUS-INFINITY": {
                                "additionalProperties": false,
                                "type": "object"
                        },
                        "PLUS-INFINITY": {
                                "additionalProperties": false,
                                "type": "object"
                        }
                },
                "type": [
                        "object",
                        "string",
                        "number",
                        "boolean"
                ]
        },
        "asn1:RealAssociatedType": {
                "additionalProperties": false,
                "properties": {
                        "base": {
                                "$ref": "#/definitions/xsd:integer"
                        },
                        "exponent": {
                                "$ref": "#/definitions/xsd:integer"
                        },
                        "mantissa": {
                                "$ref": "#/definitions/xsd:integer"
                        }
                },
                "required": [
                        "base",
                        "exponent",
                        "mantissa"
                ],
                "type": "object"
        },
        "asn1:RelativeOID": {
                "pattern": "^([\\d]+(\\.[\\d]+)*)$",
                "type": "string"
        },
        "asn1:RelativeOIDIRI": {
                "type": "string"
        },
        "asn1:T61String": {
                "pattern": "^([ -\"%-\\[\\]_a-z]*)$",
                "type": "string"
        },
        "asn1:TeletexString": {
                "pattern": "^([ -\"%-\\[\\]_a-z]*)$",
                "type": "string"
        },
        "asn1:UTF8String": {
                "type": "string"
        },
        "asn1:UniversalString": {
                "type": "string"
        },
        "asn1:VideotexString": {
                "type": "string"
```

```
            },
            "asn1:VisibleString": {
                    "pattern": "^([ -z]*)$",
                    "type": "string"
            },
            "i4:AtkOFLDeleteSession": {
                    "maxLength": 32,
                    "minLength": 32,
                    "type": "string"
            },
            "i4:AtkOFLDoOperate": {
                    "maxLength": 32,
                    "minLength": 32,
                    "type": "string"
            },
            "i4:BoundImage": {
                    "additionalProperties": false,
                    "patternProperties": {
                            "^\\w+$": {
                            }
                    },
                    "properties": {
                            "i4:aChangeSegmentParameters": {
                                    "$ref": "#/definitions/i4:ChangeSegmentParameters"
                            },
                            "i4:aDoOperateParameter": {
                                    "$ref": "#/definitions/i4:DoOperateParameter"
                            },
                            "i4:aFirmwareFamilyID": {
                                    "$ref": "#/definitions/i4:FirmwareFamilyID"
                            },
                            "i4:aFirmwareID": {
                                    "$ref": "#/definitions/i4:FirmwareID"
                            },
                            "i4:aFirmwareSize": {
                                    "$ref": "#/definitions/xsd:integer"
                            },
                            "i4:aImageMakerID": {
                                    "$ref": "#/definitions/i4:ImageMakerID"
                            },
                            "i4:aImageOwnerID": {
                                    "$ref": "#/definitions/i4:ImageOwnerID"
                            },
                            "i4:aLoadSegmentParameters": {
                                    "$ref": "#/definitions/i4:LoadSegmentParameters"
                            },
                            "i4:aMetaDataImage": {
                                    "$ref": "#/definitions/i4:Metadata"
                            },
                            "i4:aNumberSegment": {
                                    "$ref": "#/definitions/i4:NumberSegment"
                            },
                            "i4:aImageSessionID": {
                                    "$ref": "#/definitions/i4:ImageSessionID"
                            }
                    },
                    "required": [
                            "i4:aDoOperateParameter",
                            "i4:aFirmwareFamilyID",
                            "i4:aFirmwareID",
                            "i4:aFirmwareSize",
                            "i4:aImageOwnerID",
                            "i4:aNumberSegment"
                    ],
```

```
                "type": "object"
        },
        "i4:Certificate": {
                "type": "string"
        },
        "i4:Certificates": {
                "items": {
                        "type": "string"
                },
                "type": "array"
        },
        "i4:ChangeSegmentParameter": {
                "type": "string"
        },
        "i4:ChangeSegmentParameters": {
                "items": {
                        "type": "string"
                },
                "type": "array"
        },
        "i4:DoOperateParameter": {
                "type": "string"
        },
        "i4:FirmwareFamilyID": {
                "maxLength": 16,
                "minLength": 16,
                "type": "string"
        },
        "i4:FirmwareID": {
                "maxLength": 16,
                "minLength": 16,
                "type": "string"
        },
        "i4:GetCertificateRequest": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aMetaDataRequest": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aVersion": {
                                "$ref": "#/definitions/i4:Version"
                        },
                        "i4:aVersionOFL": {
                                "$ref": "#/definitions/i4:VersionOFL"
                        }
                },
                "required": [
                        "i4:aVersionOFL"
                ],
                "type": "object"
        },
        "i4:GetCertificateResponse": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aCertificates": {
                                "$ref": "#/definitions/i4:Certificates"
```

```
                        },
                        "i4:aMetaDataReponse": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aStatus": {
                                "$ref": "#/definitions/i4:Status"
                        }
                },
                "required": [
                        "i4:aCertificates",
                        "i4:aStatus"
                ],
                "type": "object"
        },
        "i4:GetImageFromRefRequest": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aMetaDataRequest": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aImageSessionIDList": {
                                "$ref": "#/definitions/i4:ImageSessionIDList"
                        },
                        "i4:aVersion": {
                                "$ref": "#/definitions/i4:Version"
                        },
                        "i4:aVersionOFL": {
                                "$ref": "#/definitions/i4:VersionOFL"
                        }
                },
                "required": [
                        "i4:aImageSessionIDList",
                        "i4:aVersionOFL"
                ],
                "type": "object"
        },
        "i4:GetImageFromRefResponse": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aBoundImages": {
                                "additionalProperties": false,
                                "properties": {
                                        "i4:BoundImage": {
                                                "items": {
                                                        "$ref": "#/definitions/i4:BoundImage"
                                                },
                                                "type": "array"
                                        }
                                },
                                "type": "object"
                        },
                        "i4:aMetaDataReponse": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aStatus": {
                                "$ref": "#/definitions/i4:Status"
```

```
                        }
                },
                "required": [
                        "i4:aStatus"
                ],
                "type": "object"
        },
        "i4:GetImageRequest": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aMetaDataRequest": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aTreCredentialsParameter": {
                                "$ref": "#/definitions/i4:TreCredentialsParameter"
                        },
                        "i4:aVersion": {
                                "$ref": "#/definitions/i4:Version"
                        },
                        "i4:aVersionOFL": {
                                "$ref": "#/definitions/i4:VersionOFL"
                        }
                },
                "required": [
                        "i4:aTreCredentialsParameter",
                        "i4:aVersionOFL"
                ],
                "type": "object"
        },
        "i4:GetImageResponse": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aMetaDataReponse": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aResult": {
                                "additionalProperties": false,
                                "patternProperties": {
                                        "^\\w+$": {
                                        }
                                },
                                "properties": {
                                        "i4:aBoundImage": {
                                                "$ref": "#/definitions/i4:BoundImage"
                                        },
                                        "i4:aImageSessionID": {
                                                "$ref": "#/definitions/i4:ImageSessionID"
                                        }
                                },
                                "type": "object"
                        },
                        "i4:aStatus": {
                                "$ref": "#/definitions/i4:Status"
                        }
                },
                "required": [
```

```
                        "i4:aStatus"
                ],
                "type": "object"
        },
        "i4:GetMulticastImageRequest": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aGroupIDList": {
                                "$ref": "#/definitions/i4:GroupIDList"
                        },
                        "i4:aMetaDataRequest": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aVersion": {
                                "$ref": "#/definitions/i4:Version"
                        },
                        "i4:aVersionOFL": {
                                "$ref": "#/definitions/i4:VersionOFL"
                        }
                },
                "required": [
                        "i4:aGroupIDList",
                        "i4:aVersionOFL"
                ],
                "type": "object"
        },
        "i4:GetMulticastImageResponse": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aBoundImages": {
                                "additionalProperties": false,
                                "properties": {
                                        "i4:BoundImage": {
                                                "items": {
                                                        "$ref": "#/definitions/i4:BoundImage"
                                                },
                                                "type": "array"
                                        }
                                },
                                "type": "object"
                        },
                        "i4:aMetaDataReponse": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aStatus": {
                                "$ref": "#/definitions/i4:Status"
                        }
                },
                "required": [
                        "i4:aStatus"
                ],
                "type": "object"
        },
        "i4:GroupIDList": {
                "type": "string"
        },
```

```
            "i4:ImageMakerID": {
                    "maxLength": 16,
                    "minLength": 16,
                    "type": "string"
            },
            "i4:ImageOwnerID": {
                    "maxLength": 16,
                    "minLength": 16,
                    "type": "string"
            },
            "i4:LoadSegmentParameter": {
                    "type": "string"
            },
            "i4:LoadSegmentParameters": {
                    "items": {
                            "type": "string"
                    },
                    "type": "array"
            },
            "i4:MetaDatum": {
                    "additionalProperties": false,
                    "patternProperties": {
                            "^\\w+$": {
                            }
                    },
                    "properties": {
                            "i4:aData": {
                                    "maxLength": 8196,
                                    "minLength": 0,
                                    "type": "string"
                            },
                            "i4:aTypeDatum": {
                                    "$ref": "#/definitions/asn1:ObjectIdentifier"
                            }
                    },
                    "required": [
                            "i4:aTypeDatum"
                    ],
                    "type": "object"
            },
            "i4:Metadata": {
                    "additionalProperties": false,
                    "properties": {
                            "i4:MetaDatum": {
                                    "items": {
                                            "$ref": "#/definitions/i4:MetaDatum"
                                    },
                                    "minItems": 1,
                                    "type": "array"
                            }
                    },
                    "required": [
                            "i4:MetaDatum"
                    ],
                    "type": "object"
            },
            "i4:NotifyDeleteStatus": {
                    "additionalProperties": false,
                    "patternProperties": {
                            "^\\w+$": {
                            }
                    },
                    "properties": {
                            "i4:aAtkOFLDeleteSession": {
```

```
                                "$ref": "#/definitions/i4:AtkOFLDeleteSession"
                        },
                        "i4:aFirmwareID": {
                                "$ref": "#/definitions/i4:FirmwareID"
                        },
                        "i4:aImageMakerID": {
                                "$ref": "#/definitions/i4:ImageMakerID"
                        },
                        "i4:aMetaDataNotification": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aStatus": {
                                "$ref": "#/definitions/i4:Status"
                        },
                        "i4:aVersion": {
                                "$ref": "#/definitions/i4:Version"
                        },
                        "i4:aVersionOFL": {
                                "$ref": "#/definitions/i4:VersionOFL"
                        }
                },
                "required": [
                        "i4:aFirmwareID",
                        "i4:aImageMakerID",
                        "i4:aStatus",
                        "i4:aVersionOFL"
                ],
                "type": "object"
        },
        "i4:NotifyLoadStatus": {
                "additionalProperties": false,
                "patternProperties": {
                        "^\\w+$": {
                        }
                },
                "properties": {
                        "i4:aAtkOFLDoOperate": {
                                "$ref": "#/definitions/i4:AtkOFLDoOperate"
                        },
                        "i4:aFirmwareID": {
                                "$ref": "#/definitions/i4:FirmwareID"
                        },
                        "i4:aImageMakerID": {
                                "$ref": "#/definitions/i4:ImageMakerID"
                        },
                        "i4:aMetaDataNotification": {
                                "$ref": "#/definitions/i4:Metadata"
                        },
                        "i4:aStatus": {
                                "$ref": "#/definitions/i4:Status"
                        },
                        "i4:aVersion": {
                                "$ref": "#/definitions/i4:Version"
                        },
                        "i4:aVersionOFL": {
                                "$ref": "#/definitions/i4:VersionOFL"
                        }
                },
                "required": [
                        "i4:aFirmwareID",
                        "i4:aImageMakerID",
                        "i4:aStatus",
                        "i4:aVersionOFL"
                ],
```

```
                "type": "object"
        },
        "i4:NumberSegment": {
                "maximum": 65535,
                "minimum": 0,
                "type": "integer"
        },
        "i4:Status": {
                "maximum": 255,
                "minimum": 1,
                "type": "integer"
        },
        "i4:ImageSessionID": {
                "maxLength": 16,
                "minLength": 16,
                "type": "string"
        },
        "i4:ImageSessionIDList": {
                "type": "string"
        },
        "i4:TreCredentialsParameter": {
                "type": "string"
        },
        "i4:UUID": {
                "maxLength": 16,
                "minLength": 16,
                "type": "string"
        },
        "i4:Version": {
                "anyOf": [
                        {
                                "enum": [
                                        "v1"
                                ],
                                "type": "string"
                        },
                        {
                                "type": "integer"
                        }
                ]
        },
        "i4:VersionOFL": {
                "maxLength": 2,
                "minLength": 2,
                "type": "string"
        },
        "xsd:hexBinary": {
                "type": "string"
        },
        "xsd:integer": {
                "type": "integer"
        },
        "xsd:string": {
                "type": "string"
        }
    },
    "description": "JSON Schema generated by XMLSpy v2019 sp1 (http://www.altova.com)",
    "properties": {
        "@xmlns:asn1": {
                "default": "http://www.obj-sys.com/v1.0/XMLSchema"
        },
        "@xmlns:i4": {
                "default": "https://simalliance.org/INT4Interface"
        },
```

```
                "@xmlns:xsd": {
                        "default": "http://www.w3.org/2001/XMLSchema"
                },
                "i4:getCertificateRequest": {
                        "$ref": "#/definitions/.i4:getCertificateRequest"
                },
                "i4:getCertificateResponse": {
                        "$ref": "#/definitions/.i4:getCertificateResponse"
                },
                "i4:getImageFromRefRequest": {
                        "$ref": "#/definitions/.i4:getImageFromRefRequest"
                },
                "i4:getImageFromRefResponse": {
                        "$ref": "#/definitions/.i4:getImageFromRefResponse"
                },
                "i4:getImageRequest": {
                        "$ref": "#/definitions/.i4:getImageRequest"
                },
                "i4:getImageResponse": {
                        "$ref": "#/definitions/.i4:getImageResponse"
                },
                "i4:getMulticastImageRequest": {
                        "$ref": "#/definitions/.i4:getMulticastImageRequest"
                },
                "i4:getMulticastImageResponse": {
                        "$ref": "#/definitions/.i4:getMulticastImageResponse"
                },
                "i4:notifyDeleteStatus": {
                        "$ref": "#/definitions/.i4:notifyDeleteStatus"
                },
                "i4:notifyLoadStatus": {
                        "$ref": "#/definitions/.i4:notifyLoadStatus"
                }
        },
        "type": "object"
}
```

7 Annex C (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	02/04/2019	Updated version with comment resolution before Publication
V1.0.2	08/04/2019	Updated version after sanity check and introduction of late comment resolution
V1.0.3	22/04/2019	Publication after Board approval