Contents

1 Scope .......................................................................................................................................................... 5
2 References .................................................................................................................................................. 5
3 Definitions, symbols and abbreviations ................................................................................................. 6
   3.1 Definitions ............................................................................................................................................ 6
   3.2 Abbreviations .................................................................................................................................... 6
   3.3 Use of Words .................................................................................................................................... 6
4 Mandatory Resources ............................................................................................................................. 7
   4.1 Operator Profile Version 2 ............................................................................................................... 7
   4.2 Host Control Version 3 ................................................................................................................... 8
   4.3 Low Speed Communication Version 4 for IP connection ............................................................... 8
   4.4 High-Level MMI ............................................................................................................................. 9
   4.5 Application MMI ............................................................................................................................. 9
   4.5.1 CI Plus Browser Extensions ....................................................................................................... 9
   4.5.2 Application Life Cycle Management .......................................................................................... 9
   4.6 Content Control ............................................................................................................................. 9
   4.6.1 Critical Security Update Version protocol ................................................................................. 9
   4.6.2 SRM file transmission for DTCP ............................................................................................... 10
   4.6.3 Transport stream output protection ............................................................................................ 10
   4.7 Application Information .................................................................................................................. 10
5 Optional Functionalities .......................................................................................................................... 10
   5.1 Multi-Stream..................................................................................................................................... 10
   5.1.1 Additional mandatory resources for multi-stream ...................................................................... 10
   5.1.2 Resource advertisement ............................................................................................................ 11
   5.1.3 Diversification of CCK computation .......................................................................................... 11
   5.1.4 Application MMI ....................................................................................................................... 11
   5.1.5 Allocation of LTS_id ............................................................................................................... 11
   5.1.6 PID selection ............................................................................................................................. 11
   5.1.7 Content Control ......................................................................................................................... 11
   5.1.8 Host Control .............................................................................................................................. 12
   5.1.9 High-Level MMI ....................................................................................................................... 12
   5.2 CICAM Player Mode ...................................................................................................................... 12
   5.2.1 Additional Mandatory resources ............................................................................................ 12
   5.2.2 Low Speed Communication Version 4 for Hybrid connection ............................................. 12
   5.2.3 Access from Virtual Channel ................................................................................................... 12
   5.3 Host Player Mode ........................................................................................................................... 13
   5.3.1 Additional Mandatory resources ............................................................................................ 13
   5.3.2 Formats and protocols .............................................................................................................. 13
   5.4 HbbTV CICAM AppMMI Application ............................................................................................ 13
   5.4.1 Additional Mandatory resources ............................................................................................ 13
   5.4.2 Application Domain and InitialObject ..................................................................................... 13
6 CI Plus 2nd Root of Trust ......................................................................................................................... 14
   6.1 Introduction ....................................................................................................................................... 14
   6.2 Content Control Resource ............................................................................................................ 14
   6.2.1 Resource Version .................................................................................................................... 14
   6.2.2 CI Plus CC system ID ............................................................................................................. 14
   6.2.3 Keys on the credentials layer .................................................................................................. 15
   6.2.4 Authentication ........................................................................................................................... 15
   6.2.4.1 Random Number Generation ............................................................................................. 15
   6.2.4.2 Signature of Messages ......................................................................................................... 15
   6.2.5 Content Key Calculation ......................................................................................................... 15
   6.2.6 Power-Up Re-Authentication .................................................................................................. 15
   6.3 CI Plus 2nd Root Certificate Chain ................................................................................................ 17
   6.3.1 Introduction ............................................................................................................................... 17
   6.3.2 Certificate Management Architecture ........................................................................................ 17
6.3.3 Certificate Formats ................................................................. 18
6.3.3.1 version .................................................................................. 18
6.3.3.2 serial number ........................................................................ 18
6.3.3.3 signature ............................................................................... 18
6.3.3.4 issuer .................................................................................... 19
6.3.3.5 validity ................................................................................. 19
6.3.3.6 subject .................................................................................. 19
6.3.3.7 subjectPublicKeyInfo ........................................................... 19
6.3.3.8 issuerUniqueID and subjectUniqueID .................................... 19
6.3.3.9 extensions ............................................................................. 19
6.3.3.10 signatureAlgorithm ............................................................... 21
6.3.3.11 signatureValue ................................................................. 21
6.3.4 Certificate Verification .............................................................. 21

7 Root of Trust Support ................................................................. 22

Annex A (normative): Parameters exchanged in APDUs .......................... 23
Annex B (Informative): DVB-IPTV FCC/RET in the CICA ....................... 25
Annex C (normative): Use of PKCS#1 ............................................... 27

History .............................................................................................. 28
1 Scope

This specification provides the description of a CI Plus LLP implementation based on the TS 103 205 [3], Bluebook A173-2 [5] and CI Plus 1.3 specification [2], pulling together those specifications and specifying what parts need to be implemented in order to realise a device compliant with CI Plus LLP.

This specification is intended to be used in combination with the appropriate certification process, and subject to conformance by the manufacturers to the CI Plus Compliance and Robustness Rules [4].

In addition, this specification introduces the CI Plus 2nd Root of Trust based on the SHA-256 Hash algorithm.

2 References

[4] CI Plus DEVICE INTERIM LICENSE AGREEMENT
[12] ETSI TS 102 809 V1.2.1: “Digital Video Broadcasting (DVB); Signalling and carriage of interactive applications and services in Hybrid Broadcast/Broadband environments”.
3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply in addition to those defined in CI Plus Specification 1.3 [2] and TS 103 205 [3]:

**Standard Security Level:** The security level achieved by a device of a Device Type as defined in the ILA [4]

**ECP Security Level:** The security level achieved by a device of an ECP Device Type as defined in the ILA Addendum for ECP [21]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply in addition to those defined in CI Plus Specification 1.3 [2]:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSUV</td>
<td>Critical Security Update Version</td>
</tr>
<tr>
<td>ECP</td>
<td>Enhanced Content Protection</td>
</tr>
<tr>
<td>EPG</td>
<td>Electronic Program Guide</td>
</tr>
<tr>
<td>FCC</td>
<td>Fast Channel Change</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet Protocol TeleVision</td>
</tr>
<tr>
<td>LCN</td>
<td>Logical Channel Number</td>
</tr>
<tr>
<td>LLP</td>
<td>Limited Liability Partnership</td>
</tr>
<tr>
<td>LTS_id</td>
<td>Local Transport Stream identifier</td>
</tr>
<tr>
<td>OSDT</td>
<td>Online SDT</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RAMS</td>
<td>Rapid Acquisition of Multicast RTP Sessions</td>
</tr>
<tr>
<td>RET</td>
<td>RETransmission</td>
</tr>
<tr>
<td>RR</td>
<td>Receiver Report</td>
</tr>
<tr>
<td>RTCP</td>
<td>Real-time Transport Control Protocol</td>
</tr>
<tr>
<td>SDT</td>
<td>Service Descriptor Table</td>
</tr>
<tr>
<td>SR</td>
<td>Sender Report</td>
</tr>
<tr>
<td>TS</td>
<td>Transport Stream</td>
</tr>
</tbody>
</table>

3.3 Use of Words

The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the specification and from which no deviation is permitted (*shall equals is required to*).

The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should equals is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the specification (*may equals is permitted to*).
4 Mandatory Resources

A CI Plus LLP compliant device shall support the mandatory resources shown in Table 4.1:

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Identifier</th>
<th>Class</th>
<th>Type</th>
<th>Version</th>
<th>Comment</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Manager</td>
<td>00 01 00 41</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td></td>
<td>00 01 00 42</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td>TS 101 699 [16]</td>
</tr>
<tr>
<td>Application Information</td>
<td>00 02 00 41</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td></td>
<td>00 02 00 42</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td></td>
<td>TS 101 699 [16]</td>
</tr>
<tr>
<td></td>
<td>00 02 00 43</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 02 00 45</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td></td>
<td>Bluebook A173-2 [5]</td>
</tr>
<tr>
<td>Conditional Access Support</td>
<td>00 03 00 41</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td>Host Control</td>
<td>00 20 00 41</td>
<td>32</td>
<td>1</td>
<td>1</td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td></td>
<td>00 20 00 42</td>
<td>32</td>
<td>1</td>
<td>2</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 20 00 43</td>
<td>32</td>
<td>1</td>
<td>3</td>
<td></td>
<td>TS 103 205 [3]</td>
</tr>
<tr>
<td>Date-Time</td>
<td>00 24 00 41</td>
<td>36</td>
<td>1</td>
<td>1</td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td>MMI</td>
<td>00 40 00 41</td>
<td>64</td>
<td>1</td>
<td>1</td>
<td></td>
<td>High level only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td>LSC</td>
<td>00 60 60 01</td>
<td>96</td>
<td>384</td>
<td>1</td>
<td></td>
<td>EN 50221 [15]</td>
</tr>
<tr>
<td></td>
<td>00 60 60 02</td>
<td>96</td>
<td>384</td>
<td>2</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 60 60 03</td>
<td>96</td>
<td>384</td>
<td>3</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 60 60 04</td>
<td>96</td>
<td>384</td>
<td>4</td>
<td></td>
<td>TS 103 205 [3]</td>
</tr>
<tr>
<td>Content Control</td>
<td>00 8C 10 01</td>
<td>140</td>
<td>64</td>
<td>1</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 8C 10 02</td>
<td>140</td>
<td>64</td>
<td>2</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 8C 10 04</td>
<td>140</td>
<td>64</td>
<td>4</td>
<td></td>
<td>Bluebook A173-2 [5]</td>
</tr>
<tr>
<td>Host Lang &amp; Country</td>
<td>00 8D 10 01</td>
<td>141</td>
<td>64</td>
<td>1</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>CICAM Upgrade</td>
<td>00 8E 10 01</td>
<td>142</td>
<td>64</td>
<td>1</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>Operator Profile</td>
<td>00 8F 10 01</td>
<td>143</td>
<td>64</td>
<td>1</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td></td>
<td>00 8F 10 02</td>
<td>143</td>
<td>64</td>
<td>2</td>
<td></td>
<td>TS 103 205 [3]</td>
</tr>
<tr>
<td>Application MMI</td>
<td>00 41 00 41</td>
<td>65</td>
<td>1</td>
<td>2</td>
<td></td>
<td>Mandatory for CICAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Optional for Host</td>
</tr>
<tr>
<td></td>
<td>00 41 00 42</td>
<td>65</td>
<td>1</td>
<td>2</td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
</tbody>
</table>

4.1 Operator Profile Version 2

The Host shall implement profile_type=0 and profile_type=1 defined in CI Plus 1.3 [2] clause 14.7.2 as well as profile_type=2 defined in TS 103 205 [3] clause 15.2.

The installation of IP delivered services by use of the OSDT as defined in TS 103 205 [3] clause 15.4 is optional. However, when a Host implements installation of IP delivered services by use of the OSDT, it shall be available for both profile_type 1 and 2.

The Host shall support the Virtual Channel as defined in TS 103 205 [3] clause 15.3 for both profile_type 1 and 2.
The Host shall manage the Virtual Channel in a similar manner to other installed broadcast services. It is recommended that Hosts treat the Event Information associated with the Virtual Channel as if it were the event name in a short_event_descriptor(). The Host may ignore the service provider name of the cicam_virtual_channel_descriptor().

The Host shall make the Virtual Channel as accessible as other services, including but not limited to:

- Direct LCN tune
- CH+ and CH- keys
- EPG
- Accessible from any interactive applications i.e. HbbTV/MHEG LCN tuning operation.

The CICAM Virtual Channel descriptor shall:

- Assign a valid service name to the Virtual Channel of between 1 and 14 characters
- Limit the event_information_length to 40 characters

The Host may ignore the declaration of the Virtual Channel when the service_name_length of the cicam_virtual_channel_descriptor() is set to zero.

When installing a profile with profile type 2, the CICAM may attempt to use any logical_channel_number (LCN), including zero. With profile_type 2, the Host is not guaranteed to honour this LCN request and may re-negotiate with the CICAM for a new LCN.

4.2 Host Control Version 3

The Host shall interpret a tune_triplet_req() with a service_id of value 0x0000 as a tune operation to a multiplex with no service selection. The recommendations of CI Plus 1.3 [2] in Annex E.16.2 should be observed in this case. The CICAM shall only rely on the tune_reply() APDU for the confirmation that the tune has been done.

Support for tune_ip_req() is not mandatory; Hosts not supporting tuning to IP-delivered services shall return a tune_reply() with status_field set to 0x01 (unsupported delivery system descriptor) in reply to a tune_ip_req() APDU sent by the CICAM.

4.3 Low Speed Communication Version 4 for IP connection

The Low Speed Communication resource version 4 as defined in TS 103 205 [3] with device_type 0x60 (IP connection) is mandatory for all Hosts that support an IP connection.

The Host shall support connection requests for LSC resource with device_type 0x60 with the following connection descriptor types:

- IP_descriptor
- Hostname_descriptor

The Host may support connection requests with IP_multicast_descriptor for LSC resource with device_type 0x60. If connections with IP_multicast_descriptor() are not supported the Host shall reply with a comms_reply() indicating the error.

The CICAM shall not use the following connection descriptors when sending a connection request for LSC resource with device_type 0x60:

- telephone_descriptor()
- hybrid_descriptor()

If the CICAM sends a comms_cmd() APDU with a connection descriptor type that is not supported by the Host, the Host shall respond with a comms_reply() APDU with comms_reply_id=Connect_Ack and set the field return_value to 0xFE (Connection protocol not supported).

If the CICAM sends a comms_info_req() APDU for LSC resource with device type 0x60 the Host shall return a comms_info_reply() APDU with status field set to 0b0. The CICAM shall not use this APDU to determine if a connection has succeeded, and should rather rely on the comms_reply() APDU.
The CICAM may send the comms_IP_config_req() APDU for LSC resource with device type 0x60 at any time; the Host shall respond with the comms_IP_config_reply() APDU.

4.4 High-Level MMI

The Host shall support the requirements for implementation of the High-Level MMI resource as defined in TS 103 205 [3] clause 16 with the following exceptions, which represent limits that are practically used in the field:

- Host shall be able to display a menu() object containing up to 50 items.
- Host shall be able to display a list() object containing up to 50 items.

The High-Level MMI shall have priority over any broadcast application where the CICAM is descrambling the service being presented, which may require the broadcast application to be terminated. Whenever the High-Level MMI is displayed by the Host, it shall have focus and be visible to the user.

4.5 Application MMI

4.5.1 CI Plus Browser Extensions

Host support of the CI Plus Browser Extensions defined in clause 4.4 of TS 103 205 [3] is optional.

4.5.2 Application Life Cycle Management

The Host shall give priority to broadcast applications as defined in clause 12.4.4.2 of TS 103 205 [3]. Where the Host is unable to execute the CICAM AppMMI application then the Host shall respond to the RequestStart() APDU with a RequestStartAck() APDU with an AckCode value of 0x03 (API Busy) or refuse to open the session to Application MMI resource.

When the CICAM application is running, it shall not be interrupted until the application exits or the Application MMI session is closed, or specific user interaction takes place.

When a CICAM AppMMI application is running, if the Host terminates the application, then the AppAbortRequest() APDU shall be sent by the Host to inform the CICAM.

4.6 Content Control

A CI Plus compliant device shall support

- versions 1, 2 and 4 of the Content Control resource and the requirements of this chapter. Support of version 3 of the Content Control resource is not required.
- versions 0x01, 0x02 and 0x04 of the URI and may ignore other URI versions. The support of the URI version 3 is not required.

The CICAM shall not request a session to version 3 of the Content Control resource and shall not use the URI version 0x03.

Refer to the ILA [4] for compliance rules for the trick_mode_control_info parameter of the URI.

4.6.1 Critical Security Update Version protocol

Table 4.2 shows the critical security update version protocol. The critical security update version parameter allows the Host to inform the CICAM that it is running a software version that includes a critical security update. The CICAM may use the Host’s critical security update version as part of its revocation process.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>APDU</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CICAM requests the Host critical security update version</td>
<td>cc_sac_data_req</td>
<td>request_datatype_nbr=1&lt;br&gt;index</td>
</tr>
<tr>
<td>2</td>
<td>Host sends an acknowledgement with its critical security update</td>
<td>cc_sac_data_cnf</td>
<td>send_datatype_nbr=1&lt;br&gt;index</td>
</tr>
</tbody>
</table>

Table 4.2: critical security update version protocol
The CICAM may request the Host critical security update version at any time but shall wait for the acknowledgement from the Host before sending any further critical security update version protocol message. The Host shall implement the critical security update version protocol.

The critical security update version is maintained by the Host, the version starts at 0x00 and shall only be incremented when the hardware or software is modified such that it improves or fixes a security or non-conformance issue. The Host shall not use the version value of 0xFF.

There is no requirement to increment critical security update version for every software update.

A CICAM shall not request the critical security update version in Content Control versions 1 or 2 for resource_type 64.

4.6.2 SRM file transmission for DTCP

The Host shall support the SRM delivery protocol for DTCP as defined in clause 5.13 of CI Plus 1.3 [2].

4.6.3 Transport stream output protection

A CI Plus compliant device shall support the AES-128-CBC scrambler option as defined in clause 5.6.2.1 of CI Plus 1.3 [2]. The DES-56-ECB scrambler option is not required for a CI Plus compliant device, implementation is optional.

The scrambler capabilities present in each device certificate shall be interpreted according to table 4.3

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Forbidden (note 1)</td>
</tr>
<tr>
<td>1</td>
<td>AES</td>
</tr>
<tr>
<td>all others</td>
<td>reserved for future use</td>
</tr>
</tbody>
</table>

**Note 1:** DES only scrambler capability is not allowed for new device registrations and has never been deployed in the market.

4.7 Application Information

A CI Plus compliant device shall support the version 1, 2, 3 and 5 of the Application Information resource. The support of the version 4 of the Application Information resource is not required. The CICAM shall not request a session to version 4 of the Application Information resource.

5 Optional Functionalities

5.1 Multi-Stream

Support of multi-stream functionality as described in clause 6 of TS 103 205 [3] is optional for both Host and CICAM devices. Multi-stream capable devices shall meet the requirements of the current chapter and clause 6 of TS 103 205 [3].

5.1.1 Additional mandatory resources for multi-stream

A CI Plus LLP compliant device supporting the multi-stream functionality shall support the additional mandatory resources shown in Table 5.1:

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Identifier</th>
<th>Class</th>
<th>Type</th>
<th>Version</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditional Access Support</td>
<td>00 03 00 81</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>TS 103 205 [3]</td>
</tr>
</tbody>
</table>
The requirements of chapter 4 for single-stream resources are applicable to the corresponding multi-stream resources of this chapter.

### 5.1.2 Resource advertisement

A Host shall advertise in the profile_reply() APDU the resources as listed in table 4.1 and table 5.1. The Host may advertise the resources in any order and the CICAM shall not make any assumptions on the ordering of the resource identifiers in the profile_reply().

Where the Host advertises some but not all of the resources listed in table 5.1, the CICAM shall not open a session to the multi-stream resource and it shall restrict to the single stream versions of the resources.

### 5.1.3 Diversification of CCK computation

When operating in multi-stream mode, the Host and the CICAM shall compute a CCK for each Local TS, identified by its LTS_id, and use the function \( f_{CC}(K_p, \text{LTS_id}) \) as defined in the CI Plus Licensee Specification [1].

### 5.1.4 Application MMI

The Host shall implement the Application MMI resource with resource_type 2 and version 1 with the requirements as defined in clause 4.5, and with the following restrictions:

- The Host may ignore the Application Domain Query (ADQ) option.
- The Host may not implement the caching mechanism.

A CICAM shall implement the caching mechanism and shall not include the ADQ option in the RequestStart() APDU.

### 5.1.5 Allocation of LTS_id

A Host shall not allocate LTS_id 0x00 or 0xFF.

### 5.1.6 PID selection

A Host implementing multi-stream should include a sufficient number of PID filters to allow the smooth operation of the CICAM. In addition to the set of PIDs that the Host shall select for a LTS_id, as described in clause 6.3.2 and 6.3.3 of TS 103 205, it is recommended that the Host provisions for at least 8 additional PIDs filters per LTS_id to be selected by the CICAM with the PID_select_req() APDU.

Below is a typical selection of PIDs filtering:

- 1 for the CAT (EMM)
- 1 for the PAT (TS changes, PMTs)
- 1 for Current PMT (Availability of the whole PMT)
- 1 for TS scan (Channel change time improvement)
- 1 for SDT, BAT (Parental Control, CICAM Upgrade, revocation)
- 1 for NIT (CICAM Upgrade, revocation)
- 1 for EIT (Parental Control)
- 1 for TOT, TDT (Date and time for authentication)
- 1 for carousel download (CICAM Upgrade, revocation)

### 5.1.7 Content Control

A CI Plus compliant device shall support:
• resource_type 65 and version 2. The support of the Content Control resource with resource_type 65 and version 1 is not required.
• Versions 0x01, 0x02 and 0x04 of the URI and may ignore other URI versions. The support of the URI version 3 is not required
• Output control protocol as defined in Bluebook A173-2 [5]
• Critical Security Update Version protocol as defined in clause 4.6.1
• SRM file transmission protocol for DTCP as defined in clause 4.6.2

The CICAM shall not request a session to resource_type 65 and version 1 of the Content Control resource and shall not use the URI version 0x03.

5.1.8 Host Control

The Host shall implement the Host Control resource with resource_type 2 and version 1 with the restrictions as defined in clause 4.2.

5.1.9 High-Level MMI

The Host shall implement the High-level MMI resource with resource_type 2 and version 1 with the requirements as defined in clause 4.4.

5.2 CICAM Player Mode

Support of the CICAM Player Mode is optional for both Host and CICAM devices. CICAM Player Mode capable devices shall meet the requirements of clauses 8 and 10 of TS 103 205 [3] and the requirements of this chapter.

5.2.1 Additional Mandatory resources

A CI Plus LLP compliant device supporting the CICAM Player functionality shall support the additional mandatory resources shown in Table 5.2:

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Identifier</th>
<th>Class</th>
<th>Type</th>
<th>Version</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CICAM Player</td>
<td>00 93 00 41</td>
<td>147</td>
<td>1</td>
<td>1</td>
<td>TS 103 205 [3]</td>
</tr>
<tr>
<td>LSC</td>
<td>00 60 70 04</td>
<td>96</td>
<td>448</td>
<td>4</td>
<td>TS 103 205 [3]</td>
</tr>
</tbody>
</table>

5.2.2 Low Speed Communication Version 4 for Hybrid connection

The Low Speed Communication resource version 4 as defined in TS 103 205 [3] with device type 0x70 (Hybrid connection) is mandatory for a Host that is CICAM Player capable.

The Host shall support connection requests for LSC resource with device_type 0x70 with the following connection descriptor types:

• IP_descriptor
• Hostname_descriptor
• multicast_descriptor

It is recommended that the Host minimally supports 12 concurrent LSC sessions, with device types 0x60 or 0x70. The allocation of those 12 sessions with device_type 0x60 or 0x70 is determined by the CICAM. A representative system using the CICAM player mode is described in Annex B, showing a possible allocation of concurrent LSC sessions with different device types.

5.2.3 Access from Virtual Channel

When the Virtual Channel is accessed, a Host that is CICAM Player capable shall allow the CICAM to initiate a play session with CICAM_player_start_req() APDU.
5.3 Host Player Mode

Support of the Host Player Mode is optional for both Host and CICAM devices. Host Player Mode capable devices shall meet the requirements of clause 7 of TS 103 205 [3] and the requirements of this chapter.

5.3.1 Additional Mandatory resources

A CI Plus LLP compliant device supporting the Host Player functionality shall support the additional mandatory resources shown in Table 5.3:

<table>
<thead>
<tr>
<th>Table 5.3: Mandatory resources for Host Player Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
</tr>
<tr>
<td>Sample Decryption</td>
</tr>
</tbody>
</table>

5.3.2 Formats and protocols

A Host shall minimally support ISOBMFF [7] or DVB-DASH [6] with the following minimum requirements:

- Support of AVC_SD_25 video format as defined in OIPF “Media Formats” [14] clause 5.1.2.1
- Support of HEAAC audio format as defined in OIPF “Media Formats” [14] clause 8.1.1
- Support of video bitrate of at least 1 Mbps

5.4 HbbTV CICAM AppMMI Application

Support for execution of an HbbTV CICAM AppMMI Application is optional for both Host and CICAM devices.

5.4.1 Additional Mandatory resources

A CI Plus LLP compliant device supporting the execution of a HbbTV CICAM AppMMI Application shall support the additional mandatory resources shown in Table 5.4:

<table>
<thead>
<tr>
<th>Table 5.4: Mandatory resources for HbbTV CICAM AppMMI Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
</tr>
<tr>
<td>Auxiliary File System</td>
</tr>
</tbody>
</table>

5.4.2 Application Domain and InitialObject

When the CICAM requests the launching of an HbbTV Application resident in the CICAM by use of the Application MMI resource, the CICAM shall use the Application MMI resource RequestStart() APDU with:

- The AppDomainIdentifier set to “HbbTVEngineProfile1”.
- The InitialObject shall be a text string containing a URL of the path of an XML AIT from the CICAM File System advertised with the Auxiliary File System resource.

The XML AIT file shall be as defined in clause 5.4 of TS 102 809 [12].

The URL schemes for the HbbTV Application accessing files are as defined in the clause 9.2 of HbbTV Specification [11].

The CICAM shall offer the file system by use of the Auxiliary File System resource FileSystemOffer() APDU with the DomainIdentifier set to “HbbTVEngineProfile1” as defined in clause 11.4.3 of HbbTV Specification [11].

The semantic of table 7 of HbbTV Specification [11] shall apply except that the applicationTransport field in the XML AIT shall be either HTTPTransportType (as defined in table 7 of HbbTV Specification [11]) or CIITransportType (as defined in clause 12.4.3.3.3 of TS 103 205 [3]).

The XML file shall contain an application discovery record containing one or more <application> elements, all with the same orgId and appId values but with different application types.

The application launched by this method shall be broadcast independent.
The application launched by this method shall be considered as a CICAM AppMMI application and the requirements of the clause 4.5.2 are then applicable for its life cycle.

In case of multiple CICAMs in a Host, the Host should use the Auxiliary File System resource of the CICAM that started the HbbTV application.

## 6 CI Plus 2nd Root of Trust

### 6.1 Introduction

To keep pace with the advance of technology, CI Plus LLP has defined a CI Plus 2nd Root of Trust based on the SHA-256 Hash algorithm.

This chapter defines the format of the certificates issued from the CI Plus 2nd Root of Trust and how a CI Plus device declares the support of and makes use of this new Root of Trust.

However, chapter 7 defines specific restrictions and requirements on CI Plus devices.

A device supporting the CI Plus 2nd Root of Trust shall:

- Support the CC system ID 2 as defined in clause 6.2.
- Embed credential materials issued from the CI Plus 2nd Root of Trust Certificate Chain as defined in clause 6.3.

### 6.2 Content Control Resource

#### 6.2.1 Resource Version

The Host shall not advertise the support of CC system ID 2 for a session of the Content Control resource with resource identifier 0x008C1001 or 0x008C1002.

A Host that does not support CC system ID 1 and only supports CC system ID 2 shall only support Content Control resource with resource identifier 0x008C1004 for single stream and 0x008C1042 for multi stream, if multi stream functionality is supported. If a CICAM attempts to open the Content Control resource with a different identifier, then the Host shall deny the resource opening as specified in EN50221 [15] and may inform the end user.

The table 6.1 below indicates the cc_system_id_bitmask advertised by the Host according to (i) the identifier of the Content Control resource opened by the CICAM and (ii) the CC system ID(s) supported by the Host.

<table>
<thead>
<tr>
<th>CC system ID supported by Host</th>
<th>cc_system_id_bitmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only CC system ID 1</td>
<td>0b00000001</td>
</tr>
<tr>
<td>CC system ID 1 and 2</td>
<td>0b00000001</td>
</tr>
<tr>
<td>Only CC system ID 2</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

**NOTE 1:** Host shall deny Content Control resource opening

#### 6.2.2 CI Plus CC system ID

CC system ID 1 is allocated for the CI Plus LLP PKI as defined in CI Plus Specification 1.3 [2] (CI Plus Root of Trust).

CC system ID 2 is allocated for the CI Plus LLP PKI as defined in clause 6.3 of the present document (CI Plus 2nd Root of Trust).
During the Authentication protocol, the Host shall advertise the supported CC system ID(s) using the method defined in clause 11.3.1.2 of CI Plus Specification 1.3 [2].

Table 11.34 of CI Plus Specification 1.3 [2] shall be replaced by Table 6.2:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>APDU</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CICAM requests the Host's CC system ID bitmask</td>
<td>cc_open_req</td>
<td></td>
</tr>
</tbody>
</table>
| 2    | Host sends its CC system ID bitmask | cc_open_cnf | cc_system_id_bitmask:  
  - bit 0 set indicates support for CC system ID 1  
  - bit 1 set indicates support for CC system ID 2 |

A CI Plus device may advertise support for both CC system ID 1 and CC system ID 2.

A CICAM supporting CC system ID 2 shall select the CC system ID 2 when the Host advertises it regardless of the Security Level supported by the Host. The Security Level extension is defined in clause 6.3.3.9.8.

The CICAM shall inform the Host of the selection of the CC system as described in clause 20 of BlueBook A165 [17].

6.2.3 Keys on the credentials layer

A CI Plus device supporting the CC system ID 2 is provisioned with a pair of public (MDP or HDP) and private (MDQ or HDQ) keys dedicated to the CI Plus LLP PKI as defined in clause 6.3.

NOTE: The CC system ID 1 public and private keys are different from the CC system ID 2 public and private keys.

The certificate chain for both CICAM and Host for CC system ID 2 is described in clause 6.3 of the present document. This certificate chain is independent from the certificate chain for CC system ID 1 defined in CI Plus Specification 1.3 [2].

When the CC system ID 2 is selected, the constants (DH_p, DH_g, DH_q) involved in operations on the authentication layer are specific to CC system ID 2 and are different from the constants used for the CC system ID 1.

6.2.4 Authentication

6.2.4.1 Random Number Generation

During the execution of the authentication protocol for CC system ID 1 and CC system ID 2, a CI Plus device shall generate the random values listed in Table A.1 of CI Plus Specification 1.3 [2] by use of either a PRNG as defined in Annex A of the CI Plus Specification 1.3 [2] or a PRNG as defined in NIST 800-90A Revision 1[19].

6.2.4.2 Signature of Messages

During the execution of the Authentication protocol for CC system ID 2, Host and CICAM shall create and verify a signature for messages (message_A and message_B as referred to in Table 6.3 of CI Plus Specification 1.3 [2]) using the signing method as defined in Annex C of the present document.

6.2.5 Content Key Calculation

During the Content Control Key computation, the CICAM shall generate Kp using a nonce generated by use of either of the PRNG algorithms defined in clause 6.2.4.1.

6.2.6 Power-Up Re-Authentication

The authentication context stored by the CICAM shall contain the CC system ID that was selected by the CICAM during the previous authentication process. When the CICAM has a valid stored authentication context, during the Power-Up Re-Authentication, as described in clause 6.3 of the CI Plus Specification 1.3 [2], the CICAM shall verify that the selected CC system ID matches the one stored in the authentication context. If there is no match, the CICAM shall start the authentication protocol.

The Figure 6.1 of CI Plus Specification 1.3 [2] is then updated per Figure 6.1 below:
Figure 6.1: Overview of CICAM and Host in the CC Operation (Informative)

Step 5 of the authentication basic steps as described in clause 6.1.4 of the CI Plus Specification 1.3 [2] is updated as followed:

5. The CICAM shall compare its stored AKM with the received AKH. If the authentication keys match and the selected CC system ID is the same as the CC system ID stored in the authentication context, then a
previous authentication has been completed successfully with the selected CC system ID and the certificates are considered valid. The DH Secret Key (DHSK) and authentication keys (AKM/AKH) computed on both sides are then preserved; the key material for the SAC (SAK and SEK) and the Content Control Key (CCK) are independently (re)generated and synchronized on both sides. The system shall then continue with step (10). If the authentication keys or the CC system IDs do not match then the system is required to authenticate and shall continue with step (6). Note that Host behaviour for multiple modules and multiple slots is defined in clause 6.3 of the CI Plus Specification 1.3 [2].

6.3 CI Plus 2nd Root Certificate Chain

6.3.1 Introduction

This chapter defines the CI Plus 2nd Root certificate chain which is fully independent from the certificate chain defined in CI Plus Specification 1.3 [2].

6.3.2 Certificate Management Architecture

The trust hierarchy is organized as a tree structure with a single CI Plus 2nd Root of Trust (2nd ROT). There is only one tree for all participants in CI Plus 2nd Root of Trust, see Figure 6.2.

![Figure 6.2: Certificate Hierarchy Tree](image)

There are four different types of certificates.

- **2nd Root certificate**
  - issued by the 2nd ROT
  - self-signed
  - only one root certificate exists for all of CI Plus 2nd Root of Trust

- **Brand certificate**
  - issued by the 2nd ROT
  - signed with the private key of the 2nd Root certificate
  - one certificate of this type exists for each brand (or manufacturer)

- **Device certificate**
  - issued by the 2nd ROT
  - signed with the private key of the brand certificate
  - each single device has a unique device certificate
• Service operator certificate
  - issued by the 2nd ROT
  - signed with the private key of the 2nd Root certificate
  - one certificate of this type exists for each service operator

Each certificate contains a public key (MDP/HDP) for which there is a corresponding private key (MDQ/HDQ).

Each Host and CICAM shall integrate the following certificate related information at manufacturing time:
• the CI Plus 2nd Root certificate
• the brand certificate
• the device certificate
• the private key corresponding to the device certificate (MDQ or HDQ, see Table 5.2 of CI Plus Specification 1.3 [2])

Unlike other certificates, the service operator certificate does not have to be integrated into the Host or CICAM at time of manufacturing.

6.3.3 Certificate Formats

As defined in CI Plus Specification 1.3 [2] clause 9.3 except that references to RFC3280 shall be replaced by references to RFC5280 [20].

6.3.3.1 version


6.3.3.2 serial number

As defined in CI Plus Specification 1.3 [2] clause 9.3.2.

6.3.3.3 signature

All certificates use RSASSA-PSS signatures as defined in PKCS#1v2.1 [18], clause 8.1.1.

The fields of the RSASSA-PSS-params shall have values as defined in Table 6.3:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>hashAlgorithm</td>
<td>SHA-256</td>
</tr>
<tr>
<td>maskGenAlgorithm</td>
<td>MGF1 using SHA-256</td>
</tr>
<tr>
<td>saltLength</td>
<td>32 bytes</td>
</tr>
<tr>
<td>trailerField</td>
<td>one byte: 0xbc</td>
</tr>
</tbody>
</table>

The corresponding ASN.1 object identifiers are:

```
id-RSASSA-PSS OBJECT IDENTIFIER ::= { pkcs-1 10 }
pkcs-1 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}
rSASSA-PSS-Default-Params RSASSA-PSS-Params ::= {
  sha256Identifier, mgf1SHA256Identifier, 32, 1}
sha256Identifier AlgorithmIdentifier ::= {id-sha256, NULL}
id-sha256 OBJECT IDENTIFIER ::= {
  joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
  csor(3) nistalgorithm(4) hashalgs(2) 1 }
```
mgf1SHA256Identifier AlgorithmIdentifier ::= { id-mgf1, sha256Identifier }

6.3.3.4 issuer

As defined in CI Plus Specification 1.3 [2] clause 9.3.4 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20], and the following definitions shall replace those in CI Plus Specification 1.3 [2] Table 9.2:

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certificate</td>
<td>CN: “CI Plus 2nd Root CA certificate”</td>
</tr>
<tr>
<td>Brand certificate</td>
<td>CN: “CI Plus 2nd Root CA certificate”</td>
</tr>
<tr>
<td>Device certificate</td>
<td>CN: “CI Plus 2nd ROT for &lt;brand name&gt;”</td>
</tr>
<tr>
<td>Service operator certificate</td>
<td>CN: “CI Plus 2nd Root CA certificate”</td>
</tr>
</tbody>
</table>

NOTE: Attributes not listed remain as defined in CI Plus Specification 1.3 [2] Table 9.2.

6.3.3.5 validity

As defined in CI Plus Specification 1.3 [2] clause 9.3.5 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

6.3.3.6 subject

As defined in CI Plus Specification 1.3 [2] clause 9.3.6 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20], and the following definitions shall replace those in CI Plus Specification 1.3 [2] Table 9.3:

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certificate</td>
<td>CN: “CI Plus 2nd Root CA certificate”</td>
</tr>
<tr>
<td>Brand certificate</td>
<td>CN: “CI Plus 2nd ROT for &lt;brand name&gt;”</td>
</tr>
</tbody>
</table>

NOTE: Attributes not listed remain as defined in CI Plus Specification 1.3 [2] Table 9.3.

6.3.3.7 subjectPublicKeyInfo

As defined in CI Plus Specification 1.3 [2] clause 9.3.7 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

6.3.3.8 issuerUniqueID and subjectUniqueID

As defined in CI Plus Specification 1.3 [2] clause 9.3.8 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

6.3.3.9 extensions

As defined in CI Plus Specification 1.3 [2] clause 9.3.9 except that:

- Reference to RFC3280 shall be replaced by reference to RFC5280 [20].
- Table 9.4 of CI Plus Specification 1.3 [2] shall be replaced by Table 6.6:
### Table 6.6: Certificate Extensions

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Mandatory Extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certificate</td>
<td>key usage, subject key identifier, basic constraints</td>
</tr>
<tr>
<td>Brand certificate</td>
<td>key usage, subject key identifier, authority key identifier, basic constraints</td>
</tr>
<tr>
<td>Device certificate</td>
<td>key usage, authority key identifier, basic constraints, scrambler capabilities, CI Plus info (optional), CICAM brand identifier (CICAM only), Security Level</td>
</tr>
<tr>
<td>Service operator certificate</td>
<td>key usage, authority key identifier, basic constraints</td>
</tr>
</tbody>
</table>

#### 6.3.3.9.1 Subject Key Identifier

As defined in CI Plus Specification 1.3 [2] clause 9.3.9.1 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

#### 6.3.3.9.2 Authority Key Identifier

As defined in CI Plus Specification 1.3 [2] clause 9.3.9.2 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

#### 6.3.3.9.3 Key usage

As defined in CI Plus Specification 1.3 [2] clause 9.3.9.3 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

#### 6.3.3.9.4 Basic Constraints

As defined in CI Plus Specification 1.3 [2] clause 9.3.9.4 except that reference to RFC3280 shall be replaced by reference to RFC5280 [20].

#### 6.3.3.9.5 Scrambler capabilities

Scrambler capabilities is a private extension for CI Plus. It shall be present in each device certificate and shall be marked as critical. The ASN.1 definition is defined as

```asn1
id-pe-scramblerCapabilities OBJECT IDENTIFIER ::= { id-pe 25 }
id-pe ::= { 
  iso(1) identified-organization(3) dod(6) internet(1) security(5) 
  mechanisms(5) pkix(7) 1 }

ScramblerCapabilities ::= SEQUENCE { 
  capability INTEGER (0..MAX), 
  version INTEGER (0..MAX) }
```

The following values are supported for capability:
### Table 6.6: Capabilities Supported

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
</tr>
<tr>
<td>1</td>
<td>AES</td>
</tr>
<tr>
<td>all others</td>
<td>reserved for future use</td>
</tr>
</tbody>
</table>

#### 6.3.3.9.6 CI Plus Info


#### 6.3.3.9.7 CICAM brand identifier


#### 6.3.3.9.8 Security Level

Security Level is a private extension for CI Plus. It shall be present in each device certificate and shall not be marked as critical. The ASN.1 definition is defined as:

```plaintext
id-pe-securityLevel OBJECT IDENTIFIER ::= { id-pe 50 }
id-pe ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 1 }
SecurityLevel ::= INTEGER (0..MAX)
```

The following values are supported for SecurityLevel:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Standard Security Level</td>
</tr>
<tr>
<td>1</td>
<td>ECP Security Level</td>
</tr>
<tr>
<td>all others</td>
<td>reserved for future use for higher security levels</td>
</tr>
</tbody>
</table>

The CICAM may use the Security Level extension to determine the Security Level supported by the Host and decide whether to descramble content when the Host supports a sufficient Security Level for accessing such content.

A CICAM using the Security Level shall store the Security Level supported by the Host as part of the Authentication Context.

The Host may ignore the Security Level extension.

#### 6.3.3.10 signatureAlgorithm

This field is as defined in clause 6.3.3.3.

#### 6.3.3.11 signatureValue

This field is defined in RFC 5280 [20], section 4.1.1.3.

#### 6.3.4 Certificate Verification

As defined in CI Plus Specification 1.3 [2] clause 9.4 except the following:

- Reference to RFC3280 shall be replaced by reference to RFC5280 [20]
- The mandatory extensions are listed in section 6.3.3.9
7 Root of Trust Support

This chapter specifies the support of the Roots of Trust for devices compliant with the present document.

A CICAM shall support both the CI Plus Root of Trust defined in CI Plus Specification 1.3 [2] and the CI Plus 2nd Root of Trust defined in chapter 6 of the present document.

A Host shall support the CI Plus Root of Trust defined in CI Plus Specification 1.3 [2] and shall not support the CI Plus 2nd Root of Trust defined in chapter 6 of the present document.

The CI Plus 2nd Root of Trust Device Certificate shall indicate support of the Standard Security Level, as defined in clause 6.3.3.9.8.
### Annex A (normative): Parameters exchanged in APDUs

<table>
<thead>
<tr>
<th>datatype_id</th>
<th>Key or variable</th>
<th>No. of bits</th>
<th>Description</th>
<th>Defined in</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>1</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>2</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>3</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>4</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>5</td>
<td>HOST_ID</td>
<td>64</td>
<td>Generated by the ROT and included in the X.509 certificate.</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>6</td>
<td>CICAM_ID</td>
<td>64</td>
<td>Generated by the ROT and included in the X.509 certificate.</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>7</td>
<td>Host_BrandCert</td>
<td>variable</td>
<td>Host Brand Certificate</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>8</td>
<td>CICAM_BrandCert</td>
<td>variable</td>
<td>CICAM Brand Certificate</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>9</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>10</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>11</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>12</td>
<td>Kp</td>
<td>256</td>
<td>CICAM's key precursor to Host for CCK</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>13</td>
<td>DHPH</td>
<td>2048</td>
<td>DH Public Key of the Host</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>14</td>
<td>DHPM</td>
<td>2048</td>
<td>DH Public Key of the CICAM</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>15</td>
<td>Host_DevCert</td>
<td>variable</td>
<td>Host Device Certificate</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>16</td>
<td>CICAM_DevCert</td>
<td>variable</td>
<td>CICAM Device Certificate</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>17</td>
<td>Signature_A</td>
<td>2048</td>
<td>The signature of Host DH public key</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>18</td>
<td>Signature_B</td>
<td>2048</td>
<td>The signature of CICAM DH public key</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>19</td>
<td>auth_nonce</td>
<td>256</td>
<td>Random nonce of 256 bits generated by the CICAM and transmitted by the CICAM to the Host for use in the authentication protocol</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>20</td>
<td>Ns_Host</td>
<td>64</td>
<td>Host's challenge to CICAM for SAC</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>21</td>
<td>Ns_CICAM</td>
<td>64</td>
<td>CICAM's challenge to Host for SAC</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>22</td>
<td>AKH</td>
<td>256</td>
<td>Authentication Key Host</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>23</td>
<td>AKM</td>
<td>256</td>
<td>Authentication Key Module/CICAM</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>24</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>25</td>
<td>uri_message</td>
<td>64</td>
<td>Data message carrying the Usage Rules Information</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>26</td>
<td>program_number</td>
<td>16</td>
<td>MPEG program number</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>27</td>
<td>uri_confirm</td>
<td>256</td>
<td>Hash on the data confirmed by the Host</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>28</td>
<td>key register</td>
<td>8</td>
<td>Selection of the odd (1) or even (0) key register in the descrambler</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>29</td>
<td>uri_versions</td>
<td>256</td>
<td>Bitmask expressing the URI versions that can be supported by the Host. Format is ‘uimsbf’</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>30</td>
<td>status_field</td>
<td>8</td>
<td>Status field in APDU confirm messages</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>31</td>
<td>smr_data</td>
<td>variable</td>
<td>SRM for HDPU (note 1)</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>32</td>
<td>smr_confirm</td>
<td>256</td>
<td>Hash on the data confirmed by the Host</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>33</td>
<td>cicam_license</td>
<td>variable</td>
<td>Licence from CICAM associated with content (note 2)</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>34</td>
<td>license_status</td>
<td>8</td>
<td>Current status of the content licence</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>35</td>
<td>license_rcvd_status</td>
<td>8</td>
<td>Status from the exchange of content licence</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>36</td>
<td>Host_license</td>
<td>variable</td>
<td>Licence for which the Host requires current status. (note 2)</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>37</td>
<td>play_count</td>
<td>8</td>
<td>Remaining Play Count</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>38</td>
<td>operating_mode</td>
<td>8</td>
<td>Record operating mode</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>39</td>
<td>PINcode_data</td>
<td>variable</td>
<td>CICAM PIN code one byte for each pin code digit</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>40</td>
<td>record_start_status</td>
<td>8</td>
<td>CICAM status after a record_start protocol</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>41</td>
<td>mode_change_status</td>
<td>8</td>
<td>CICAM status after a change operating mode protocol</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>42</td>
<td>record_stop_status</td>
<td>8</td>
<td>CICAM status after a record_stop protocol</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>43</td>
<td>smr_data_dtcp</td>
<td>variable</td>
<td>SRM for DTCP (see note 3)</td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>44</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>45</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>46</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>47</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>48</td>
<td>Reserved for future use</td>
<td></td>
<td></td>
<td>CI Plus 1.3 [2]</td>
</tr>
<tr>
<td>49</td>
<td>csuv</td>
<td>8</td>
<td>Critical Security Update Version (see note 4)</td>
<td>Clause 4.9.1</td>
</tr>
</tbody>
</table>

---

Note 1: SRM for HDCP

Note 2: LICENCE FROM CICAM ASSOCIATED WITH CONTENT

Note 3: SRM for DTCP

Note 4: CSUV - Critical Security Update Version

Clause 4.9.1
<table>
<thead>
<tr>
<th>datatype_id</th>
<th>Key or variable</th>
<th>No. of bits</th>
<th>Description</th>
<th>Defined in</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>LTS_id</td>
<td>8</td>
<td>Local Transport Stream identifier</td>
<td>TS 103 205[3]</td>
</tr>
<tr>
<td>51</td>
<td>output_num</td>
<td>8</td>
<td>number of additional, simultaneous outputs of CI Plus controlled content to client devices</td>
<td>Bluebook A173-2[5]</td>
</tr>
</tbody>
</table>

52 to 255 Reserved for future use

**NOTE 1:** SRMs for HDCP are defined in the HDCP specification [8] and [9]. First generation SRMs do not exceed 5 kilobytes. Second generation HDCP v2.x SRMs may be larger than 5 kilobytes.

**NOTE 2:** Licenses are not zero length, and are padded to the next byte boundary. Licenses are no larger than 1024 bytes.

**NOTE 3:** SRMs for DTCP are defined in the DTCP specification [10]. First generation SRMs do not exceed 5 kilobytes.

**NOTE 4:** This definition replaces the reservation for SRM from CI Plus 1.3 [2]
Annex B (Informative): DVB-IPTV FCC/RET in the CICAM

This annex describes a typical usage of the LSC resources where the CAM uses the CICAM Player Mode to implement an IPTV client supporting the FCC and RET.

Figure B.1 depicts the implementation of an IPTV client with the support of FCC and RET in the CICAM, where the FCC Server is compliant with the definition of Annex I of DVB-IPTV [13]. The figure shows the involved LSC sessions and their corresponding device type is indicated in table B.1.

**Figure B.1: LSC sessions for FCC use case**

<table>
<thead>
<tr>
<th>LSC Session</th>
<th>Device Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x60 (IP connection)</td>
<td>Session for the RET request (of the unicast traffic) and FCC termination message</td>
</tr>
<tr>
<td>2</td>
<td>0x70 (Hybrid connection)</td>
<td>Session for RET request (of multicast) and FCC request. The reply consists of FCC information, RET sender reports and the unicast burst (and RET packets)</td>
</tr>
<tr>
<td>3</td>
<td>0x60 (IP connection)</td>
<td>Session for the Management Channel for configuration of the FCC client</td>
</tr>
<tr>
<td>4</td>
<td>0x70 (Hybrid connection)</td>
<td>Multicast session – initiated by an IGMP request</td>
</tr>
<tr>
<td>5</td>
<td>0x60 (IP connection)</td>
<td>Multicast session for FCC reporting channel</td>
</tr>
</tbody>
</table>
Some further LSC sessions may be necessary for the purposes as described in the table B.2:

**Table B.2: LSC sessions for further usage**

<table>
<thead>
<tr>
<th>LSC Session</th>
<th>Device Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>0x70 (Hybrid connection)</td>
<td>Multicast session for audio – initiated by an IGMP request</td>
</tr>
<tr>
<td>7, 8</td>
<td>0x60 (IP connection)</td>
<td>x2 sessions for the CAS/DRM traffic</td>
</tr>
<tr>
<td>9</td>
<td>0x60 (IP connection)</td>
<td>Session for the quality monitoring traffic</td>
</tr>
<tr>
<td>10,11</td>
<td>0x60 (IP connection)</td>
<td>x2 sessions for authentication</td>
</tr>
</tbody>
</table>
Annex C (normative): Use of PKCS#1

RSA signatures shall be constructed using the implementation guidelines of RSA PKCS#1 [18].

The signature scheme shall be RSASSA-PSS.

SHA-256 is the underlying hash function.

The signatures shall be 2048 bits long.
## History

### Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4</td>
<td>29-Jun-2015</td>
<td>Publication for comments</td>
</tr>
<tr>
<td>1.4.1</td>
<td>20-Nov-2015</td>
<td>Update of reference [3] from DVB Bluebook A165 to ETSI TS 103 205 Typos error correction Clarification on handling of multiple CICAMs with Auxiliary File System resource</td>
</tr>
<tr>
<td>1.4.2</td>
<td>09-May-2016</td>
<td>Fixed typo errors for Content Control resource and LSC resource in Table 4.1 Fixed typo error for LSC resource identifier in Table 5.2 Consistent renumbering of tables Combination of Application MMI sections</td>
</tr>
<tr>
<td>1.4.3</td>
<td>18-Oct-2017</td>
<td>Introduction of the CI plus 2nd Root of Trust in chapter 6 Support of the 2nd Root of Trust becomes mandatory for CICAM (chapter 7)</td>
</tr>
</tbody>
</table>