CI Plus Specification v1.4.3 (2017-11)

Technical Specification

CI Plus Specification.
Content Security Extensions to the Common Interface.

CI Plus LLP
31 Chertsey Street,
Guildford,
Surrey,
GU1 4HD,
UK

A company registered in England and Wales
Registered Number: OC341596

Contents

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

[1] CI Plus Licensee Specification, available under licence from the CI Plus Trust Authority.

[2] CI Plus Specification V1.3.2 (03-2015): “Content Security Extensions to the Common Interface”.

[3] ETSI TS 103 205 V1.2.1 (2015-11): “Digital Video Broadcasting (DVB); Extensions to the CI Plus Specification”.

[4] CI Plus DEVICE INTERIM LICENSE AGREEMENT

[5] Bluebook A173-2 (2015-06): “Digital Video Broadcasting (DVB); Second Generation Common Interface (CI); Part 2: Extension to the CI Plus Specification”.

[6] ETSI TS 103 285 V1.1.1: “MPEG-DASH Profile for Transport of ISO BMFF Based DVB Services over IP Based Networks”.

[7] ISO/IEC 14496-12 (2012): "Information technology -- coding of audio-visual objects -- Part 12: ISO Base File Format".

[8] High-bandwidth Digital Content Protection System, Interface Independent Adaptation, Revision 2.0.

[9] High-bandwidth Digital Content Protection System, Interface Independent Adaptation, Revision 2.2.

[10] Digital Transmission Content Protection Specification Volume 1 (Informational Version) Revision 1.7.

[11] HbbTV 2.0 Specification (2015-05-01)

[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".

[13] ETSI TS 102 034 V1.5.1 (2014-05): “Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks”

[14] Open IPTV Forum Release 2 specification, volume 2 (V2.3): "Media Formats".

[15] EN 50221:1996 (February, 1997): “Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications”. https://www.dvb.org/resources/public/standards/En50221.V1.pdf

[16] ETSI TS 101 699 V1.1.1 (November, 1999): “Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification”.

[17] Bluebook A165 (2017-01): “Digital Video Broadcasting (DVB); Extensions to the CI Plus Specification https://www.dvb.org/resources/public/standards/a165_dvb_ci_plus_1_4_jan_2017.pdf

[18] RSA PKCS#1 v2.1: June 14, 2002. RSA Cryptography Standard, RSA security inc.

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[19] NIST Special Publication 800-90A Revision 1 (June 2015): Recommendation for Random Number Generation Using Deterministic Random Bit Generators

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

[20] RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (version 3).
https://www.ietf.org/rfc/rfc5280.txt

[21] CI Plus ILA Addendum for ECP

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]:

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

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 4.1: Mandatory resources

Resource Name	Identifier	Class	Type	Version	Comment	Specification
Resource Manager	00 01 00 41	1	1	1		EN 50221 [15]
	00 01 00 42	1	1	2		TS 101 699 [16]
Application Information	00 02 00 41	2	1	1		EN50221 [15]
	00 02 00 42	2	1	2		TS 101 699 [16]
	00 02 00 43	2	1	3		CI Plus 1.3 [2]
	00 02 00 45	2	1	5		Bluebook A173-2 [5]
Conditional Access Support	00 03 00 41	3	1	1		EN 50221 [15]
Host Control	00 20 00 41	32	1	1		EN 50221 [15]
	00 20 00 42	32	1	2		CI Plus 1.3 [2]
	00 20 00 43	32	1	3		TS 103 205 [3]
Date-Time	00 24 00 41	36	1	1		EN 50221 [15]
MMI	00 40 00 41	64	1	1	High level only	EN 50221 [15]
LSC	00 60 60 01	96	384	1	where Host IP support exists	EN 50221 [15]
	00 60 60 02	96	384	2	where Host IP support exists	CI Plus 1.3 [2]
	00 60 60 03	96	384	3	where Host IP support exists	CI Plus 1.3 [2]
	00 60 60 04	96	384	4	where Host IP support exists	TS 103 205 [3]
Content Control	00 8C 10 01	140	64	1		CI Plus 1.3 [2]
	00 8C 10 02	140	64	2		CI Plus 1.3 [2]
	00 8C 10 04	140	64	4		Bluebook A173-2 [5]
Host Lang & Country	00 8D 10 01	141	64	1		CI Plus 1.3 [2]
CICAM Upgrade	00 8E 10 01	142	64	1		CI Plus 1.3 [2]
Operator Profile	00 8F 10 01	143	64	1		CI Plus 1.3 [2]
	00 8F 10 02	143	64	2		TS 103 205 [3]
Application MMI	00 41 00 41	65	1	1		TS 101 699 [16]
	00 41 00 42	65	1	2	Mandatory for CICAM Optional for Host	CI Plus 1.3 [2]

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 4.2: critical security update version protocol

Step	Action	APDU	Content		
1	CICAM requests the Host critical security update version	cc_sac_data_req	request_datatype_nbr=1		
			index	**datatype_id**	
			0	49 (csuv)	
2	Host sends an acknowledgement with its critical security update	cc_sac_data_cnf	send_datatype_nbr=1		
			index	**datatype_id**	**datatype_len**
			0	49 (csuv)	8 bits

	version to the CICAM				

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 4.3: scrambler capabilities

Value	Meaning
0	Forbidden (note 1)
1	AES
all others	reserved for future use

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 5.1: Mandatory resources for Multi-stream

Resource Name	Identifier	Class	Type	Version	Specification
Conditional Access Support	00 03 00 81	3	2	1	TS 103 205 [3]

Host Control	00 20 00 81	32	2	1	TS 103 205 [3]
MMI	00 40 00 81	64	2	1	TS 103 205 [3]
Content Control	00 8C 10 42	140	65	2	Bluebook A173-2 [5]
Application MMI	00 41 00 81	65	2	1	TS 103 205 [3]
Multi-stream	00 90 00 41	144	1	1	TS 103 205 [3]

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} (Kp, 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 5.2: Mandatory resources for CICAM Player Mode

Resource Name	Identifier	Class	Type	Version	Specification
CICAM Player	00 93 00 41	147	1	1	TS 103 205 [3]
LSC	00 60 70 04	96	448	4	TS 103 205 [3]

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 5.3: Mandatory resources for Host Player Mode

Resource Name	Identifier	Class	Type	Version	Specification
Sample Decryption	00 92 00 41	146	1	1	TS 103 205 [3]

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 5.4: Mandatory resources for HbbTV CICAM AppMMI Application

Resource Name	Identifier	Class	Type	Version	Specification
Auxiliary File System	00 91 00 41	145	1	1	TS 103 205 [3]

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 CITransportType (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 6.1: CC system ID and Content Control Resource version

CC system ID supported by Host	**cc_system_id_bitmask**			
	CC v1 (00 8C 10 01)	**CC v2 (00 8C 10 02)**	**CC v4 (00 8C 10 04)**	**CC v2 for multi-stream (00 8C 10 42)**
Only CC system ID 1	0b00000001	0b00000001	0b00000001	0b00000001
CC system ID 1 and 2	0b00000001	0b00000001	0b00000011	0b00000011
Only CC system ID 2	Not Applicable (see Note 1)	Not Applicable (see Note 1)	0b00000010	0b00000010
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 6.2: Host Capability Evaluation

Step	Action	APDU	Content
1	CICAM requests the Host's CC system ID bitmask	cc_open_req	
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 6.1below:

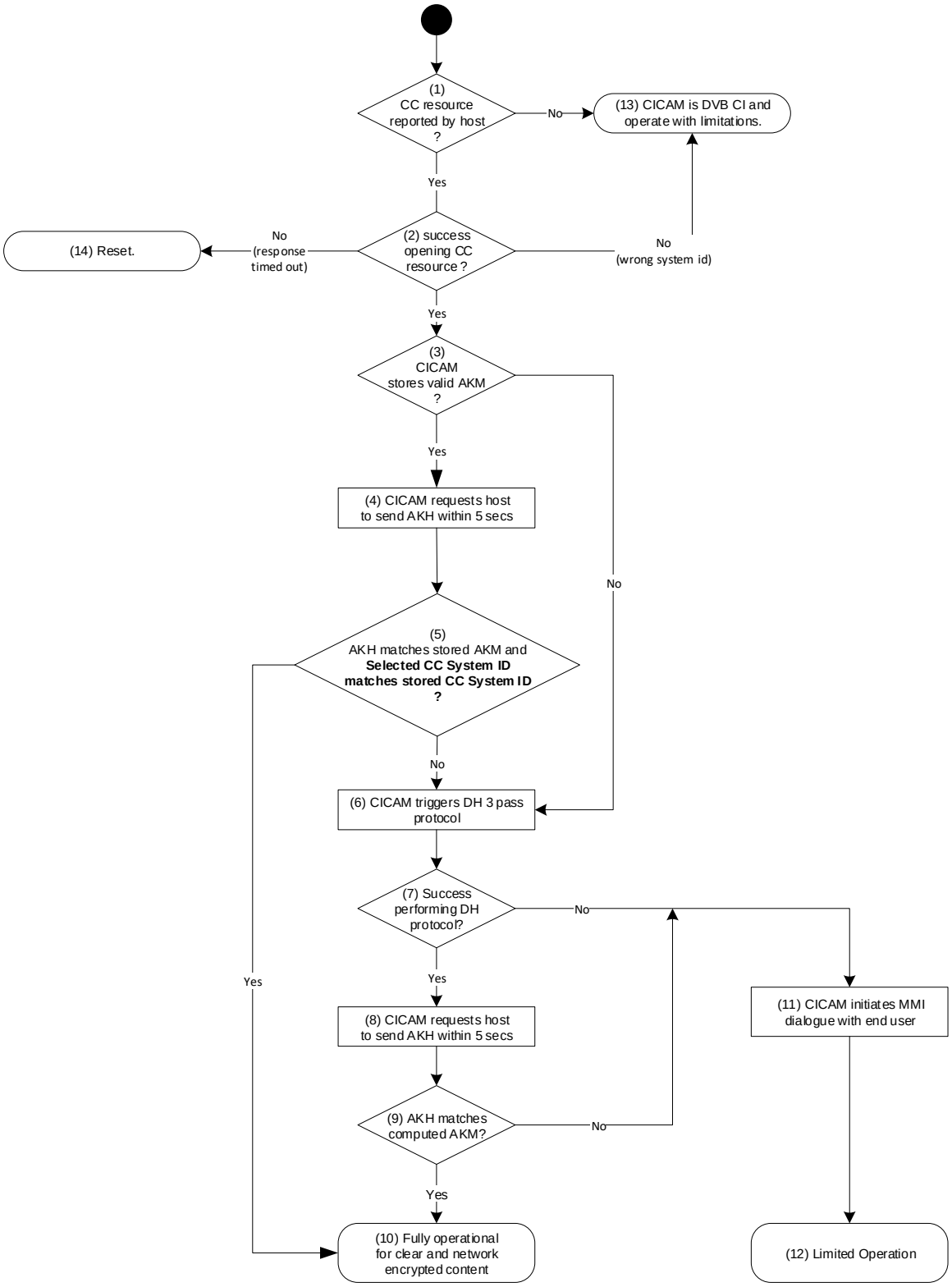

Figure 6.1: Overview of CICAM and Host in the CC Operation (Informative)

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.

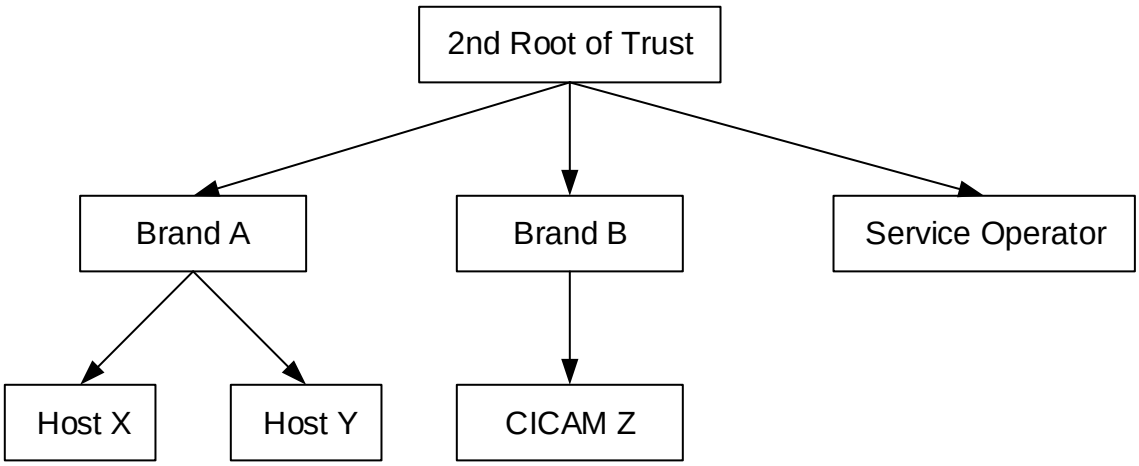

Figure 6.2: Certificate Hierarchy Tree

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

As defined in CI Plus Specification 1.3 [2] clause 9.3.1.

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 6.3: Certificate Signature Algorithm

Parameter	Value
hashAlgorithm	SHA-256
maskGenAlgorithm	MGF1 using SHA-256
saltLength	32 bytes
trailerField	one byte: 0xbc

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 6.4: Certificate Issuer

Certificate type	Issuer
Root certificate	CN: “CI Plus 2nd Root CA certificate”
Brand certificate	CN: “CI Plus 2nd Root CA certificate”
Device certificate	CN: “CI Plus 2nd ROT for <brand name>”
Service operator certificate	CN: “CI Plus 2nd Root CA certificate”
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 6.5: Certificate Subject

Certificate type	Subject
Root certificate	CN: “CI Plus 2nd Root CA certificate”
Brand certificate	CN: “CI Plus 2nd ROT for <brand name>”
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

Certificate Type	Mandatory Extensions
Root certificate	key usage subject key identifier basic constraints
Brand certificate	key usage subject key identifier authority key identifier basic constraints
Device certificate	key usage authority key identifier basic constraints scrambler capabilities CI Plus info (optional) CICAM brand identifier (CICAM only) Security Level
Service operator certificate	key usage authority key identifier basic constraints

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

```
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

Value	Meaning
0	Reserved
1	AES
all others	reserved for future use

6.3.3.9.6 CI Plus Info

As defined in CI Plus Specification 1.3 [2] clause 9.3.9.6.

6.3.3.9.7 CICAM brand identifier

As defined in CI Plus Specification 1.3 [2] clause 9.3.9.7.

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:

```
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 6.7: Security Levels Supported

Value	Meaning
0	Standard Security Level
1	ECP Security Level
all others	reserved for future use for higher security levels

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

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

datatype_id	Key or variable	No. of bits	Description	Defined in
50	LTS_id	8	Local Transport Stream identifier	TS 103 205[3]
51	output_num	8	number of additional, simultaneous outputs of CI Plus controlled content to client devices	Bluebook A173-2[5]
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 a 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]. Th

e 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

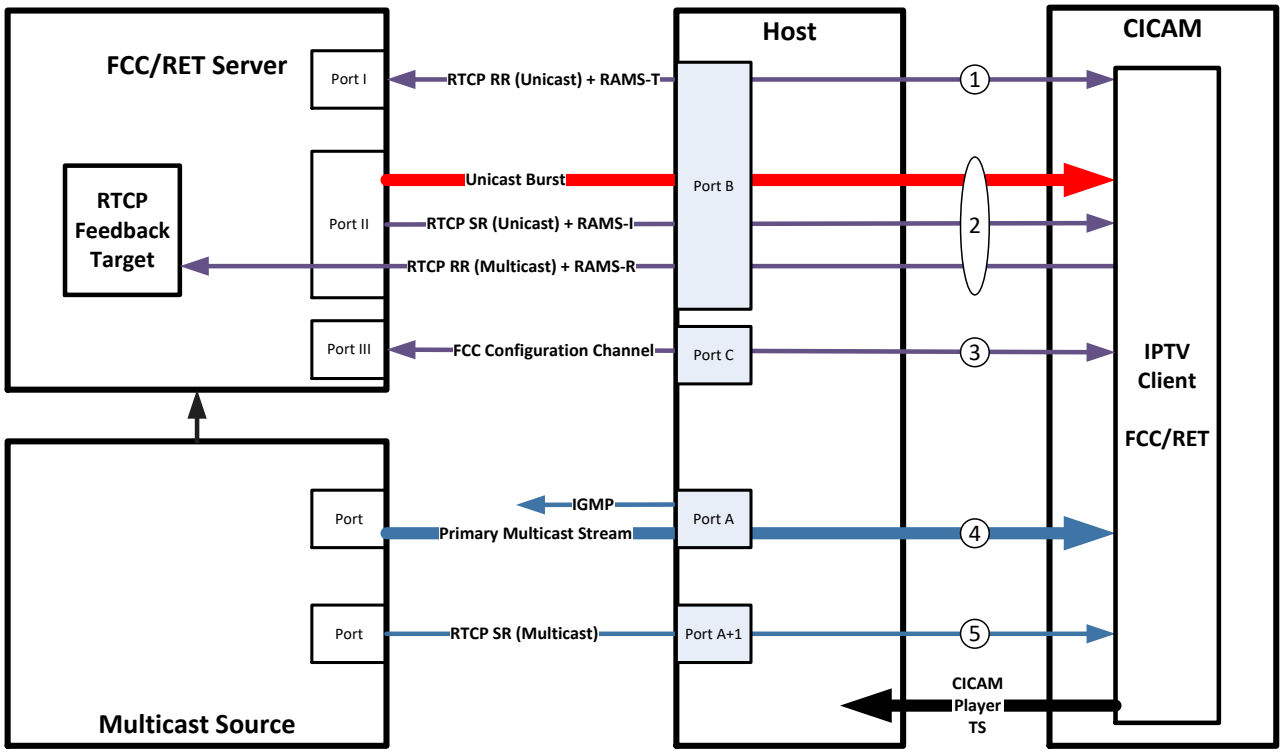

Table B.1: LSC sessions for FCC use case

LSC Session	Device Type	Purpose
1	0x60 (IP connection)	Session for the RET request (of the unicast traffic) and FCC termination message
2	0x70 (Hybrid connection)	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)
3	0x60 (IP connection)	Session for the Management Channel for configuration of the FCC client
4	0x70 (Hybrid connection)	Multicast session – initiated by an IGMP request
5	0x60 (IP connection)	Multicast session for FCC reporting channel

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

LSC Session	Device Type	Purpose
6	0x70 (Hybrid connection)	Multicast session for audio – initiated by an IGMP request
7, 8	0x60 (IP connection)	x2sessions for the CAS/DRM traffic
9	0x60 (IP connection)	Session for the quality monitoring traffic
10,11	0x60 (IP connection)	x2 sessions for authentication

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		
Version	**Date**	**Description**
1.4	29-Jun-2015	Publication for comments
1.4.1	20-Nov-2015	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
1.4.2	09-May-2016	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
1.4.3	18-Oct-2017	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)