

ANSI/CTA Standard

SD Card Common Interface Standard

ANSI/CTA-2040

(Formerly ANSI/CEA-2040)

July 2011



NOTICE

Consumer Technology Association (CTA)™ Standards, Bulletins and other technical publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards, Bulletins and other technical publications shall not in any respect preclude any member or nonmember of the Consumer Technology Association from manufacturing or selling products not conforming to such Standards, Bulletins or other technical publications, nor shall the existence of such Standards, Bulletins and other technical publications preclude their voluntary use by those other than Consumer Technology Association members, whether the standard is to be used either domestically or internationally.

Standards, Bulletins and other technical publications are adopted by the Consumer Technology Association in accordance with the American National Standards Institute (ANSI) patent policy. By such action, the Consumer Technology Association does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard, Bulletin or other technical publication.

This document does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this document to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

This document is copyrighted by the Consumer Technology Association and may not be reproduced, in whole or part, without written permission. Federal copyright law prohibits unauthorized reproduction of this document by any means. Organizations may obtain permission to reproduce a limited number of copies by entering into a license agreement. Requests to reproduce text, data, charts, figures or other material should be made to the Consumer Technology Association.

(Formulated under the cognizance of the CTA **R4.8 DTV Interface Subcommittee.**)

Published by
©CONSUMER TECHNOLOGY ASSOCIATION 2015
Technology & Standards Department
www.CTA.tech

All rights reserved

FOREWORD

This standard was developed under the auspices of the Consumer Electronics Association (CEA) R4.8 DTV Subcommittee.

Copyright Consumer Technology Association
Provided by IHS Markit under license with CTA
No reproduction or networking permitted without license from IHS
Full document details: CTA CTA-2040 2011

CONTENTS

1.	Scope.....	1
2.	Normative References	1
2.1	Normative Reference List.....	1
2.2	Normative Reference Acquisition Lists	1
3.	Acronyms.....	2
4.	Definitions.....	2
5.	Overview	3
5.1	Architecture	3
5.2	Physical Interface.....	3
5.3	Logical Interface.....	3
5.4	Form Factor	3
6.	Transport Protocol	4
6.1	Writing Data to the CI Module	4
6.2	Reading Data from the CI Module.....	5
7.	Text Strings.....	7
8.	Workflow	8
8.1	Workflow	8
8.1.1	Initialization Sequence	8
8.1.2	EMM Reception.....	8
8.1.3	Media Service Decryption	9
8.2	Commands.....	9
8.2.1	Commands Tags	9
8.2.2	Initialization Commands.....	9
8.2.2.1	Reset (0x01)	9
8.2.2.1.1	Command.....	10
8.2.2.1.2	Response	10
8.2.2.2	Get Parameters (0x02)	11
8.2.2.2.1	Command.....	11
8.2.2.2.2	Response	13
8.2.2.3	Get CA Information (0x03).....	14
8.2.2.3.1	Command.....	14
8.2.2.3.2	Response	15
8.2.2.4	SAC Information Exchange (0x06)	15
8.2.2.4.1	Command.....	16

8.2.2.4.2	Response	17
9.	Class 0 – Live Stream Handling	18
9.1	Open Session (0x04)	18
9.1.1	Command	18
9.1.1.1	ISMACryp Configuration	20
9.1.1.2	IPSec configuration	21
9.1.2	Response	21
9.2	Close Session (0x05)	22
9.2.1	Command	22
9.2.2	Response	22
9.3	Send Broadcast Data (0x10)	22
9.3.1	Additional Specification for Class 1 Operation	23
9.3.2	Command	23
9.3.2.1	EMM Data Block	23
9.3.2.2	ECM Data Block	24
9.3.2.3	Media Data Block	24
9.3.3	Response	25
9.4	Notification Management (0x11)	25
9.4.1	Command	26
9.4.2	Response	26
9.4.2.1	User Notification Data Block	27
9.4.2.2	Product Notification Data Block	27
10.	Class 1 – DVR	27
10.1	Workflow	27
10.1.1	Recording	27
10.1.2	Playback	28
10.1.3	Playback of an Open Session	29
10.2	Storage Information (0x20)	29
10.2.1	Command	30
10.2.2	Response	30
10.2.2.1	Record Descriptor	31
10.3	Recorded Session Management (0x26)	32
10.3.1	Command	32
10.3.2	Response	33
10.4	Start Recording (0x21)	33
10.4.1	Command	33
10.4.2	Response	34

10.5	Stop Recording (0x22)	35
10.5.1	Command	35
10.5.2	Response	35
10.6	Start Playback (0x23)	36
10.6.1	Command	36
10.6.2	Response	37
10.7	Stop Playback (0x24)	37
10.7.1	Command	37
10.7.2	Response	38
10.8	Seek (0x25).....	38
10.8.1	Command	38
10.8.2	Response	39
11.	Class 2 – Product Management	39
11.1	Workflow	40
11.2	Get Product List/Details (0x30)	40
11.2.1	Command	40
11.2.2	Response	41
11.2.2.1	Data Blocks.....	42
11.2.2.1.1	Product Name Block	42
11.2.2.1.2	Product Type Block	42
11.2.2.1.3	Product Description Block	43
11.2.2.1.4	Product Start Date Block.....	43
11.2.2.1.5	Product End Date Block	44

FIGURES

Figure 1 Terminal Architecture	3
Figure 2 Workflow	8
Figure 3 Record Workflow.....	28
Figure 4 Playback Workflow	28
Figure 5 Playback of Open Session	29
Figure 6 Product Management Workflow	40

Copyright Consumer Technology Association
 Provided by IHS Markit under license with CTA
 No reproduction or networking permitted without license from IHS
 Full document details: CTA CTA-2040 2011

(This page intentionally left blank.)

Copyright Consumer Technology Association

SD Card Common Interface Standard

1. Scope

This document describes interfaces between a Common Interface Module (CI Module) located on a microSD card and a Terminal device. The purpose of this standard is to specify the hardware, signaling, and application interface between a digital consumer electronics device e.g. television receiver (hand-held, stationary or otherwise) and a small removable, replaceable CI Module that implements and embodies significant portions of a Conditional Access System (CAS).

2. Normative References

The following references contain provisions, which, through reference in this text, constitute normative provisions of this standard. At the time of publication, the editions indicated below were valid. All documents are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

2.1 Normative Reference List

1. ATSC A/65:2009, "Program and System Information for Terrestrial Broadcast and Cable", Advanced Television Systems Committee, 2009.
2. SD Memory Card Specifications, Part 1, Physical Layer Specification, v3.01, May 2010.
3. ISMA Encryption and Authentication Vers. 1.1, Internet Streaming Media Alliance, Sept. 15, 2006. Available at http://www.isma.tv/specs/ISMA_E&Aspec1.1.pdf
4. RFC 3640, "RTP Payload Format for Transport of MPEG-4 Elementary Streams", IETF.
5. RFC 3602, "The AES-CBC Cipher Algorithm and its use with IPsec", IETF.
6. ISO: "ISO 639.2, Code for the Representation of Names of Languages — Part 2: alpha-3 code," as maintained by the ISO 639/Joint Advisory Committee (ISO 639/JAC), <http://www.loc.gov/standards/iso639-2/iso639jac.html>.

2.2 Normative Reference Acquisition Lists

The normative references listed in section 1 may be acquired from the following sources:

ATSC Standards:

- Advanced Television Systems Committee (ATSC), 1750 K Street, N.W., Suite 1200, Washington, DC 20006, Phone 202-872-9160; Fax 202-872-9161; Fax 202-828-3131; Internet <http://www.atsc.org>

DVB Registry:

- DVB Services Sàrl is 17A Ancienne Route, CH -1218 le Grand Saconnex, Switzerland; Internet http://www.dvbservices.com/identifiers/cp_system_id.

SD Memory Card specifications:

- SD Association, c/o Global Inventures, Inc., 2400 Camino Ramon, Suite 375, San Ramon, CA 94583; Phone 925-275-6615; Fax 925-886-4870; Internet <http://www.sdcard.org>

Internet Engineering Task Force standards:

- IETF Secretariat, c/o Association Management Solutions, LLC (AMS), 48377 Fremont Blvd., Suite 117, Fremont, California 94538; Phone: 510-492-4080; Fax: 510-492-4001; Internet: <http://www.ietf.org>

Internet Streaming Media Alliance specifications:

- Internet Streaming Media Alliance, Presidio of San Francisco, P.O. Box 29920, 572 B Ruger Street, San Francisco, CA 94129-0920; Phone: 415-561-6276; Fax: 415-561-6120; Internet <http://www.isma.tv>

ISO standards:

- Library of Congress via <http://www.loc.gov/standards/iso639-2/langhome.html>

3. Acronyms

AU	Access Unit
CAS	Conditional Access System
CI	Common Interface
CID	Card Identification register
CP	Copy Protection
ECM	Entitlement Control Message
EMM	Entitlement Management Message
ESP	Encapsulating Security Payload, part of the IPsec protocol suite
ESG	Electronic Service Guide
IP	Internet Protocol
PNM	Product Name
SAC	Secure Authenticated Channel

4. Definitions

Closed Recording Session – A Recording Session that is not in progress and no **data** may be added to it.

Common Interface Module – A small device, not working by itself, designed to run specialized conditional access processing in association with a Terminal.

Open Recording Session – A Recording Session that is in progress and **data** may be added to it.

Recording Session – The result of all the **data** received for a particular Service over a period of time.

Service - A set of synchronized media streams delivered in a time-constrained or unconstrained manner for immediate consumption (during the reception).

Terminal – The television receiver (not including the CI Module) device with a CI Module interface

The diagram illustrates the system architecture, divided into two main sections: Terminal and CI Module, separated by a vertical dashed line.

Terminal Section:

- Signal** enters from the bottom left.
- Demod Demux** (solid box) receives the signal and outputs to **Packet Filter** (solid box).
- Packet Filter** outputs to **SAC Decryption** (dashed box).
- SAC Decryption** outputs **AV** (Audio/Video) to **Media Player** (solid box).
- SAC Decryption** also receives a **SAC Key** (dashed line) from the **HTTP(S) client (example)** (dashed box).
- HTTP(S) client (example)** is connected to **Terminal Application (example)** (dashed box) via a bidirectional arrow.

CI Module Section:

- Packet Filter** (solid box) receives input from the Terminal's Packet Filter and outputs to **Descrambler (ISMALCryp/IPSec/SRTP)** (solid box).
- Descrambler** outputs **AV** to **SAC Encryption** (dashed box).
- SAC Encryption** outputs to **CAS** (solid box).
- CAS** outputs **TEK** (Temporary Encryption Key) to the **Descrambler**.
- CAS** also receives **ECM / EMM** (Entitlement Control Message / Event Management Message) from the **Packet Filter**.
- CAS** outputs a **SAC Key** (dashed line) to the **HTTP(S) server (example)** (dashed box).
- HTTP(S) server (example)** is connected to **HTTP(S) client (example)** via a bidirectional arrow.

The CI Module based system consists of a Terminal and a CI Module. The Terminal provides the reception and decoding functionality whilst the CI Module provides the decryption functionality. The Terminal and the CI Module are connected through the Common Interface. Please refer to the documentation of the applicable broadcast standard for a detailed description of the Terminal architecture and requirements.

The Common Interface specified in this document allows independent operation of both Terminal and the CI Module. In the case that the CI Module is not present in the Terminal, the Terminal should be able to render only the unencrypted broadcast channels. In case that the CI Module is present in the Terminal the encrypted broadcast channels shall be presented to the CI Module for decryption.

5.2 Physical Interface

5.3 Logical Interface

5.4 Form Factor

100 90 80 70 60 50 40 30 20 10 0

6. Transport Protocol

Communications between the Terminal and the CI Module shall consist of a series of pairs of write commands followed by read commands.

All CI Module commands shall be formatted using the READ_SINGLE_BLOCK (CMD17), READ_MULTIPLE_BLOCK (CMD18), WRITE_SINGLE_BLOCK (CMD24) and WRITE_MULTIPLE_BLOCK (CMD25) commands. The "multiple block" commands should be used for performance reasons.

For all commands (CMD17, CMD18, CMD24 and CMD25), the "data address" on bits 39 to 8 (inclusive) shall be set to 0xFFFF.

A read command shall immediately follow the write command.

If the CI Module is not ready to answer the command carried in the write command, it shall respond to the read command with a Status Word of 0x6E04 (Busy) and the Terminal shall issue the read command once more after waiting the period of time described in the delay field, see section 8.2.2.1.2.

Note that all commands except for "Send Broadcast Data" (9.3) will fit in a single 512 byte data block (see 4.3.4 of [2]). Responses to commands will fit in a single 512 byte data block (see 4.3.3 of [2]), except for some responses to "SAC Information Exchange" (8.2.2.4), "Notification management" (9.4), "Storage Information" (10.2), and "Get Product List/Details" (11.2), and except for most responses to "Send Broadcast Data" (9.3).

6.1 Writing Data to the CI Module

The payload of the write commands (CMD24 and CMD25) shall be as follows (general form):

Syntax	Bytes	Format
head_string	32	(fixed)
tag	1	uimsbf
length	2	uimsbf
data	length	

head_string – The **head_string** constant value is used by the CI Module to differentiate regular file write commands from commands meant for the CAS functionality of the CI Module. The **head_string** shall be 0x2AB5534443492A436F6D6D616E642A48656164537472696E672A57726974652A (32 bytes). Note that the **head_string** value for write operations is different from that of read operations.

tag – The **tag** field identifies the command sent.

length – The **length** field indicates the number of bytes following this field (not including the **length** field bytes) in this message.

data – The optional **data** field contains the details of the command. If the **length** field is zero, there shall be no bytes of **data** (no payload).

The values of **tag**, **length** and **data** vary by the message written.

6.2 Reading Data from the CI Module

The payload of the read commands (CMD17 and CMD18) shall be as follows (general form):

Syntax	Bytes	Format
head_string	32	(fixed)
tag	1	uimsbf
length	2	uimsbf
data	length	
status_word	2	uimsbf
status_flags	2	bslbf

head_string – The **head_string** constant value is used by the CI Module to differentiate regular file read commands from commands meant for the CAS functionality of the CI module. The **head_string** shall be 0x2AB5534443492A436F6D6D616E642A48656164537472696E672A726561642A2A (32 bytes). Note that the **head_string** value for read operations is different from that of write operations.

tag – The **tag** field identifies the command responded to.

length – The **length** field indicates the number of bytes of **data** that follow this field (not including the **length** field bytes, and not including the two bytes of **status_word** , and not including the two bytes of **status_flags**) in this message.

data – The optional **data** field contains the details of the command. If the **length** field is zero, there shall be no bytes of **data** (no payload).

status_word – The **status_word** is a response code. Possible values for the **status_word** are shown below. Some values are not returned for some commands.

status_word	Description
0x9000	Command executed normally
0x9240	Storage error
0x9500	No authorization
0x9501	ECM not received
0x9502	Invalid data format
0x9503	No corresponding CAS module
0x9504	EMM error in CAS module
0x9505	ECM error in CAS module
0x9506	Authorization about to expire
0x9507	CAS module banned
0x9508	Descrambler not configured
0x9509	Descrambler context count exceeded
0x950a	Session count exceeded
0x6dXX	Unrecognized command*
0x6e00	Incorrect command
0x6e01	Invalid argument
0x6e02	Missing information
0x6e03	End of file
0x6e04	Busy
0x6fXX	Technical error. No diagnostics available.*

* In these cases, the byte indicated as 'XX' will contain the **tag** value of the Command.

status_flags – The **status_flags** is a bit field used for indications from the CI Module to the Terminal. **status_flags** bit meanings shall be as shown below:

status_flags	Description
0bxxxx xxxx xxxx xxx1	Notification Pending
Other bits	reserved

The CI Module shall set the Notification Pending bit to indicate that information is ready to be supplied to the Terminal via the Notification Management command (see section 9.4 below). Upon receiving a response with the Notification Pending bit set, the Terminal may retrieve the pending information via the Notification Management command.

7. Text Strings

Text may be supplied by the CI Module to the Terminal which may then be displayed to the end user by the Terminal. The ATSC A/65 Multiple String Structure, as constrained below, shall be used to convey text strings when the CI Module supplies text to the Terminal. See ATSC A/65:2009 [1] Section 6.10.

The syntax for the Multiple String Structure is as shown below (included for convenience):

Syntax	Bytes	Format
multiple_string_structure() { number_strings for (i=0 ; i<n ; ++i) { ISO_639_language_code number_segments for (j=0 ; j<number_segments ; ++j) { compression_type mode number_bytes for (k=0 ; k<number_bytes ; ++k) { compressed_string_byte[k] } } } }	1 3 1 1 1 1 8	uimbsf uimbsf uimbsf uimbsf uimbsf uimbsf bslbf

compression_type – **compression_type** shall be 0x00 (no compression).

mode –The **mode** field shall be 0x42, indicating UTF-8 encoded character data.

8. Workflow

8.1 Workflow

The workflow when receiving audio/video/data between the Terminal and CI Module is described by the following diagram:

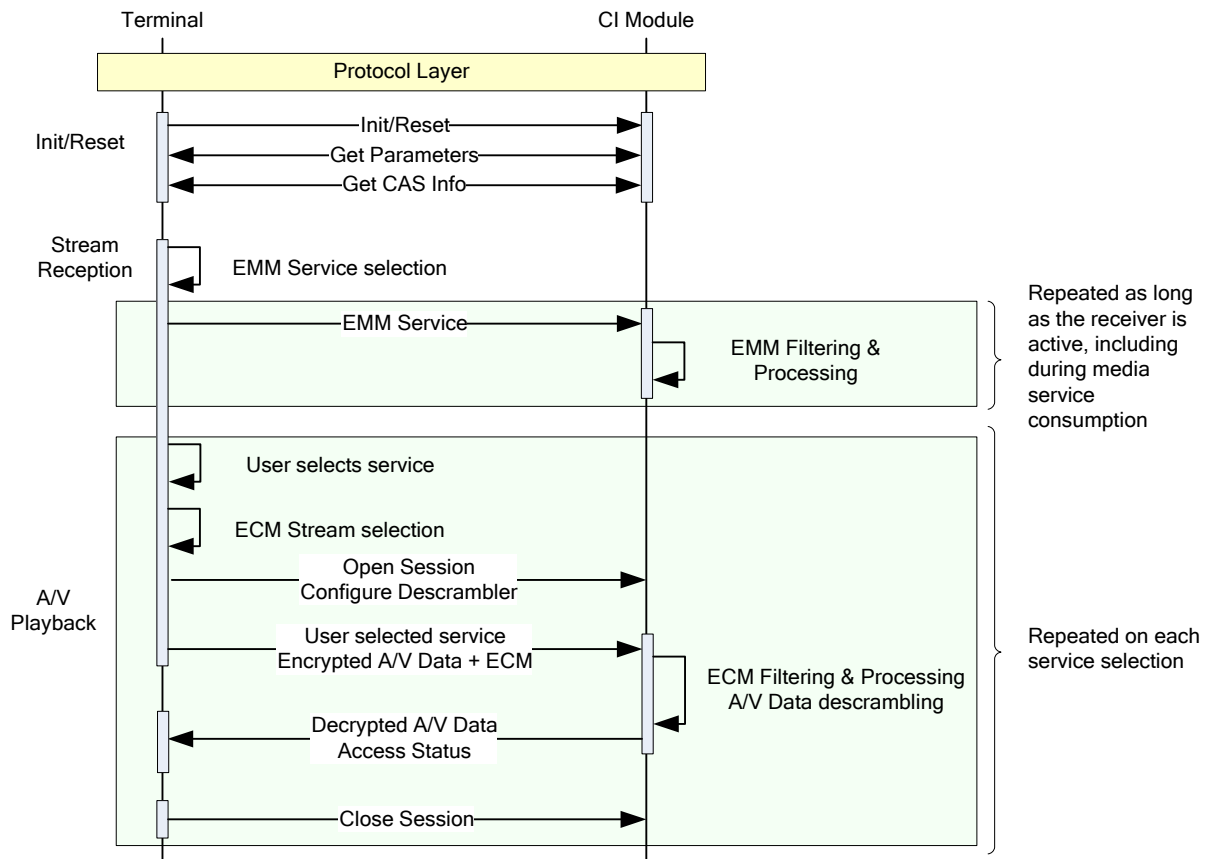


Figure 2 Workflow

8.1.1 Initialization Sequence

After the powerup (or hard reset) of the CI Module, the Terminal shall establish whether the SD card is a valid and compliant CI Module by retrieving its CID Register and extracting from it the Product Name (PNM). CI Modules compliant with this specification shall carry a PNM of 0xB5 53 44 43 49.¹ If the PNM is not equal to this value, the Terminal shall consider that the card is a regular storage device and may use it so.

The Terminal shall then perform a Reset exchange (reset of the CI Module functionality, not of the SD card), followed by a Get Parameters and a Get CAS Info exchange.

8.1.2 EMM Reception

EMM reception workflow shall be performed as soon as, and as long as, a media service (e.g. TV channel) is received and processed and in parallel to the media service reception.

¹ These five bytes are the ASCII representation of "µSDCI".