

# CTA Standard

**National Renewable Security  
Standard (NRSS)**

**CTA-679-C R-2013**

**(Formerly CEA-679-C R-2013)**

**October 2005**



**Consumer  
Technology  
Association™**

## NOTICE

Consumer Technology Association (CTA)<sup>TM</sup> 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.

*Note: The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.*

*By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher.*

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](http://www.CTA.tech)

All rights reserved

## FOREWORD

The National Renewable Security Standard provides a means for renewable security to be employed with digital consumer electronics devices such as digital television receivers and digital VCRs. Renewable security encompasses upgradeable, extensible, removable and replaceable security, and may be implemented with a variety of embedded and removable approaches that may vary in complexity, feature set and security level. This standard does not address intended applications for either Part A or Part B devices.

The National Renewable Security Standard provides two physical designs, one in part A and one in part B. Part A defines a removable and renewable security element form factor that is an extension of the ISO-7816 standard. Part B defines a removable and renewable security element based on the PCMCIA ("PC Card") form factor. The common attributes allow either an NRSS-A or NRSS-B device to provide security for applications involving pay and subscription cable or satellite television services, telephony, and all forms of electronic commerce.

The main differences between NRSS-A and NRSS-B devices are the range of capabilities and the capacity for extension. The NRSS-A interface is limited to 8 electrical contacts using serial communication, whereas the NRSS-B interface uses 68 electrical contacts and parallel communication. Potentially, the NRSS-A device could be smaller and less complex, while the NRSS-B device could be more robust and extensible.

The video distribution industries (cable TV, DBS, MMDS, etc.) are utilizing a variety of implementations for securing digital video: a) embedded, b) totally removable and replaceable, c) hybrid, and d) split.

Embedded security involves circuitry that is permanently installed within a consumer electronics host device (e.g., cable converter, DBS receiver, TV receiver).

Removable security involves circuitry that may be totally extracted from the host device; when security is removable, the consumer electronics device can be "secret-free".

A hybrid security system uses embedded circuitry but, if necessary, this circuitry may be upgraded or overridden and replaced with replaceable elements. Thus, embedded security may nonetheless be replaceable.

A split security system has both embedded circuitry that supports some security functions (e.g., descrambling) and replaceable circuitry that supports other security functions (e.g., key management).

Both NRSS-A and NRSS-B support all options except the embedded security.

The consumer electronics industry is looking for a digital standard "cable ready" television set, receiving both broadcast and cable digital services, that is secret-free and mass merchandiseable. The availability of NRSS-A and/or NRSS-B security elements allows support for the consumer electronics needs.

This discussion is provided in order to explain the environment in which this standard has been developed. This standard was developed under the auspices of the CEMA Technology & Standards/NCTA JEC National Renewable Security Standard (NRSS) Subcommittee.

(This page intentionally left blank.)

## PART A CONTENTS

<b>1 Introduction .....</b>	<b>1</b>
<b>2 Scope and Field of Application .....</b>	<b>1</b>
<b>3 Normative References .....</b>	<b>1</b>
3.1 Normative Reference List .....	1
3.2 Normative Reference Acquisition .....	1
<b>4 Definitions.....</b>	<b>2</b>
<b>5 General Electrical and Physical Characteristics .....</b>	<b>2</b>
<b>6 Exceptions and Additional Physical Characteristics .....</b>	<b>3</b>
<b>7 Exceptions and Additional Electrical Characteristics.....</b>	<b>3</b>
7.1 High-speed Data-in .....	4
7.2 High-speed Clock .....	4
7.3 High-speed Data-out.....	4
7.4 Functional Operations on High-speed Data .....	5
7.5 Communications Protocol and Flow Control .....	5
7.5.1 CA Module Implementation of Flow Control.....	5
7.5.2 Host Implementation of Flow Control.....	5
<b>8 Commands.....</b>	<b>6</b>
<b>9 General Commands .....</b>	<b>7</b>
9.1 Answer-to-Reset .....	7
9.2 Get CA Module Configuration .....	7
9.3 Get CA Module Status .....	8
9.4 Put CE device ID .....	10
9.5 Get Suggested ID.....	10
9.6 Put Host Configuration/Status .....	10
9.7 Get Requested Homing Time .....	11
<b>10 Purchase and Cancel IPPV Commands.....</b>	<b>11</b>
10.1 Put Purchase Action .....	11
10.2 Get Number of Purchase Offers.....	12
10.3 Get Purchase Offer Data .....	12
10.4 Get Purchase Offer Title .....	13
10.5 Put Purchase Action .....	13
10.6 Put Purchase Cancellation .....	14
10.7 Get Purchase Status .....	14
10.7.1 CA Status Byte.....	14
10.7.2 Program Status Byte .....	15
10.7.3 Status Byte Interpretation.....	15
10.8 Get Special Reason Message.....	15
<b>11 Purchase History Commands.....</b>	<b>16</b>
11.1 Get Purchase Record Length .....	16
11.2 Get Purchase Record .....	16
11.3 Put Purchase Data.....	17

11.4 Get Updated Purchase Slot Info.....	17
12 Chaining Commands .....	17
12.1 Get Number of Chaining Blocks .....	17
12.2 Get Block.....	18
12.3 Put Block .....	18
13 Reportback Commands.....	18
13.1 Get Open Reportback Request .....	18
13.2 Get Reportback Values .....	19
13.3 Get Reportback Message.....	19
13.4 Put Reportback Buffer .....	19
13.5 Put Reportback Status .....	19
14 Locks and Limits Commands .....	20
14.1 Get PIN.....	20
14.2 Put PIN .....	20
14.3 Get PIN Action Result .....	21
14.4 Get Lock State.....	22
14.5 Get User Parameter .....	22
14.6 Put User Parameter .....	22
15 Service Changes and Related Commands.....	23
15.1 Put Add-Service Packet Identification (PID) Numbers.....	23
15.2 Put Remove-Service Packet Identification (PID) Numbers .....	23
15.3 Get Decode Status for PIDs.....	23
15.4 Put CE Device PowerState.....	24
15.5 Get Forced Service Change.....	24
15.6 Put EMM PID.....	25
16 Display and Menu Commands.....	25
16.1 Get Display Message Size .....	25
16.2 Get Display Message.....	25
16.3 Get Alpha Box Request.....	26
16.4 Get Alpha Box Parameters .....	26
16.5 Put Alpha Box Input .....	26
16.6 Get Menu Request .....	26
16.7 Get Menu Parameters.....	27
16.8 Put User Response.....	27
17 Mail Handling Commands .....	27
17.1 Get Mail Message Length .....	27
17.2 Get Mail Message Text .....	27
18 Intercard Message Commands.....	28
18.1 Get Intercard Message Sizes.....	28
18.2 Get Intercard Message .....	28
18.3 Put Intercard Message .....	28
18.4 Put Card Numbers .....	28
19 NVM Storage Commands .....	28
19.1 Put NVM Available .....	28
19.2 Get Allocation Size .....	29
19.3 Put Allocation Tag.....	29
19.4 Get Operation and Tag.....	29
19.5 Put Operation Results.....	29

19.6 Put Read Data .....	29
19.7 Get Write Data .....	30
<b>20 Copy Protection Framework .....</b>	<b>30</b>
20.1 Service Provider [Informative] .....	30
20.2 Back Channel [Informative] .....	30
20.2.1 Service Provider Processing [Informative] .....	30
20.2.1.1 Checking Validity of Host Information [Informative].....	30
20.2.1.2 Host Revocation [Informative].....	30
20.3 CP System Negotiation .....	31
20.4 CA Module/Host Binding .....	31
20.4.1 Discrete Logarithm DH.....	31
20.4.2 Elliptic Curve DH.....	31
20.4.3 Needham-Schroeder Key Exchange Protocol .....	32
20.4.4 Computation of Kcpss and Kvalidated_cpss .....	32
20.5 Copy Control Information Definition .....	32
20.5.1 private_CCI.....	33
20.5.2 APS (Analog Protection System) Information .....	33
20.5.3 Copy Generation Management System (CGMS-A) Information.....	33
20.6 Scrambling .....	33
20.6.1 Key Derivation.....	34
20.6.1.1 ODD/EVEN Key Generation Formulae .....	34
20.6.1.2 Initial Key Derivation Procedure.....	35
20.6.1.3 Subsequent Key Derivation Procedure .....	36
20.6.2 Content Encryption .....	38
20.6.3 Transport Scrambling Control.....	38
20.7 Key Application for the Data Channel .....	39
20.8 CP Parameter Passing .....	39
<b>21 Copy Protection Commands.....</b>	<b>40</b>
21.1 PutCP_parameter.....	40
21.2 GetCP_Parameter .....	41
21.3 GetCACP_Request .....	41
21.4 PutCP_Synchro_Reply (CP Synchronization).....	41
<b>Annex A Serial Processing One MPEG-2 Data Stream Using Two Cards (Informative).....</b>	<b>42</b>
<b>Annex B Electrical Characteristics (Normative) .....</b>	<b>43</b>
<b>Annex C CA Device Physical Size Limitations (Normative) .....</b>	<b>44</b>
<b>Annex D A Particular Implementation (Informative).....</b>	<b>45</b>
<b>Annex E An Operational Scenario (Informative).....</b>	<b>46</b>
<b>Annex F CEA-679-C Part B Extensibility (Normative) .....</b>	<b>47</b>
<b>Annex G Stored CA Display Messages (Normative) .....</b>	<b>48</b>
<b>Annex H Homing Support in Hosts (Normative).....</b>	<b>49</b>
<b>Annex I Chaining support in Hosts (Informative) .....</b>	<b>50</b>
I.1 Description .....	50
I.2 Procedure .....	50
I.4 Menus .....	50

I.5 Requirements.....	50
-----------------------	----

## FIGURES

Figure 1 Timing Diagram.....	4
Figure 2 Flow Control, Next Byte at Total Guard Time (TGT).....	5
Figure 3 Flow Control, Next Byte After end_flow_control + X .....	6
Figure 4 Procedure for Initial CP key derivation.....	35
Figure 5 Procedure for Subsequent CP Key Derivation .....	37
Figure 6 Copy Protection Key Derivation Timeline .....	38
Figure 7 Implementation Example—Two NRSS Part A Modules in One Host Device .....	42
Figure 8 NRSS Part A Form Factor .....	44
Figure 9 Sample System Block Diagram .....	45

## TABLES

Table 1 Procedure for NRSS Part A Activation/Deactivation .....	3
Table 2 Additional Contacts Used in NRSS Part A.....	3
Table 3 Timing Diagram.....	4
Table 4 Definition of CA Module Status Bit n.....	9
Table 5 Definition of Host Status Bit n.....	10
Table 6 CP_system_ID_bitmask Bit Numbers.....	11
Table 7 Purchase Type .....	13
Table 8 CA Status Byte Field .....	15
Table 9 CP_system_ID.....	31
Table 10 CCI Types and Sizes .....	33
Table 11 Baseline CCI.....	33
Table 12 Analog Protection System.....	33
Table 13 CGMS Values .....	33
Table 14 Key Derivation Sequence Parameter/Key Sizes.....	34
Table 15 CP_transport_scrambling_control_field descriptor values.....	39
Table 16 Data Channel Message Encryption Parameter Sizes.....	39
Table 17 Copy Protection datatype_ID coding.....	40
Table 18 CP_system_ID.....	40
Table 19 NRSS Part A DC Electrical Characteristics.....	43
Table 20 NRSS Part A AC Electrical Characteristics.....	43



## PART B CONTENTS

<b>1 Introduction and Scope</b> .....	<b>53</b>
<b>2 Definitions</b> .....	<b>54</b>
<b>3 Normative References</b> .....	<b>54</b>
<b>3.1 Normative Reference List</b> .....	<b>54</b>
<b>3.2 Normative Reference Acquisition</b> .....	<b>55</b>
<b>4 Design Philosophy</b> .....	<b>55</b>
<b>4.1 Layering</b> .....	<b>55</b>
<b>4.2 Physical Implementation</b> .....	<b>56</b>
<b>4.3 Coding of Data</b> .....	<b>56</b>
<b>4.4 Extensibility</b> .....	<b>56</b>
<b>4.5 Incorporation of Existing Standards</b> .....	<b>56</b>
<b>5 Description and Architecture</b> .....	<b>56</b>
<b>5.1 Overview</b> .....	<b>56</b>
<b>5.2 Transport Stream Interface</b> .....	<b>56</b>
<b>5.3 Command Interface</b> .....	<b>57</b>
<b>5.4 Physical Requirements</b> .....	<b>57</b>
<b>5.4.1 Introduction</b> .....	<b>57</b>
<b>5.4.2 Data and Command Logical Connections</b> .....	<b>58</b>
<b>5.4.3 Connection and Disconnection Behavior</b> .....	<b>59</b>
<b>5.4.4 Multiple Modules</b> .....	<b>59</b>
<b>5.5 Operational Example</b> .....	<b>60</b>
<b>6 Transport stream interface (TSI)</b> .....	<b>60</b>
<b>6.1 TSI - physical, link layers</b> .....	<b>60</b>
<b>6.2 TSI - transport layer</b> .....	<b>60</b>
<b>6.3 TSI - upper layers</b> .....	<b>60</b>
<b>7 Command Interface - Transport &amp; session layers</b> .....	<b>61</b>
<b>7.1 Generic Transport Layer</b> .....	<b>61</b>
<b>7.1.1 Introduction</b> .....	<b>61</b>
<b>7.1.2 Transport Protocol Objects</b> .....	<b>62</b>
<b>7.1.3 Transport protocol</b> .....	<b>62</b>
<b>7.2 Session Layer</b> .....	<b>67</b>
<b>7.2.1 Introduction</b> .....	<b>67</b>
<b>7.2.2 Session Protocol Objects</b> .....	<b>67</b>
<b>7.2.3 Session Protocol</b> .....	<b>67</b>
<b>7.2.4 SPDU Structure</b> .....	<b>69</b>
<b>7.2.5 Transportation of SPDU</b> .....	<b>70</b>
<b>7.2.6 Session Headers Description</b> .....	<b>70</b>
<b>7.2.6.1 Open Session Request</b> .....	<b>70</b>
<b>7.2.6.2 Open Session Response</b> .....	<b>71</b>
<b>7.2.6.3 Create Session</b> .....	<b>72</b>
<b>7.2.6.4 Create Session Response</b> .....	<b>72</b>
<b>7.2.6.5 Close Session Request</b> .....	<b>72</b>
<b>7.2.6.6 Close Session Response</b> .....	<b>73</b>
<b>7.2.6.7 Session Number</b> .....	<b>73</b>
<b>7.2.7 Coding of the Session Tags</b> .....	<b>73</b>

<b>8 Command Interface—Application Layer</b> .....	<b>74</b>
<b>8.1 Introduction</b> .....	<b>74</b>
<b>8.2 Resources</b> .....	<b>74</b>
8.2.1 Introduction .....	74
8.2.2 Resource Identifier .....	75
8.2.3 Applications and Resource Providers.....	75
<b>8.3 Application Protocol Data Units</b> .....	<b>75</b>
8.3.1 Introduction .....	75
8.3.2 Chaining of APDU data fields .....	76
8.3.3 Transportation of APDU within SPDU .....	76
<b>8.4 System Management Resources</b> .....	<b>76</b>
<b>8.4.1 Resource Manager</b> .....	<b>76</b>
8.4.1.1 Resource Manager Protocol.....	77
8.4.1.2 Profile Inquiry .....	77
8.4.1.3 Profile Reply .....	77
8.4.1.4 Profile Changed.....	78
<b>8.4.2 Application Information</b> .....	<b>78</b>
8.4.2.1 Application Info Inquiry .....	78
8.4.2.2 Application Info .....	79
8.4.2.3 Enter Menu.....	79
<b>8.4.3 Conditional Access Support</b> .....	<b>79</b>
8.4.3.1 CA_Info Inquiry .....	80
8.4.3.2 CA_Info .....	80
8.4.3.3 Selection of services to be descrambled .....	80
8.4.3.4 CA_PMT .....	80
8.4.3.5 CA_PMT Reply.....	82
<b>8.5 Host Control and Information Resources</b> .....	<b>84</b>
<b>8.5.1 NRSS Host Control</b> .....	<b>84</b>
8.5.1.1 Tune .....	84
8.5.1.2 Replace .....	84
8.5.1.3 Clear Replace .....	85
8.5.1.4 Ask Release.....	85
<b>8.5.2 System Time</b> .....	<b>86</b>
8.5.2.1 System Time Inquiry .....	86
8.5.2.2 System Time .....	86
<b>8.6 Man-Machine Interface Resource</b> .....	<b>86</b>
<b>8.6.1 Introduction</b> .....	<b>86</b>
<b>8.6.2 MMI Objects</b> .....	<b>86</b>
8.6.2.1 close_MMI.....	86
8.6.2.2 Display Control.....	87
8.6.2.3 Display Reply.....	88
<b>8.6.3 MMI Keypad objects</b> .....	<b>88</b>
8.6.3.1 Keypad Control .....	88
8.6.3.2 Keypress .....	89
8.6.3.3 Table of Key Codes.....	89
<b>8.6.4 MMI File Transfer objects</b> .....	<b>89</b>
8.6.4.1 Server Query.....	90
8.6.4.2 Server Reply .....	90
<b>8.7 Communications Resources</b> .....	<b>91</b>
<b>8.7.1 Low-Speed Communication Resource Class</b> .....	<b>91</b>
8.7.1.1 Introduction .....	91
8.7.1.2 Requirements .....	91
8.7.1.3 Objects Supporting the Low-Speed Communications Resource .....	91
8.7.1.4 Comms Cmd .....	92
8.7.1.5 Comms Reply .....	93
8.7.1.6 Comms Send .....	94
8.7.1.7 Comms Rcv .....	94
<b>8.8 Homing Resources</b> .....	<b>94</b>
<b>8.8.1 Host Homing Resource Class</b> .....	<b>94</b>

8.8.1.1 Introduction .....	94
8.8.1.2 Requirements .....	95
8.8.1.3 Objects Supporting the Homing Resource .....	95
8.8.1.4 Homing Resource Coding .....	95
8.8.1.5 Open Homing.....	95
8.8.1.6 Homing_Cancelled.....	96
8.8.1.7 open_homing_Reply .....	96
8.8.1.8 Homing Active .....	97
8.8.1.9 Homing Done.....	97
<b>8.9 Copy Protection Framework.....</b>	<b>97</b>
8.9.1 Copy Protection Resource Class .....	97
8.9.2 Service Provider [Informative].....	97
8.9.2.1 Back Channel [Informative].....	98
8.9.2.2 Service Provider Processing [Informative].....	98
8.9.2.2.1 Checking Validity of Host Information .....	98
8.9.2.2.2 Host Revocation .....	98
8.9.3 CA Module/Host Binding.....	98
8.9.4 Discrete Logarithm DH .....	98
8.9.4.1 Elliptic Curve DH .....	98
8.9.4.2 Needham-Schroeder Key Exchange Protocol .....	99
8.9.4.3 Computation of $K_{cpss}$ and $K_{validated\_cpss}$ .....	99
8.9.5 Copy Control Information Definition.....	99
8.9.6 Scrambling .....	101
8.9.6.1 Key Derivation Sequence .....	101
8.9.6.2 ODD/EVEN Key Generation .....	102
8.9.6.3 Key Application for In-Band Channel .....	103
8.9.6.4 Content (In-Band Channel) Encryption .....	103
8.9.6.5 Data Channel Encryption.....	103
8.9.7 Copy Protection resource coding .....	104
8.9.8 APDU .....	104
8.9.8.1 CP_open.....	104
8.9.8.1.1 CP_open_req() .....	104
8.9.8.1.2 CP_open_cnf() .....	104
8.9.8.2 CP_data.....	105
8.9.8.2.1 CP_data_req() .....	105
8.9.8.2.2 CP_system_id .....	105
8.9.8.2.3 program_number .....	106
8.9.8.2.4 datatype_ID .....	106
8.9.8.2.5 CP_data_cnf() .....	106
8.9.8.3 CP_sync.....	107
8.9.8.3.1 CP_sync_req() .....	107
8.9.8.3.2 CP_sync_cnf().....	107
8.9.8.3.3 status_field.....	107
8.9.9 transport_scrambling_control Field .....	108
<b>8.10 Chaining .....</b>	<b>108</b>
8.10.1 Chaining Resource Class .....	108
8.10.2 Chaining resource coding .....	108
8.10.3 Objects Supporting the Chaining Resource .....	108
8.10.4 chaining_request .....	109
8.10.5 chaining_Status .....	109
8.10.5.1 chaining_status_ID .....	109
8.10.5.2 chaining_address_ID .....	109
8.10.6 chaining_control.....	109
8.10.7 buffer_write .....	110
8.10.8 buffer_write_reply.....	110
8.10.9 buffer_write_status_ID.....	110
8.10.10 buffer_Read_Request.....	110
8.10.11 buffer_read .....	111

8.11 Resource Identifiers and Application Object Tags .....	111
8.11.1 Resource Identifiers .....	111
8.11.1.1 Low-Speed Communications Resource Types .....	111
8.11.2 Application Object Tags.....	113
8.12 Host Control .....	115
8.12.1 OOB_TX_tune_req() & OOB_TX_tune_cnf() .....	115
8.12.2 OOB_RX_tune_req() & OOB_RX_tune_cnf().....	116
8.12.3 Extended Channel Support.....	117
8.12.4 new_flow_req() & new_flow_cnf().....	118
8.12.5 delete_flow_req() & delete_flow_cnf() .....	120
8.12.6 index_flow_req() & index_flow_cnf() .....	120
8.13 Generic IPPV Support .....	121
8.13.1 program_req() & Program_cnf().....	121
purchase_req() & purchase_cnf() .....	124
8.13.2 cancel_req() & Cancel_cnf() .....	126
8.13.3 history_req() & history_cnf() .....	127
<b>Annex A PC Card-Based Physical Layer (Normative).....</b>	<b>129</b>
<b>A.1 General Description.....</b>	<b>129</b>
A.1.1 PC Card interface .....	129
A.1.2 Descrambler.....	129
A.1.3 Filter/Extract .....	130
A.1.4 CPU.....	130
A.1.5 ROM/EPROM and RAM/NVRAM.....	130
A.1.6 Security Processor .....	130
<b>A.2 Electrical Interface .....</b>	<b>130</b>
A.2.1 Transport Stream Interface .....	130
A.2.2 Command Interface.....	130
A.2.2.1 Hardware Interface Description.....	130
A.2.2.1.1 Initialization .....	131
A.2.2.1.2 Host to Module Transfers.....	132
A.2.2.1.3 Module to Host Transfers.....	132
A.2.2.2 Hardware Support in the Module .....	132
<b>A.3 Link Layer .....</b>	<b>133</b>
A.3.1 Transport Stream Interface .....	133
A.3.2 Command Interface.....	133
<b>A.4 Implementation-specific Transport sublayer over PC Card Interface.....</b>	<b>133</b>
A.4.1 Transport Protocol Objects.....	133
A.4.1.1 Command TPDU .....	134
A.4.1.2 Response TPDU.....	134
A.4.1.3 Chaining of Command or Response TPDU Data Fields .....	135
A.4.1.4 Create Transport Connection (create_t_c).....	136
A.4.1.5 Create Transport Connection Reply (c_t_c_reply) .....	136
A.4.1.6 Delete Transport Connection (delete_t_c).....	137
A.4.1.7 Delete Transport Connection Reply (d_t_c_reply) .....	137
A.4.1.8 Request Transport Connection (request_t_c).....	137
A.4.1.9 New Transport Connection (new_t_c) .....	138
A.4.1.10 Transport Connection Error (t_c_error).....	138
A.4.1.11 List of c_tpdus and associated r_tpdus .....	139
A.4.1.11.1 Send Data command .....	139
A.4.1.11.2 Receive Data Command .....	140
A.4.1.12 Rules for the Polling Function.....	140
A.4.1.13 List of Transport Tags.....	140
<b>A.5 PC Card Subset to be Used by Conformant Hosts and Modules .....</b>	<b>141</b>
A.5.1 Objectives .....	141
A.5.2 Introduction .....	141
A.5.3 Terminology.....	141

<b>A.5.4 Physical Specification .....</b>	<b>141</b>
A.5.4.1 Card dimensions .....	141
A.5.4.2 Connector.....	141
A.5.4.3 PC Card Guidance .....	141
A.5.4.4 Grounding/EMI Clips .....	141
A.5.4.5 Connector Reliability.....	141
A.5.4.6 Connector Durability .....	142
A.5.4.7 PC Card Environmental.....	142
<b>A.5.5 Electrical Specification.....</b>	<b>142</b>
A.5.5.1 Card Type Detection.....	142
A.5.5.2 Pin Assignments .....	142
A.5.5.3 16-bit PC Card features .....	143
A.5.5.4 Signal Description .....	143
A.5.5.5 Memory Function.....	146
A.5.5.6 Timing Functions.....	146
A.5.5.7 Electrical interface.....	146
A.5.5.8 Card Detect .....	146
A.5.5.9 Battery Voltage Detect .....	146
A.5.5.10 Power Supply Management .....	146
A.5.5.11 I/O Function.....	147
A.5.5.12 Function Configuration .....	147
A.5.5.13 Card Configuration.....	147
<b>A.5.6 Metaformat Specification .....</b>	<b>147</b>
<b>Annex B MMI Display Requirements (Normative) .....</b>	<b>149</b>
B.1 HTML Requirements .....	149
B.2 Optional HTPV Extensions.....	150
<b>Annex C Additional Objects (Informative).....</b>	<b>152</b>
C.1 Authentication .....	152
C.1.1 Authentication Request and Authentication Response.....	152
C.1.2 Authentication Resource Coding .....	152
C.2 Mating.....	152
C.2.1 Mating Request and Mating Response .....	153
C.2.2 Mating Resource Coding.....	153
C.3 Smart Card Reader Resource Class .....	153
C.3.1 Objects .....	154
C.3.1.1 Smart Card Cmd .....	154
C.3.1.2 Smart Card Reply .....	155
C.3.1.3 Smart Card Send .....	156
C.3.1.4 Smart Card Rcv.....	156
C.3.2 Smart Card Reader Resource Coding.....	157
C.3.2.1 Resource Type Coding.....	157
<b>Annex D Homing Support in Hosts (Informative) .....</b>	<b>158</b>
<b>Annex E Chaining of CA Modules (Informative) .....</b>	<b>159</b>
<b>Annex F ISO-7816 Interface Extensibility (Normative).....</b>	<b>160</b>

## Figures

Figure 1 Example of Single Module in Connection with Host .....	53
Figure 2 Layering on the command interface .....	56
Figure 3 Transport Stream Interface Layers .....	57
Figure 4 Command Interface Layers .....	57
Figure 5 Transport Stream Interface Chaining between Modules .....	60
Figure 6 State Transition Diagram for the Host side of the Transport Protocol .....	64
Figure 7 State Transition Diagram for the Module side of the Transport Protocol.....	65
Figure 8 Object Transfer Sequence Example for the Transport Protocol.....	66
Figure 9 Session to a Host-provided Resource.....	68
Figure 10 Session to a Module-provided Resource .....	69
Figure 11 SPDU Structure .....	70
Figure 12 APDU structure .....	75
Figure 13 Illustration of the Chaining Mechanism.....	76
Figure 14 Baseline CCI Field.....	100
Figure 15 Copy Protection Key Derivation.....	102
Figure 16 Low-Speed Communications Resource Type Structure.....	112
Figure 17 Resource Type Structure for Modems.....	112
Figure 18 Primitive Tag Coding .....	113
Figure 19 RF_TX_frequency_value Coding.....	116
Figure 20 RF_TX_coding_value Coding .....	116
Figure 21 RF_RX_frequency_value Value .....	117
Figure 22 RF_RX_coding_value Value.....	117
Figure 23 Status_register Field .....	126
Figure 24 Typical CA Module Architecture showing the Position of the PC Card Interface.....	129
Figure 25 Map of Hardware Interface Registers .....	130
Figure 26 Status Register.....	131
Figure 27 Command Register .....	131
Figure 28 Layout of Link Protocol Data Unit.....	133
Figure 29 c_tpdu structure.....	134
Figure 30 r_tpdu structure .....	134
Figure 31 SB_value coding .....	135
Figure 32 Illustration of the Chaining Mechanism with c_tpduTPDU.....	135
Figure 33 Illustration of the Chaining Mechanism with r_tpdu .....	136
Figure 34 create_t_c structure.....	136
Figure 35 c_t_c_Reply Structure .....	136
Figure 36 delete_t_c Structure .....	137
Figure 37 d_t_c_reply Structure .....	137
Figure 38 request_t_c Structure .....	137
Figure 39 new_t_c Structure.....	138
Figure 40 t_c_error Structure .....	138
Figure 41 Send Data command/response pair.....	139
Figure 42 Receive Data command/response pair.....	140
Figure 43 Timing Relationships for Transport Stream Interface Signals.....	145
Figure 44 Smart Card Reader Resource Type Structure .....	157

## TABLES

Table 1 Length field used by all Protocol Data Units at Transport, Session & Application Layers .61	
Table 2 Objects Expected to be Received in the States of a Transport Connection on the Host .... 64	
Table 3 Objects Expected to be Received in the States of a Transport Connection on the Module 65	
Table 4 SPDU Coding .....	70

Table 5 Open Session Request Coding .....	71
Table 6 Open Session Response Coding .....	71
Table 7 Open Session Status Values .....	71
Table 8 Create Session Coding .....	72
Table 9 Create Session Response Coding .....	72
Table 10 Close Session Request Coding .....	73
Table 11 Close Session Response Coding .....	73
Table 12 Close Session Status Values .....	73
Table 13 Session Number Coding .....	73
Table 14 Session Tag Values .....	74
Table 15 resource_identifier coding .....	75
Table 16 APDU coding .....	76
Table 17 Profile Inquiry Object Coding .....	77
Table 18 Profile Reply Object Coding .....	78
Table 19 Profile Changed Object Coding .....	78
Table 20 Application Info Inquiry Object Coding .....	78
Table 21 Application Info object coding .....	79
Table 22 Enter Menu Object Coding .....	79
Table 23 CA_info Inquiry Object Coding .....	80
Table 24 CA_info Object Coding .....	80
Table 25 CA_PMT Object Coding .....	81
Table 26 CA_PMT_list_management Values .....	82
Table 27 CA_PMT_cmd_ID Values .....	82
Table 28 CA_PMT Reply Object Coding .....	83
Table 29 CA_enable Values .....	83
Table 30 Tune Object Coding .....	84
Table 31 Replace Object Coding .....	85
Table 32 Clear Replace Object Coding .....	85
Table 33 Ask Release Object Coding .....	85
Table 34 System Time Inquiry Object Coding .....	86
Table 35 System Time Object Coding .....	86
Table 36 Close MMI Object Coding .....	87
Table 37 close_MMI_cmd_ID Values .....	87
Table 38 Display Control Object Coding .....	87
Table 39 MMI_mode Values .....	88
Table 40 Display Reply Object Coding .....	88
Table 41 Keypad Control Object Coding .....	88
Table 42 Keypress Object Coding .....	89
Table 43 Key Code Values .....	89
Table 44 Server Query Object Coding .....	90
Table 45 Server Reply Object Coding .....	90
Table 46 file_status Values .....	90
Table 47 comms_cmd Object Coding .....	92
Table 48 Connection Descriptor Object Coding .....	92
Table 49 comms_reply Object Coding .....	93
Table 50 Comms Send Object Coding .....	94
Table 51 Comms Rcv Object Coding .....	94
Table 52 Objects Used in Homing Resource .....	95
Table 53 Homing Resource Coding .....	95
Table 54 open_homing Object Coding .....	95
Table 55 Comms Reply Object Coding .....	96
Table 56 homing_cancelled_id Values .....	96
Table 57 open_homing_reply Object Coding .....	96
Table 58 system_time Value in system_time() .....	96
Table 59 homing_active Object Coding .....	97
Table 60 homing_done Object Coding .....	97

Table 61 CCI Types and Sizes .....	100
Table 62 Baseline CCI.....	100
Table 63 CGMS Values .....	100
Table 64 Analog Protection System.....	100
Table 65 Key Derivation Sequence Parameter/Key Sizes.....	101
Table 66 Data Channel Message Encryption Parameter Sizes.....	103
Table 67 Copy Protection resource coding.....	104
Table 68 Objects Used in Copy Protection Resource .....	104
Table 69 CP_open_req() Object Coding .....	104
Table 70 CP_open_cnf() Object Coding.....	105
Table 71 CP_system_id_bitmask Values.....	105
Table 72 CP_data_req() Object Coding.....	105
Table 73 CP_system_id .....	106
Table 74 program_number .....	106
Table 75 datatype_ID values .....	106
Table 76 CP_data_cnf() Object Coding.....	107
Table 77 CP_sync_req () Coding.....	107
Table 78 CP_sync_cnf () Syntax.....	107
Table 79 status_field Value .....	108
Table 80 CP_transport_scrambling_control_field Descriptor Values .....	108
Table 81 Chaining Resource Coding .....	108
Table 82 Objects Used in Chaining Rresource .....	109
Table 83 chaining_request Descriptor Object Coding .....	109
Table 84 chaining_status Descriptor Object Coding .....	109
Table 85 chaining_status_id Values .....	109
Table 86 chaining_control Descriptor Object Coding.....	110
Table 87 buffer_write Descriptor Object Coding .....	110
Table 88 buffer_write_reply Descriptor Object Coding.....	110
Table 89 buffer_write_status_ID Values .....	110
Table 90 buffer_read_request Descriptor Object Coding .....	111
Table 91 buffer_read Descriptor Object Coding .....	111
Table 92 Resource Identifier Values .....	111
Table 93 Device Field Values .....	112
Table 94 dataproc Field Values .....	112
Table 95 Modem Type Field Values.....	113
Table 96 Application Object Tag Values.....	114
Table 97 Host Control Resource .....	115
Table 98 Host Control Objects.....	115
Table 99 OOB_TX_tune_req() and OOB_TX_tune_cnf() .....	115
Table 100 OOB_TX_tune_cnf() & OOB_TX_tune_cnf_tag .....	116
Table 101 status_field Values .....	116
Table 102 OOB_RX_tune_req() & OOB_RX_tune_req_tag Coding.....	116
Table 103 OOB_RS_tune_cnf() & OOB_TX_tune_cnf_tag Coding .....	117
Table 104 status_field Values .....	117
Table 105 extended_channel Identifier .....	118
Table 106 extended_channel Objects .....	118
Table 107 new_flow_req() & new_flow_cnf() Coding .....	118
Table 108 service_type Value .....	118
Table 109 new_flow_cnf() & new_flow_cnf_tag Coding .....	119
Table 110 status_field Values .....	119
Table 111 delete_flow_req() & delete_flow_req_tag Coding .....	120
Table 112 delete_flow_cnf() & delete_flow_cnf_tag Coding.....	120
Table 113 status_field Values .....	120
Table 114 index_flow_req() & index_flow_req_tag Coding .....	120
Table 115 index_flow_cnf() & index_flow_cnf_tag Coding.....	121
Table 116 status_field Values .....	121



Table 117 Generic IPPV Support Identifier .....	121
Table 118 Generic IPPV Support Objects .....	121
Table 119 status_field Values .....	123
Table 120 purchase_type Value.....	123
Table 121 c_tpdu coding .....	134
Table 122 r_tpdu coding.....	134
Table 123 Coding of bit8 of SB_value.....	135
Table 124 create_t_c coding .....	136
Table 125 c_t_c_Reply Coding .....	136
Table 126 delete_t_c coding .....	137
Table 127 d_t_c_reply coding.....	137
Table 128 request_t_c coding.....	138
Table 129 new_t_c coding.....	138
Table 130 t_c_error coding .....	138
Table 131 Error Code Values .....	139
Table 132 Coding of Send Data c_tpdu .....	139
Table 133 Coding of Send Data r_tpdu .....	139
Table 134 Coding of Receive Data C_TPDU .....	140
Table 135 Coding of Receive Data r_tpdu .....	140
Table 136 Transport Tag Values .....	141
Table 137 Pin assignments for this PC CARD variant .....	143
Table 138 Timing Relationship Limits.....	146
Table 139 NRSS Subset of HTML 3.2 .....	149
Table 140 HTVP Functions .....	151

(This page intentionally left blank.)

## NATIONAL RENEWABLE SECURITY STANDARD (NRSS) PART A

### 1 Introduction

CEA-679-C Part A describes the physical and electrical parameters of the interface for conditional access (CA) devices for consumer electronics (CE). The purpose of this standard is to specify the interface to a CA device that performs the signal access and, optionally, descrambling and key generation. It is possible to imagine that several CA devices could be interfaced to the same CE device, simultaneously (see Annex A (informative)). This interface definition allows the entire CA system to be removable and hence replaceable. Very few constraints, if any, are placed on the CA system architecture.

### 2 Scope and Field of Application

CEA-679-C describes the interface from a physical, electrical, and functional view and the physical form factor for the CA device. There may be other specifications that apply generally to consumer household electronic devices, for example, environmental protection and radiation requirements. CEA-679-C is not inclusive of all specifications that may apply to the CA device.

### 3 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 edition indicated was valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of the standard indicated.

#### 3.1 Normative Reference List

CEA-796-A, NRSS Copy Protection Systems, October 2005

ISO 7810 - Identification cards. Physical characteristics (Second Edition, 1995)

ISO 7816 - Identification cards. Integrated circuit(s) cards with contacts, Part 1: Physical characteristics (First Edition, 1987).

ISO 7816 - Identification cards. Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts (Revision of first edition, 1988).

ISO 7816 - Identification cards. Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols (First edition, 1989 with Amendment 1, 1992)

ISO/IEC 13818-1(Draft International Standard, 1994) Information Technology - Generic Coding of Moving Pictures and Associated Audio

ATSC A/65—Program and System Information Protocol for Terrestrial Broadcast and Cable, 12/23/97

NIST FIPS PUB 46-3, Data Encryption Standard, October 25, 1999 (withdrawn May 19, 2005)

NIST FIPS PUB 81, DES Modes of Operation, December 2, 1980 (withdrawn May 19, 2005)

#### 3.2 Normative Reference Acquisition

ATSC Standards:

- Advanced Television Systems Committee (ATSC), 1750 K Street, N.W., Suite 800, Washington, DC 20006, Phone 202-828-3130; Fax 202-828-3131; Internet <http://www.atsc.org>

CEA Standards:

- Global Engineering Documents, World Headquarters, 15 Inverness Way East, Englewood, CO USA 80112-5776; Phone 800-854-7179; Fax 303-397-2740; Internet <http://global.ihs.com>; Email [global@ihs.com](mailto:global@ihs.com)