CTA Standard

National Renewable Security Standard (NRSS)

CTA-679-C R-2013

(Formerly CEA-679-C R-2013)

October 2005

ANSI Accredited Standards Developer

Consumer Technology Association™

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.

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.

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

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

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

FIGURES

TABLES

PART B CONTENTS

Figures

TABLES

(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