CTA Standard

NRSS Copy Protection Systems

CTA-796-A R-2012

(Formerly CEA-796-A R-2012)

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

CONTENTS

(This page intentionally left blank.)

FOREWORD

This standard was developed under the auspices of the Consumer Electronics Association (CEA) Technology & Standards R8 Cable Compatibility Committee.

> NOTE—In 2003, CEA redesignated EIA/CEA standards and bulletins, and those EIA standards under CEA auspices, as CEA standards or bulletins, respectively. Please see http://techstreet.com for the most recent designation.

(This page intentionally left blank.)

NRSS Copy Protection Systems

1 Copy Protection for the NRSS Interface

The copy protection systems included here are itemized for the purpose of identification. The systems outlined in CEA-796-A all support the copy protection frameworks described in CEA-679-C, Parts A and B.

2 Normative References

The following standards contain provisions that, through reference in this text, constitute normative provisions of this standard. At the time of publication, the editions indicated were 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 editions of the standards listed in Section 2.1.

2.1 Normative Reference List

CEA-679-C, National Renewable Security Standard (NRSS), October, 2005

2.2 Normative Reference Acquisition

CEA Standards:

- Techstreet, 3916 Ranchero Drive, Ann Arbor, MI USA 48108; Phone 800-699-9277; Fax 734-780-2046; Internet http://www.techstreet.com; Email techstreet.service@thomsonreuters.com

3 Systems for Communicating Copy Protection Methods Implemented between Host and the CA Device

The value of CP_system_ID (as used in CEA-679-C, Parts A and B) shall be the system number defined in Section 4.

3.1 NRSS Part A System Protocols

Information concerning commands necessary to use CEA-796-A systems in conjunction with NRSS Part A devices may be found CEA-679-C, Part A, Section 20.

3.2 NRSS Part B System Protocols

Information concerning commands necessary to use CEA-796-A systems in conjunction with NRSS Part B devices may be found in CEA-679-C, Part B, Section 8.9.

4 Copy Protection Systems

When any of the copy protection systems described in Section 4 is implemented, it shall be implemented as indicated in this section.

4.1 System 1—Data Scrambling with Diffie-Hellman Based Keys

System 1 is designed to protect data returning from an NRSS module for display to the consumer. Protection is based on three primary principles:

a) Restricting the devices that may receive copy protected data. Intellectual property embedded within this copy protection method will require a license for manufacture, sale, or use. Licensing terms are designed to prevent devices that facilitate copying unscrambled bitstreams. Devices capable of recording an unscrambled bitstream, capable of making an unscrambled bitstream available for recording, or capable of being readily modified to record/provide bitstreams will not be granted a license.
b) Scrambling data and protecting the keys so that passive devices cannot record signals and decode a clear bitstream. Content data is protected with DES and keys are negotiated using Diffie-Hellman (DH) key exchange. While it is possible to passively eavesdrop and decode data from the information, it is prohibitively difficult for the value of the data being sent, which is already-purchased A/V content.
c) Closely coupling the host and CA module devices so that active devices to record bitstreams are difficult to create. Real-time constraints and complexities make active (‘man-in-the-middle’) devices complex to design and manufacture.

4.1.1 Licensing
Licensing shall be required.[1]

4.2 System 2--Cryptographic Copy Protection I

4.2.1 Introduction
This section describes a mechanism for protecting the interface between the user renewable conditional access module (POD) and the STB. The mechanism is simple yet secure, and lays the foundation for incorporating evolutionary improvements in the security of STBs, PODs, and key management infrastructures. The mechanism incorporates the following design principles: Localization of vulnerability, so security is a property of the integrity of the two communicating device (i.e., no universal secrets that enable the pirate to leverage off of the compromise of a third device); cryptographic protection of data; IP protected functionality that enables the legal prosecution of circumvention devices; and the fresh authorization of devices by means of the bi-directional communication inherent in cable systems.

4.2.2 Licensing
Licensing shall be required.[2]

4.3 System 3--Cryptographic Copy Protection II

Basics

a) Each CE manufacturer generates its own secret-public key pair and has the public key certified by the licensing authority (LA). The CE public-key is stored in the “Manufacturer Certificate” in the device. The CE secret-key is used by the CE manufacturer to certify its own individual devices' public keys. It is proposed that the certificates be signed and checked using the Fiat Shamir Signature algorithm (FSS).
b) For each CE device, a DH secret-public key pair (x,g^x mod p) is generated (perhaps by the device itself). The device DH public key (g^x mod p) is certified by the CE device manufacturer. The device DH public key is stored in the “Device-Certificate”
c) When two CE devices--the host and the CA module--are connected, they exchange certificates that will enable them to perform an authenticated key exchange and establish a secure channel between them.
d) After the certificates are verified, the devices have each other’s certified DH public key. Using that key, each device continues with the standard DH protocol (compute g^(x1*x2) mod p, from the received public key and its own secret). This generates a shared key for these two devices.
e) To generate a session key, the devices exchange some numbers which are hashed with the shared key above. The session key can be updated as desired by the same hash mechanism--exchange of numbers and the hash.
f) The session key is used to establish a control content channel on which control words and other items can be passed between the Host and CA module.

4.3.1 Licensing
Licensing shall be required.[3]

4.4 System 4—Cryptographic Copy Protection III

4.4.1 Intellectual Property
Implementation of the technology described in this section requires a license from the licensing authority and possibly other licenses.

---

[1] For System 1 licensing information, contact: Manager, Licensing-Paris, Thomson multimedia, 46 quai Alphonse Le Gallo, 92648 Boulogne Cedex, France, phone 330 1 41 86 5288, fax 330 1 41 86 0925, Email mesj@thmulti.com.
[2] For System 2 licensing information, contact: CableLabs, 858 Coal Creek Circle , Louisville, CO 80027-9750, phone 303 661 9100.
[3] For System 3 licensing information, contact: CTO, NDS-TI, Box 23012, Jerusalem, Israel, phone 972-2-5894444, Fax 972-2-589-4000, Email ytsuria@ndsisrael.com or marketing@ndsuk.com.