ANSI/CTA Standard

Receiver Specifications for ATSC 2.0 Security

ANSI/CTA-2053

(Formerly ANSI/CEA-2053)

August 2015

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.

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

This standard was developed by the Consumer Electronics Association's R4.8, DTV Interface Subcommittee.

(This page intentionally left blank.)

CONTENTS

1 Scope 1

2 Revision History 1

3 References 1
- **3.1 Normative References** 1
  - **3.1.1 Normative Reference List** 1
  - **3.1.2 Normative Reference Acquisition** 1
- **3.2 Informative References** 1
  - **3.2.1 Informative Reference List** 1
  - **3.2.2 Informative Reference Acquisition** 2
- **3.3 Compliance Notation** 2
- **3.4 Definitions** 2
- **3.5 Symbols and Abbreviations** 2

4 Overview 2

5 Receiver Platform Requirements 2
- **5.1 Time** 2
- **5.2 Network Services** 2
- **5.3 Transport Layer Security for the Interaction Channel** 3
- **5.4 DO Application Code Verification** 3

6 Trusted Certificate Storage 4
- **6.1 Trusted Root Storage** 4
- **6.2 Trusted Root Updates** 4
- **6.3 Runtime Storage of Certificates** 4
- **6.4 Certificate Profiles** 4

7 Certificate Revocation and Status Information (TLS) 4
- **7.1 Verification of TLS Server Certificates** 4

(This page intentionally left blank.)

Receiver Specifications for ATSC 2.0 Security

1 Scope

This document is a Standard for receiver certificate handling and processing to meet the security needs for ATSC 2.0.

2 Revision History

This is the initial version of this standard.

3 References

3.1 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 here.

3.1.1 Normative Reference List

1. RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008
2. RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013
3. HbbTV Root Certificate List, https://www.hbbtv.org/spec/certificates.html
4. Widgets-DigSig, XML Digital Signatures for Widgets, http://www.w3.org/TR/widgets-digsig

3.1.2 Normative Reference Acquisition

1. The Internet Engineering Task Force (ITEF), 48377 Fremont Blvd., Suite 117, Fremont, California 94538
2. HbbTV, www.HbbTV.org.

3.2 Informative References

The following references contain provisions that, through reference in this text, constitute informative 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 below.

3.2.1 Informative Reference List

1. None