ATSC Standard:
ATSC Security and Service Protection Standard

Doc. A/106
28 September 2015

Advanced Television Systems Committee
1776 K Street, N.W.
Washington, D.C. 20006
202-872-9160

The Advanced Television Systems Committee, Inc., is an international, non-profit organization developing voluntary standards for digital television. The ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

Specifically, ATSC is working to coordinate television standards among different communications media focusing on digital television, interactive systems, and broadband multimedia communications. ATSC is also developing digital television implementation strategies and presenting educational seminars on the ATSC standards.

ATSC was formed in 1982 by the member organizations of the Joint Committee on InterSociety Coordination (JCIC): the Electronic Industries Association (EIA), the Institute of Electrical and Electronic Engineers (IEEE), the National Association of Broadcasters (NAB), the National Cable Telecommunications Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). Currently, there are approximately 120 members representing the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

ATSC Digital TV Standards include digital high definition television (HDTV), standard definition television (SDTV), data broadcasting, multichannel surround-sound audio, and satellite direct-to-home broadcasting.

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. One or more patent holders have, however, filed a statement regarding the terms on which such patent holder(s) may be willing to grant a license under these rights to individuals or entities desiring to obtain such a license. Details may be obtained from the ATSC Secretary and the patent holder.

Revision History

Version	Date
Candidate Standard approved	1 January 2014
Standard approved	29 September 2015

Table of Contents

ATSC Standard:
ATSC Security and Service Protection Standard

1. SCOPE

This standard specifies the mechanisms for security and service protection in ATSC 2.0 systems.

1.1 Introduction and Background

This document defines the security and service protection systems for ATSC 2.0 Broadcasting. Prepared by the Specialist Group on Security (TG1/S7), the necessary building blocks are called out that will enable broadcasters to fully exploit the capabilities of digital broadcasting using ATSC 2.0. This standard is based, whenever possible, on existing open standards.

1.2 Organization

This document is organized as follows:

- Section 1 – Outlines the scope of this document and provides a general introduction.
- Section 2 – Lists references and applicable documents.
- Section 3 – Provides a definition of terms, acronyms, and abbreviations for this document.
- Section 4 – System overview (informative)
- Section 5 – System specifications (normative)

2. REFERENCES

All referenced documents are subject to revision. Users of this Standard are cautioned that newer editions might or might not be compatible.

2.1 Normative References

The following documents, in whole or in part, as referenced in this document, contain specific provisions that are to be followed strictly in order to implement a provision of this Standard.

[1] RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2," August 2008, Internet Engineering Task Force, Freemont, CA.

[2] RFC 2818, "HTTP over TLS," May 2000.

[3] RFC 6066, "Transport Layer Security (TLS) Extensions, Extension Definitions," January 2011.

[4] RFC 2560, "Online Certificate Status Protocol (OCSP)," June 1999.

[5] RFC 5019, "Lightweight Online Certificate Status Protocol Profile for High Volume Environments," September 2007.

[6] RFC 5280, "Internet X.509 Public Key Infrastructure Profile," May 2008.

[7] RFC 3279, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Profile," April 2002.

[8] RFC 4055, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Profile," June 2005.

[9] W3C: "XML Digital Signature for Widgets," March 2012, World Wide Web Consortium.

[10] ATSC: "ATSC Digital Television Standard, Part 1 – Digital Television System," Doc. A/53 Part 1:2013, Advanced Television Systems Committee, Washington, D.C., 7 August 2013.

[11] ATSC: "Program and System Information Protocol for Terrestrial Broadcast and Cable," Doc. A/65:2013 Advanced Television Systems Committee, Washington, D.C., 7 August 2013.
[12] ATSC: "Conditional Access System for Terrestrial Broadcast," Doc. A/70 Part 1:2010, Advanced Television Systems Committee, Washington, D.C. 30 November 2010.
[13] MPEG: "DASH – Dynamic Adaptive Streaming over HTTP," Doc. ISO/IEC 23009, Moving Picture Experts Group.
[14] IEEE: "Use of the International Systems of Units (SI): The Modern Metric System", Doc. IEEE/ASTM SI 10-2002, Institute of Electrical and Electronics Engineers, New York, N.Y., 2002.

2.2 Informative References

The following documents contain information that may be helpful in applying this Standard.

[15]] CEA: "Broadcast Security Receiver Platform Requirements," Doc. CEA 2053, Consumer Electronics Association, Arlington, VA. (forthcoming)
[16] RFC 6176, "Prohibiting Secure Sockets Layer (SSL) Version 2.0."

3. DEFINITION OF TERMS

With respect to definition of terms, abbreviations, and units, the practice of the Institute of Electrical and Electronics Engineers (IEEE) as outlined in the Institute's published standards [14] shall be used. Where an abbreviation is not covered by IEEE practice or industry practice differs from IEEE practice, the abbreviation in question will be described in Section 3.3 of this document.

3.1 Compliance Notation

This section defines compliance terms for use by this document:

shall – This word indicates specific provisions that are to be followed strictly (no deviation is permitted).

shall not – This phrase indicates specific provisions that are absolutely prohibited.

should – This word indicates that a certain course of action is preferred but not necessarily required.

should not – This phrase means a certain possibility or course of action is undesirable but not prohibited.

3.2 Treatment of Syntactic Elements

This document contains symbolic references to syntactic elements used in the audio, video, and transport coding subsystems. These references are typographically distinguished by the use of a different font (e.g., restricted), may contain the underscore character (e.g., sequence_end_code) and may consist of character strings that are not English words (e.g., dynrng).

3.2.1 Reserved Elements

One or more reserved bits, symbols, fields, or ranges of values (i.e., elements) may be present in this document. These are used primarily to enable adding new values to a syntactical structure without altering its syntax or causing a problem with backwards compatibility, but they also can be used for other reasons.

The ATSC default value for reserved bits is '1.' There is no default value for other reserved elements. Use of reserved elements except as defined in ATSC Standards or by an industry

standards setting body is not permitted. See individual element semantics for mandatory settings and any additional use constraints. As currently-reserved elements may be assigned values and meanings in future versions of this Standard, receiving devices built to this version are expected to ignore all values appearing in currently-reserved elements to avoid possible future failure to function as intended.

3.3 Acronyms and Abbreviation

The following acronyms and abbreviations are used within this document.

App – Application

ATSC – Advanced Television Systems Committee

DO – Declarative Object

DTCP – Digital Transmission Content Protection

IP – Internet Protocol

OCSP – Online Certificate Status Protocol (see RFC 2560[4])

SHA1 – Secure Hash Algorithm

SSL – Secure Sockets Layer (see TLS)

TLS – Transport Layer Security (formerly known as Secure Sockets Layer)

3.4 Terms

The following terms are used within this document.

ATSC 2.0 – Collective term for a set of backward compatible features added on top of "ATSC 1.0" (e.g., A/53 [10], A/65 [11]). Although ATSC 2.0 services are not expected to run on ATSC 1.0 receivers, the inclusion of ATSC 2.0 services in a transmission are designed to be compatible with ATSC 1.0 receivers' ability to receive current ATSC services in that transmission.

reserved – Set aside for future use by a Standard.

Second Screen Device (Companion Device) – ATSC 2.0 provides support for the integration of second-screen devices complementing television services. In this context, the television receiver is the first screen device, and the second screen device is a personal device that is used by a viewer while watching a first-screen device. Additionally, multiple second screen devices can be linked to a TV receiver at the same time.

Secure Connection –A private, reliable communications path as described in RFC 5246 [1].

Interaction Channel – A two-way IP communication path that enables communications between an ATSC 2.0 host receiver and a remote server.

RSA – A method for obtaining digital signatures and public-key cryptosystems (originally proposed by Rivest, Shamir, and Adelman).

4. SYSTEM OVERVIEW

This document describes several security primitives which may be used in ATSC systems to establish a certain level of security in the usage of ATSC content and applications.

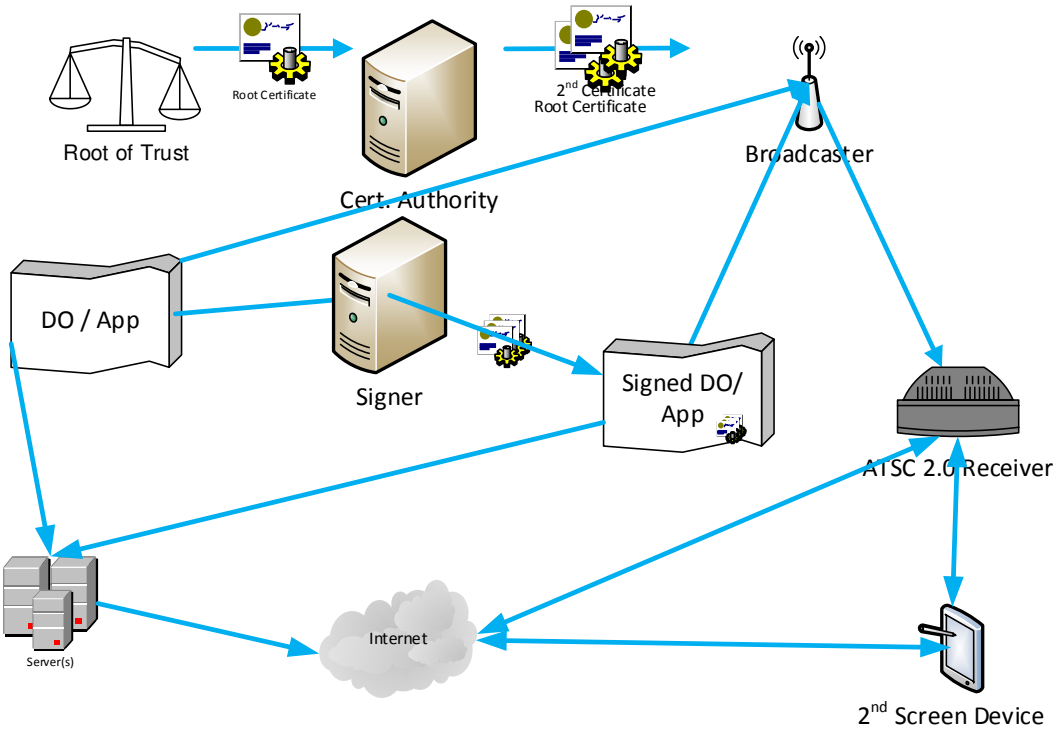

Figure 4.1 System overview.

This standard specifies means to establish security across several interfaces (as shown in Figure 4.1), including:

- Signing mechanisms for downloadable executable code
- Secure IP communications across the interaction channel for both signaling and content (using separate tools)
- Conditionally-accessed content security across the broadcast channel
- Securing communications between an ATSC receiver and a 2nd screen device (such as a tablet)

5. SYSTEM SPECIFICATIONS

5.1 Transport Layer Security for the Interaction Channel

ATSC 2.0 servers, when negotiating a Secure Connection and using ATSC 2.0 Interaction Channel protocols shall comply with TLS 1.2 (RFC 5246 [1]), with the following constraint: ATSC 2.0 servers shall not send any "Server Hello" message specifying a ProtocolVersion (see RFC 5246 [1]) less than { 0x03, 0x03 } (indicating TLS 1.2). The server shall refuse Secure Connections with clients that do not support a ProtocolVersion equal to or greater than { 0x03, 0x03 }. Therefore, ATSC 2.0 clients are expected to implement RFC 5246 [1] for Secure Connections over the Interaction Channel. ATSC 2.0 servers shall only negotiate such Secure Connections using one or more of the following Cipher Suites as specified in RFC 5246 [1] Appendix A.5:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

When an ATSC 2.0 client requests an HTTP connection over TLS, both the ATSC 2.0 client and the ATSC 2.0 server shall comply with RFC 2818 [2] for HTTP over TLS. In particular the ATSC 2.0 client shall perform the Server Identity check as described in RFC 2818 [2] Section 3.1 without relying on any external knowledge as to the identity of the server.

When the ATSC 2.0 client requests a TLS connection, it shall provide a list of the trusted root certificates that it holds in its secure store. Such list of trusted root certificates shall be either the full list of certificates described at http://www.hbbtv.org/spec/certificates.html, or some subset thereof. The list shall be formatted as specified in RFC 6066 [3] Section 6 Trusted CA Indication and shall be encoded as a SHA1 hash of the trusted root public key. The ATSC 2.0 client shall also include the Certificate Status Request extension as specified in RFC 6066 [3] Section 8. The Certificate Status Request extension shall include a list of OCSP Responder Identifiers encoded as a SHA1 hash of the trusted OCSP responder public key as defined in RFC 2560 [4]. The ATSC 2.0 client shall verify the Certificate Status message provided by the server as specified in RFC 6066 [3] Section 8.

5.2 ATSC 2.0 Device to 2nd Screen Device Communications Link Security

ATSC 2.0 devices, when negotiating a Secure Connection for signaling with a 2nd screen shall comply with TLS 1.2 (RFC 5246 [1]).

Note that since 2nd screen devices vary in implementation choice, there is no additional constraint on SSL/TLS versions established. Note that the physical transport mechanism (e.g., Wi-Fi) might have security or encryption as well.

Communicating content between ATSC 2.0 devices and 2nd screen devices can have various degrees of security, including SSL/TLS and/or other industry standard security mechanisms oriented to protecting content (e.g., DTCP-IP). Some content redistribution requires security mechanisms that are neither established nor prohibited by this standard.

This standard is silent upon the particular content protection system, if any, used to protect any particular piece of content and does not preclude or constrain such systems.

5.3 DO Application Code Signing

Executable or interpretable code may be cryptographically signed. If signatures are used, they shall be signed as follows.

Signed applications shall be signed as specified in Widgets-DigSig [9] with the addition of a SigningTime Signature Property for each signature as defined below. RSA keys used for signing shall be 2048 bits in length. The SHA-256 digest method shall be used.

> Note: The digital signatures specification allows for zero or one author signatures, and zero, one or more distributor signatures.

The SigningTime signature property shall contain the time at which the signature is generated and shall be formatted as a dateTime XML DataType. The schema definition for the SigningTime signature property is:

<element name=”SigningTime” type=”xsd:dateTime”/>

5.4 Certificates and Certificate Management

This standard uses the Internet X.509 Public Key Infrastructure Profile (RFC 5280 [6]) as the base profile for certificates used in TLS server and DO application signing authority authentication. The following types of certificate are used by ATSC 2.0 devices during the authentication process:

- One or more root certificates. These are trusted self-signed certificates issued by a trusted certificate authority as the root of trust. Each certificate path validation process completes when a trusted root certificate is reached.
- Certificate authority certificates. These certificates are issued by a trusted root certificate authority or a certificate authority whose certificate path can be validated to a trusted root certificate authority.
- TLS server certificates. These certificates are issued by a trusted certificate authority and are designated for use in server authentication.
- DO application signer certificates. These certificates are issued by a trusted certificate authority and are designated for use in code signing.
- OCSP responder certificates. These certificates are issued by a trusted certificate authority and are designated for use in OCSP responder authentication.

5.4.1 Certificate Profiles

The profile specified in RFC 5280 [6] is further constrained for certificates used in ATSC 2.0.

5.4.1.1 General

All ATSC 2.0 certificates shall be X.509 version 3 certificates.

All keys contained in ATSC 2.0 certificates shall be RSA keys encoded as specified in RFC 3279 [7] . All signatures contained in ATSC 2.0 certificates shall be encoded according to the RSA signature algorithms specified in RFC 3279 [7] and RFC 4055 [8].

All ATSC 2.0 certificates shall contain a Key Usage extension with values constrained as specified in RFC 3279 [7] and RFC 4055 [8].

ATSC 2.0 devices need not process the Authority Information Access or the Subject Information Access extensions.

5.4.1.2 Root Certificate Profile

The RSA key size for this certificate shall be at least 2048 bits and should be 4096 bits.

5.4.1.3 Certificate Authority Certificate Profile

The RSA key size for this certificate shall be at least 2048 bits.

5.4.1.4 Server Authentication Certificate Profile

The RSA key size for this certificate shall be at least 1024 bits.

The Subject Alternative Name extension shall be present and shall include either the DNS Name or the IP Address of the server being authenticated.

The Extended Key Usage extension shall be present and shall be set to the value id-kp-serverAuth to indicate that the certificate is used in TLS server authentication.

5.4.1.5 DO Application Signer Certificate Profile

The RSA key size for this certificate shall be at least 2048 bits.

The Key Usage extension shall be marked as critical and shall include only the digitalSignature value.

The Extended Key Usage extension shall be present, marked as critical, and shall be set to the value id-kp-codeSigning to indicate that the certificate is used in the signing of downloadable executable code.

5.4.1.6 OCSP Responder Certificate Profile

The RSA key size for this certificate shall be at least 1024 bits.

The Extended Key Usage extension shall be present and shall be set to the value id-kp-OCSPSigning to indicate that the certificate is used to sign OCSP responses.

5.4.2 ATSC 2.0 Client Certificate Storage

See [15], which describes secure storage of certificates, and the mechanism(s) for modifying certificates used by client devices.

Clients provide secure storage for the following set of certificates:

- The set of trusted root certificates The set of trusted signing certificate authority certificates
- The set of trusted OCSP responder certificates

Certificates are changed over time, either by download or by other means

5.4.3 Certificate Revocation and Status Information

The management of certificate status is under the control of the issuing authority who works according to their defined certification practices and policies. Each certificate authority that issues certificates used by an ATSC 2.0 server or ATSC 2.0 DO application signing authority is responsible for the timely supply of certificate status information to the OCSP responder(s). The specific methods by which this information is made available to the OCSP responder are beyond the scope of this standard.

5.4.3.1 Certificate Revocation and Status Information for TLS Server Certificates

An ATSC 2.0 server shall request certificate status information from an OCSP responder at least once per minute for each server authentication certificate that it provides as server identification when establishing a TLS connection. The request shall be in the format specified in RFC 5019 [5] and shall be unsigned and shall not use any optional extensions. The ATSC 2.0 server shall forward the most recent OCSP response for the certificate it uses to establish a connection to the ATSC 2.0 client (see Section 5.1). The format of the OCSP Response provided by the responder should be limited to the mandatory elements defined in RFC 5019 [5] and no optional elements should be included in the response.

A client uses the OCSP Response data that it receives to verify that the certificates that authenticate server connections are valid at the time the connection is established. See [15].

5.4.3.2 Certificate Revocation and Status Information for DO Application Signing Certificates

An ATSC 2.0 DO application signing authority shall request certificate status information from an OCSP responder for the signing authority certificate that validates the signing key each time that key is used in a signing operation. The SignalingTime associated with the DO application signature and the ProducedAt time of the corresponding OCSP Response providing the status of the signing authority certificate shall differ by no more than one minute. The ATSC 2.0 DO application signing authority shall include the OCSP Response in the signed application and should not issue a signed application where the OCSP Response indicates that the status of the signing authority certificate (as specified in RFC 2560 [4]) is other than “good”.

The application signing authority shall include an OCSPResponse child element within each X509Data element of the digital signature structure (see http://www.w3.org/TR/xmldsig-core1)

that contains its signing authority certificate. The OCSPResponse child element shall be included as an "Element from an external namespace" (see http://www.w3.org/TR/xmldsig-core1) and shall be formatted as base64 encoding of the OCSP Response received from the ATSC approved OCSP responder.

A client uses the OCSP Response data that it receives to verify that the certificates that authenticate the application signing authority are valid at the time the application is signed. See [15].

5.5 File Security

Provisions relating to DRM protection are encompassed within the ecosystem of the particular content protection system.

5.6 Over the Air Broadcast Service Protection (Conditional Access)

Service protection (conditional access) of over-the-air linear TV services shall be per ATSC A/70 Part 1 [12].

5.7 Other Aspects

Some elements of the ATSC 2.0 system are carried in the clear, without encryption or verification mechanisms, for example, data carousels and non-TLS-protected interaction channel communication. Implementers of the ATSC 2.0 system should take appropriate measures.

End of Document