ATSC Standard: A/360:2019 Amendment No. 2, “Signing Modifications

Doc. A/360:2019 Amend. No. 2
16 February 2021

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 and recommended practices for digital television. ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries. ATSC also develops digital television implementation strategies and supports educational activities on ATSC standards. ATSC was formed in 1983 by the member organizations of the Joint Committee on Inter-society 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). For more information visit www.atsc.org.

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.

Implementers with feedback, comments, or potential bug reports relating to this document may contact ATSC at https://www.atsc.org/feedback/.

Revision History

Version	Date
Amendment approved	16 February 2021

ATSC Standard: A/360:2019 Amendment No. 2, Signing Modifications

1. OVERVIEW

1.1 Definition

An Amendment is generated to document an enhancement, an addition or a deletion of functionality to previously agreed technical provisions in an existing ATSC document. Amendments shall be published as attachments to the original ATSC document. Distribution by ATSC of existing documents shall include any approved Amendments.

1.2 Scope

This document adds a requirement to include all Intermediate Certificate Authority Certificates in the encoding of Broadcaster Applications.

This document also clarifies the data in the CDT across which the signature is generated (ToBeSignedData), and which certificates @OCSPRefresh applies to.

This document also adds a requirement that the CDT shall be signed by a certificate which is not the NextCert (in addition to the current requirement that it be signed by a certificate which is not the CurrentCert).

This document also modifies the OCSP Response time interval described in Sec. 5.5.2, and the treatment of @OCSPRefresh in Sec. 5.2.2.2.

This document also updates two ATSC document references.

1.3 Rationale for Changes

The current A/360 text requires this for the LLS signaling (see Table 5.1) but not the Broadcaster Application. When all intermediate certificates are not present, this creates unnecessary validation overhead for the Receiver.

The "ToBeSignedData" definition is currently silent about whether the beginning/ending tags are included in the signature calculation. The @OCSPRefresh-related text could be read in a misleading way.

The requirement that the CDT not be signed by the NextCert eliminates an attack where the CDT can be signed by NextCert, and the validity period of NextCert is "a moment from now", which would allow the CDT and signaling to be signed by one certificate. There need to be at least two certificates (one to sign the CDT, one to sign the rest of the signaling).

The time interval for OCSP Response in Sec. 5.5.2 is adjusted in order to make allowance for a broader set of OCSP Responders, and the treatment of @OCSPRefresh in Section 5.2.2.2 has an exception added to accommodate testing and validation.

ATSC document references are updated to match the latest versions.

1.4 Compatibility Considerations

With respect to intermediate certificates, the changes described in this amendment are not backwards compatible with encoders, however encoder equipment is now operational to do this, and thus it is believed to not create a practical compatibility issue. It is backwards compatible with Receivers since the certificate inclusion is backward-compatible relative to the currently published

version of the standard to which this Amendment pertains and any previously approved Amendments for that standard.

With respect to OCSP validity time intervals, the changes described are backwards compatible with existing emission equipment, as the allowable time interval increases. For receivers, the changes described are not backwards compatible for receivers which are validating the SigningTime/producedAt difference. The changes are backwards compatible for receivers which do not validate this time difference.

With respect to the treatment of @OCSPRefresh, the changes are backwards compatible for production usage, as the normative specification are unchanged for non-test usage.

With respect to the document references, the changes are backwards compatible.

2. CHANGE INSTRUCTIONS

Change instructions are given below in *italics*. Unless otherwise noted, inserted text, tables, and drawings are shown in blue; deletions of existing text are shown in ~~red strikeout~~. The text "[ref]" indicates that a cross reference to a cited referenced document should be inserted.

2.1 Update Two References

Revise references as shown:

[26] ATSC: "ATSC Standard: ~~Revision of A/331:2017~~ Signaling, Delivery, Synchronization, and Error Protection," Doc. A/331:20~~19~~21, Advanced Television System Committee, Washington, D.C., ~~20 June 2019~~19 January 2021.

[29] ATSC: "ATSC Standard: Companion Device~~(A/338)~~," Doc. A/338:20~~17~~21, Advanced Television System Committee, Washington, D.C., ~~17 April 2017~~19 February 2021.

2.2 Application Intermediate Certificates

Revise 5.2.1 as follows:

5.2.1 ATSC 3.0 Application Code Signing

Executable or interpretable code shall be packaged as a multi-part MIME package and shall be cryptographically signed.

Signed applications shall be formatted as specified in S/MIME Version 3.2 (RFC 5751 [15]) as follows:

1) An Author Signature shall be added first in the manner specified in S/MIME [15] Section 3.4.3 to create a detached signature. The name attribute for the newly created Content Type application/pkcs7-signature shall be set to author.p7s and the filename attribute for the corresponding Content Disposition shall be set to author.p7s. The Author Signature shall only appear as the first detached signature in the final MIME package.
2) A Distributor Signature shall then be added in the manner specified in S/MIME [15] Section 3.4.3 to create a detached signature. The output MIME package from that Author Signature process becomes the input to this step of the process. The name attribute for the newly created Content Type application/pkcs7-signature shall be set to distrib.p7s and the filename attribute for the corresponding Content Disposition shall be set to distrib.p7s. The Author Signature shall appear as the first detached signature in the final MIME package,

and the Distributor Signature shall appear as the second detached signature in the final MIME package.

3) Any compression shall be applied after each of the signatures has been included in the multi-part MIME package. The signatures generated using S/MIME processing shall be encoded according to the Cryptographic Message Syntax (RFC 5652 [13]) with the extension for elliptic curve signature processing as defined in RFC 5753 [16]. Each CMS block shall include an End-Entity certificate that authenticates the signature and a set of any Intermediate Certificate Authority certificates that authenticate issuer(s) of the certificates included in the CMS block.

Revise 5.5.2 as follows:

5.5.2 Certificate Revocation and Status Information for ATSC 3.0 Application Signing Certificates

An ATSC 3.0 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 OCSP Request shall indicate that the preferred signature algorithm to be used by the OCSP responder is RSA with SHA-256.

The SigningTime associated with the ATSC 3.0 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~~ twenty-five (25) hours. The ATSC 3.0 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 6960 [20]) is other than "good".

The application signing authority shall include the object identifier id-ri-ocsp-response in the otherRevInfoFormat field and an OCSPResponse in the otherRevInfo field of each Cryptographic Message Syntax (RFC 5652 [13]) formatted digital signature contained in the signed multi-part MIME content. The OCSPResponse shall conform to the format specified in RFC 5940 [18].

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 CTA 2053 [26].

2.3 Certificate Data Table Certificate Requirements

Revise Sec. 5.2.2.2 as follows:

5.2.2.2 Certificate and OCSP Response LLS Table

This specification defines a new LLS Table that carries X.509 Certificates and OCSP Responses that are used to verify signed signaling tables.

When one or more signaling tables are signed, the CertificationData LLS Table shall be included among the LLS Tables described in ATSC A/331 [26] Section 6.1, and shall use LLS_table_id 0x06, and shall be represented as an XML document containing a CertificationData root element that conforms to the definitions in the XML schema that has namespace:

tag:atsc.org,2016:XMLSchemas/ATSC3/Delivery/CDT/1.0/

Note that the CertificationData LLS Table is a standalone table that contains its own signature (i.e., is not in a signed_multitable message), as the data in the CertificationData LLS Table is required to verify

the signature of a signed_multitable message. Note also that the attributes, certificates, and OCSP Responses carried in the CertificationData LLS Table are unrelated to application signing (Sec. 5.2.1), which has different requirements and a different mechanism for carrying certificates, OCSP Responses and related data.

The XML schema xmlns short name should be "cdt". The CertificationData LLS Table has the following informative description:

Table 5.1 CertificationData XML Format

Element or Attribute Name	Use	Data Type	Short Description
CertificationData			Root element of the CertificationData table.
ToBeSignedData	1		
@OCSPRefresh	1	xs:dayTimeDuration	The duration for which an OCSPResponse carried in this CertificationData is considered valid from its producedAt time.
Certificates	1..N	Base64 String	A list of certificates that are used to authenticate a broadcaster signature. This must include end-entity certificates authenticating the CurrentCert and the CMSSignedData signing certificate and any intermediate CA certificates used to validate these certificates. The Root CA certificate is not included in the list.
CurrentCert	1	Base64 String	SubjectKeyIdentifier for the certificate currently used to sign signaling messages.
CertReplacement	0..1		
@NextCertFrom	1	DateTime	Earliest time at which NextCert can be validly used.
@CurrentCertUntil	1	DateTime	Latest time at which CurrentCert can be validly used.
NextCert	1	Base64 String	SubjectKeyIdentifier for the certificate next used to sign signaling messages.
CMSSignedData	1	Base64 String	A CMS Signed Data structure authenticating the ToBeSignedData contained in this table.
OCSPResponse	1..N	Base64 String	A set of OCSP Responses that provide status information for each of the Certificates carried in this CertificationData.

Note that in the semantics following, only modified text is shown in this document.

ToBeSignedData – The data elements to be included in the signature calculation contained in the CMSSignedData element. The signature contained in CMSSignedData is across all data, including the beginning and ending tags of this field (from the initial "<" through the final ">").

@OCSPRefresh – The duration after which an OCSP Response is considered to be invalid, based on the producedAt time in the response structure and the current system time. This field shall not exceed a duration of ten days (two hundred forty hours), except for test/validation (e.g., with a test/validation indicator) or similar usage, and should not include fractional seconds. Practically, **@OCSPRefresh** should be at least one hour. But note that this value is related to vulnerability periods, see for example, Sec. 4.9.10 of [28], which limits the expiration time of certain OCSP Responses to ten days.

CMSSignedData – The CMS Signed Data (RFC 5652 [13]) element with the following characteristics:

1) The characteristics specified in Section 5.2.2.1 above.
2) The content being signed shall be the full extent of the ToBeSignedData element.
3) The SubjectKeyIdentifier shall identify an end-entity certificate in Certificates other than that identified by CurrentCert, and other than that identified by NextCert if present.

OCSPResponse – A set of one or more OCSP Response structures in the form specified in RFC 6960 [21] that provide certificate status information for the Certificates carried in this CertificationData. Each **OCSPResponse** in the set may contain a number of OCSP Single Response (see RFC 6960 [21]) structures where the same OCSP Responder is authorised to issue a response for more than one of the Certificates.

– End of Document –