ATSC
ADVANCED TELEVISION
SYSTEMS COMMITTEE

ATSC Standard:
A/360:2019 Amendment No. 4, “Section 5.2.2.6”

Doc. A/360:2019 Amend. No. 4
10 January 2022

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

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	10 January 2022

ATSC Standard:
A/360:2019 Amendment No. 4, “Section 5.2.2.6”

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 modifies the informative section 5.2.2.6 to better reflect current operation.

1.3 Rationale for Changes

A/360 Sec. 5.2.2.6 describes (informatively) partially what a receiver is expected to do to verify signatures. This section has some ambiguity and may be misleading, and some aspects of A/360 changed normatively in A/360:2019 Amd 2, so some aspects of Sec. 5.2.2.6 are out-of-date. This amendment corrects this.

1.4 Compatibility Considerations

There are no compatibility issues with this change. This amendment only modifies informative text.

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 Clarify verification of SigningTime

In A/360 Sec. 5.2.2.6, before the numbered list, revise as shown:

To help identify suspected stream tampering, t~~T~~he receiver is expected to undertake the following tasks to verify new instances of the signed signaling messages described in Sections 5.2.2.3, 5.2.2.4, and 5.2.2.5:

In A/360 Sec. 5.2.2.6, paragraph indicated 2(b), revise as shown:

2) Verify that the SigningTime attribute in the CMS Signed Data structure is:
   a) Not greater than the System Time, and
   b) Not less than the SigningTime of any previously received instance of the same type of signed signaling message. For example, the SigningTime sequence would not go backward in time for any signaling within a single message type of (i) SLS of the same specific service, or (ii) an LLS CDT message on the same RF channel or bonded channels, or (iii) an LLS SignedMultiTable message on the same RF channel with the same set of LLS tables within.

2.2 Clarify signing using bonded RF, 'matching' for sets of BSID language

In A/360 Sec. 5.2.2.6, paragraph indicated 3(b), revise as shown:

3) Verify that the key used to sign the signaling message is authenticated by an unexpired end-entity certificate carried in CertificationData message,
   a) verify that this certificate has an extended key usage that includes id-atsc-kp-signalingSigning, and
   b) verify that this certificate contains a Subject Directory Attribute extension with an attribute of type id-atsc-sdattr-bsid and values that contain a SET OF INTEGER (as described in RFC 5280 [10]), and that the set of values matches exactly the set of bsids listed in the Service List Table for this broadcast stream (e.g., when identifying a bonded pair of RF channels, both the bsids listed in the SLT and the set of bsids in the certificate identify exactly the same two bsid values), and
   c) verify that this end-entity certificate's SubjectKeyIdentifier matches either the CurrentCert or, if present, the NextCert.

– End of Document –