



**ATSC**

ADVANCED TELEVISION  
SYSTEMS COMMITTEE

# **ATSC Standard: A/360:2023-03 Amendment No. 1, “MMT DRM”**

---

Doc. A/360:2023-03 Amend. No. 1  
15 August 2023

**Advanced Television Systems Committee**  
1300 I Street, N.W., Suite 400E  
Washington, D.C. 20005  
202-872-9160

The Advanced Television Systems Committee, Inc. is an international, non-profit organization developing voluntary standards and recommended practices for broadcast television and multimedia data distribution. ATSC member organizations represent the broadcast, professional equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries. ATSC also develops 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 Consumer Technology Association (CTA), the Institute of Electrical and Electronics Engineers (IEEE), the National Association of Broadcasters (NAB), the Internet & Television Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). For more information visit [www.atsc.org](http://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	15 August 2023

# ATSC Standard: A/360:2023-03 Amendment No. 1, “MMT DRM”

## 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 updates A/360 to allow for DRM for MMT signaling in addition to DASH signaling, which is already supported.

### 1.3 Rationale for Changes

The changes described in this document are being proposed in order to enable DRM over MMT.

### 1.4 Compatibility Considerations

The changes described in this document are backward-compatible relative to the currently published version of the standard to which this Amendment pertains and any previously approved Amendments for that standard; however currently deployed receivers would not have the capability of decrypting content delivered with this method. Such receivers would need updates if they are to decrypt such content. These changes would not affect any receiver’s ability to present unencrypted content or content delivered using ROUTE-DASH.

## 2. LIST OF CHANGES

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. **Yellow highlights** indicate intended cross-references and other information that is expected to be updated prior to publication within a new revision.

### 2.2 Normative References

*No changes.*

### 2.3 Informative References

*No changes.*

### 2.4 Acronyms and Abbreviations

*No changes.*

### 2.5 Terms

*No changes.*

## 2.6 Change Instructions

*Apply the changes indicated below.*

Strike reference [3].

## 4 SYSTEM OVERVIEW

### 4.1 Features

This specification defines a set of methods designed to secure the following content and data flows described in other ATSC 3.0 specifications:

- 1) Content protection ~~for MPEG-DASH content delivery~~ (Section 5.7).
- 2) Authentication of ATSC 3.0 applications (Section 5.2).
- 3) Authentication of ATSC 3.0 Broadcast Signaling (Section 5.3).
- 4) Interactive data exchanged over an internet connection between an ATSC 3.0 application and a web content server (Section 5.1), including the use of DNS Security (Section 5.1.1.7).
- 5) Data flows between an ATSC 3.0 primary device and a companion device (Section 5.6).

### 4.2 System Architecture

This specification defines a number of profiles for established security specifications defined by IETF, ISO and W3C. In defining these profiles, this specification seeks to establish a consistent use of cryptographic algorithms across the different content and data flows that it addresses. The profiles are designed to provide some degree of flexibility in the choice of cryptographic algorithms being used in a particular flow while enabling the use of commonly available implementations of the specified standard technologies.

~~In the case of MPEG-DASH content protection,~~ This specification defines the use of common encryption techniques that allow content protection ~~licences/licenses~~ to be delivered to a number of different content decryption modules from different suppliers.

## 5 SPECIFICATION

### 5.7 Content Protection

#### 5.7.1 Common Encryption

~~ATSC 3.0 uses the DASH-IF ATSC Profile [3] as the media container that will be sent through the broadcast emission to the receiver for consumption.~~ MPEG Common Encryption (CENC) [2] has been specified as a digital rights management system suitable for use with ISO BMFF. Any media that requires DRM encryption shall use MPEG Common Encryption (CENC).

– End of Document –