ITUPublications

International Telecommunication Union
Standardization Sector

# ITU-T Technical Report

(07/2026)

# HSTP-MMAuth

## Multimedia authentication framework, workflows and procedures

# Technical Report ITU-T HSTP-MMAuth

## Multimedia authentication framework, workflows and procedures


### Summary

Technical Report ITU-T HSTP-MMAuth describes a framework, workflows and procedures for multimedia authentication. It identifies end-to-end workflows for various application scenarios and processing technologies, including streaming, file-based transfer, cross-authentication of different media types, and broadcast delivery. The Technical Report also describes authentication-related entities and their interfaces, including functions for creating, updating, embedding, extracting and verifying media authentication metadata.

The framework is intended to support authentication of multimedia content across capture, editing, packaging, distribution and playback. It considers provenance information, media authentication metadata, certificate infrastructure interactions, and verification over time-based media intervals.



### Keywords

Authentication, authentication metadata, broadcast, certificate, certificate authority, certificate infrastructure, cross-media authentication, file transfer, media authentication, media delivery, media provenance, streaming, verification, X.509.


### Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

### Change Log

This document contains Version 1 of the ITU-T Technical Report HSTP-MMAuth on "*Multimedia authentication framework, workflows and procedures*" approved at the ITU-T Study Group 21 meeting held in Geneva, 6-17 July 2026.


**Editor**: Iraj Sodagar
Dolby Laboratories
USA
E-mail: irajs@live.com



© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## Table of Contents


| | | Page |
|---|---|---|
| 1 | Scope | 1 |
| 2 | References | 1 |
| 3 | Definitions | 2 |
| | 3.1 Terms defined elsewhere | 2 |
| | 3.2 Terms defined in this Technical Report | 2 |
| 4 | Abbreviations and acronyms | 3 |
| 5 | Media authentication end-to-end workflows | 4 |
| | 5.1 General | 4 |
| | 5.2 Streaming workflow | 4 |
| | 5.3 File-based workflow | 6 |
| | 5.4 Cross-authentication workflow | 8 |
| | 5.5 Broadcast workflow | 8 |
| | 5.6 General considerations | 9 |
| | 5.7 Content properties | 9 |
| | 5.8 Authentication properties | 10 |
| 6 | Authentication functions | 10 |
| | 6.1 Authentication author (generate/validate/update) | 10 |
| | 6.2 Authentication verifier | 10 |
| | 6.3 Certificate infrastructure | 11 |

# Technical Report ITU-T HSTP-MMAuth

## Multimedia authentication framework, workflows and procedures

### 1 Scope

This Technical Report covers media authentication procedures in which authentication is achieved by attaching metadata to the content and verification is performed using this metadata and through interaction with a certification infrastructure. In such a process, the metadata contains provenance information, including ownership, and optionally revisions and edits, as well as the capture/creation location and time, and other information such as the origin and original copies of the assets used to create the media content. The information also includes authentication signature(s) as well as owner certificate(s). The information may be added during capture and editing at the source and/or changed or augmented during production and distribution. The consumer of the content may use the metadata to verify that the content has not been altered and to verify the owner certificate, and therefore verify that the content is authentic according to its owner.

The scope includes:

1) End-to-end media authentication workflows for streaming, file-based transfer, cross-authentication and broadcast applications.
2) Authentication interfaces used between capture, editing, authoring, packaging, distribution, playback and verification functions.
3) Functional descriptions of authentication-related entities, including the authentication author, authentication verifier and certificate infrastructure.
4) Considerations for time-based verification of multimedia content, including verification periods, manifest signalling and cross-media authentication.

This Technical Report does not define a specific cryptographic algorithm, certificate authority policy, media container format, manifest syntax or rights management system. Such mechanisms may be specified by other Recommendations, standards or implementation profiles.

### 2 References

[ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[ISO/IEC 14496] ISO/IEC 14496-12:2012, *Information technology – Coding of audio-visual objects – Part 12: ISO base media file format*.

[ISO/IEC 18014] ISO/IEC 18014-2:2021, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[ISO/IEC 23000] ISO/IEC 23000-19:2024, *Information technology – Multimedia application format (MPEG-A) – Part 19: Common media application format (CMAF) for segmented media*.

[ISO/IEC 23009] ISO/IEC 23009-1:2014, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*.

[ISO/IEC DIS 26080-1] ISO/IEC DIS 26080-1, *Information technology – Authenticity for Media – Part 1: Vocabulary*.

[ANSI/SCTE] ANSI/SCTE 214, *MPEG DASH for IP-Based Cable Services*.

[C2PA] Coalition for Content Provenance and Authenticity technical specification v2.4, *C2PA Content Credentials*. Available at: https://spec.c2pa.org/specifications/specifications/2.4/index.html

[ID3] ID3 (1999), *ID3 tag version 2.3.0* available at: https://id3.org/id3v2.3.0.

# 3 Definitions

## 3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

**3.1.1 certificate**: A data structure that binds an identity to a public key and is digitally signed by a certification authority or other trusted entity.

NOTE – As defined in [ITU-T X.509].

**3.1.2 certificate authority**: A trusted party that authenticates the digital identities of entities.

NOTE – As defined in [IETF RFC 5280].

**3.1.3 digital signature**: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient to verify the source and integrity of the data unit.

NOTE – As defined in [ISO/IEC 26080-1].

**3.1.4 media authentication**: Process or action of proving or showing a media asset to be true, genuine, or valid according to its producer.

NOTE – As defined in [ISO/IEC 26080-1].

**3.1.5 media authenticity**: Trustworthiness and reliability of media content, ensuring that it accurately represents the claimed information or events.

NOTE – As defined in [ISO/IEC 26080-1].

**3.1.6 media presentation**: A structured collection of media components and related information that can be delivered and presented to a user.

NOTE – As defined in [ISO/IEC 23009].

**3.1.7 media segment**: A unit of media data that can be individually referenced and retrieved for presentation.

NOTE – As defined in [ISO/IEC 23009].

**3.1.8 provenance**: The history of an asset and its interaction with entities and other assets, as represented by the provenance data.

NOTE – As defined in [ISO/IEC 26080-1].

**3.1.9 watermarking**: Process that imperceptibly inserts data representing some information into multimedia.

NOTE – As defined in [ISO/IEC 26080-1].

## 3.2 Terms defined in this Technical Report

This Technical Report defines the following terms:

**3.2.1 authentication author**: The entity responsible for creating, editing and updating the authentication metadata.

**3.2.2 authentication metadata**: The metadata that carries information necessary for authentication of the content, optionally including provenance information.

**3.2.3 authentication result**: The output of an authentication verification process indicating whether media content, metadata, provenance information or related trust information has been successfully verified.

**3.2.4 authentication status**: Information presented to an application, player, receiver or user interface describing the result or availability of media authentication verification.

**3.2.5 authentication verifier**: The entity responsible for verifying the authenticity of content.

**3.2.6 certificate infrastructure**: A comprehensive network that creates, manages, stores and distributes digital certificates and public-private key pairs.

**3.2.7 cross-authentication**: Authentication of various content components to be consumed together.

**3.2.8 file-based**: Content that is stored in a file.

**3.2.9 inserted content**: Media content that is inserted into an existing media presentation, such as advertising, emergency information, local content or replacement content.

**3.2.10 metadata redaction**: Removal or modification of authentication metadata or provenance information to limit disclosure of selected information while preserving the ability to verify other information where possible.

**3.2.11 media component**: A component of a media presentation, such as video, audio, subtitles, captions, timed metadata or an alternative representation.

**3.2.12 provenance information**: Information describing the origin, creation, editing, transformation, packaging or distribution history of media content.

**3.2.13 streaming manifest**: Document providing information about streaming media content, its format, components, network/Internet location and various attributes.

**3.2.14 verification**: Process of verifying the authenticity of media content using the provided authentication metadata.

**3.2.15 verification period**: A time interval or media interval over which authentication metadata enables verification of the corresponding media content.

## 4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

| | |
|---|---|
| AIF | Authentication Interface |
| C2PA | Coalition for Content Provenance and Authenticity |
| CA | Certificate Authority |
| CDN | Content Delivery Network |
| CMAF | Common Media Application Format |
| CRL | Certificate Revocation List |
| DASH | Dynamic Adaptive Streaming over HTTP |
| DID | Decentralized Identifier |
| DRM | Digital Rights Management |
| MPD | Media Presentation Description |

| | |
|---|---|
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| TSP | Time-Stamp Protocol |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UTC | Coordinated Universal Time |
| VC | Verifiable Credential |
| X.509 | ITU-T Recommendation X.509 public-key certificate framework |
| x-auth | cross-authentication |

# 5 Media authentication end-to-end workflows

## 5.1 General

This clause describes representative end-to-end workflows for multimedia authentication. The workflows identify where provenance information and authentication metadata may be created, updated, embedded, transported, extracted and verified. The workflows are functional and do not imply a mandatory physical deployment architecture.

In these workflows, authentication information may be carried in the media data, in packaging or manifest information, in an external service, or in a combination of these locations. The selected approach may depend on the delivery mechanism, latency requirements, privacy requirements, storage constraints and expected verification behaviour.

## 5.2 Streaming workflow

For streaming delivery, authentication metadata may be associated with media segments, groups of segments, periods, representations or media components. The manifest may provide information enabling the receiver to determine whether authentication metadata is present, which media components are covered, where additional authentication information can be obtained, and whether any playback constraints apply.

When the media presentation is updated during live or low-latency streaming, authentication metadata may also be updated progressively. The receiver may therefore verify content incrementally as media data becomes available. If some verification information is delayed or temporarily unavailable, the receiver may indicate that the corresponding content is not yet verified rather than treating it as failed verification.

If network-side or client-side operations modify the media presentation, such as ad insertion, content replacement or repackaging, the operation should preserve authentication information for unchanged content or create updated authentication metadata for the resulting media presentation.

Figure 1 describes the general end-to-end workflow of media authentication for media streaming applications.

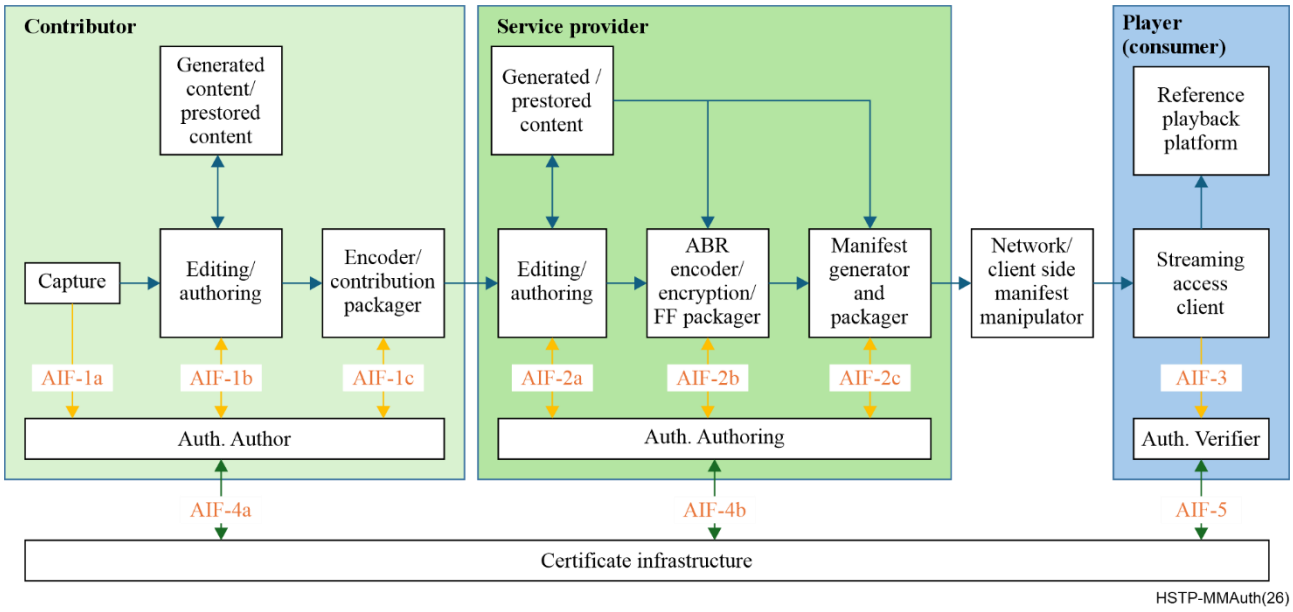



**Figure 1 – The media authentication workflow for streaming**

In this figure, the workflow consists of:

1) Media is captured by the device. Preliminary provenance information is provided to the authentication author function (AIF-1a).

2) The content is edited, manipulated and mixed with prestored and/or generated content. The provenance information is updated, and other authentication metadata is added (AIF-1b).

3) Media is encoded and packaged. The authentication authoring function runs algorithms on the data (AIF-1c), interacts with the certificate infrastructure if needed (AIF-4a) and includes the authentication metadata in encoded and packaged data (AIF-1c). Optionally, it uploads some authentication-related data to the cloud (AIF-4a).

4) Media is provided to the content/service provider.
   a) The content received may be verified by the content/service provider (AIF-2a).
   b) The authentication metadata may be removed/redacted by the content/service provider.

5) The content is edited and revised. It may be manipulated, enhanced or revised and/or combined with other prestored or generated content. The provenance information is provided to the authentication authoring function along with the provenance information provided at the contribution (AIF-2a). The new parts of the content may have their own provenance information.

6) Additional authentication metadata is included during the media packaging and streaming manifest generation (AIF-2b/2c).

7) The media presentation may be repackaged at the network or client side. Such operations maintain the authentication metadata for the part of the media originated from the service provider.
   a) The inserted content (such as an inserted ad) does not impact the authentication metadata nor verification of the main content.
   b) Each inserted content can include its own authentication metadata.
   c) If the inserted content causes failure in the verification of the main content, it either
      1) removes signalling from the manifest to avoid confusing the player, or

2) adds new authentication metadata for the combined content.

8) The player/receiver uses the authentication verifier function (AIF-3) for media verification through AIF-5.
   a) The player can use the manifest to select the media that can be verified.
   b) The verification can occur during the playback of media.

The following authentication interfaces are defined:

- AIF-1a: Capture provenance data
- AIF-1b: Authentication data created during editing
- AIF-1c: Authentication data embedding in encoding/packaging
- AIF-2a: Provenance data update during authoring
- AIF-2b: Authentication data embedding in the media content
- AIF-2c: Authentication data embedding in manifest/packaging
- AIF-3: Extraction of authentication data for verification
- AIF-4a/4b: Authentication author cloud interface
- AIF-5: Authentication verifier cloud interface

## 5.3 File-based workflow

For file-based delivery, authentication metadata may be stored within the media file, in an associated sidecar file, in an external provenance service, or in a combination of these locations. A file-based workflow may support verification before playback, during playback, after transfer, or as part of an ingest process by a service provider.

When a file contains multiple media components, the authentication metadata may identify which components are authenticated independently and which components are authenticated together. If the file is edited, repackaged or combined with other files, the resulting file may require updated provenance information and new authentication metadata.

File-based authentication may also support archival and interchange use cases, where verification is performed long after the content was created. In such cases, timestamp validation, certificate status information and long-term availability of provenance information are important considerations.

Figure 2 describes the workflow for file-based transfer applications.

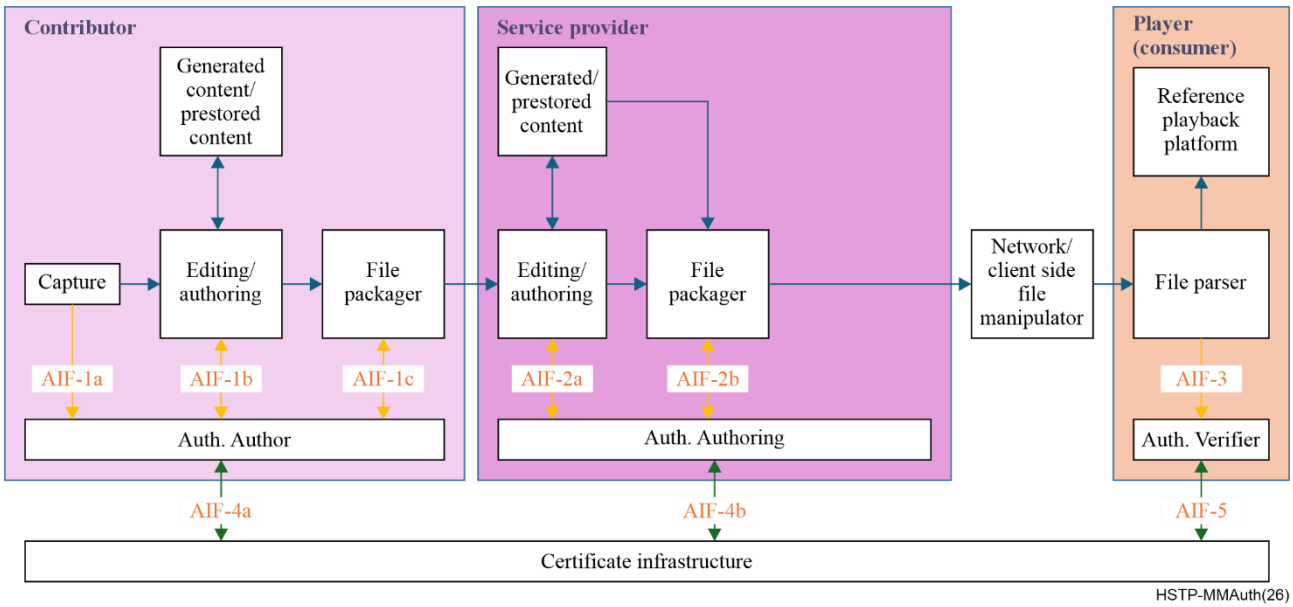



**Figure 2 – The media authentication workflow for file-based transfer**

In this figure, the workflow consists of:

1) Media is captured by the device. Preliminary provenance information is provided to the authentication author function (AIF-1a).

2) The content is edited, manipulated and mixed with prestored and/or generated content. The provenance information is updated (AIF-1b).

3) Media is encoded and packaged into one or multiple files. The authentication author runs algorithms on the data (AIF-1c), interacts with the certificate infrastructure if needed (AIF-4a) and includes the authentication metadata in encoded and packaged data (AIF-1c). Optionally, it uploads some related authentication data to the cloud (AIF-4a).

4) Media is provided to the content/service provider.

   a) The content received may be verified by the content/service provider (AIF-2a).

   b) The authentication metadata may be removed/redacted by the content/service provider.

5) The content is edited and revised. It may be manipulated, enhanced or revised and/or combined with other prestored or generated content. The provenance information is provided to the authentication authoring function along with the provenance information provided at the contribution (AIF-2a). The new parts of the content may have their own provenance information.

6) The media presentation may be repackaged at the network or client side. Such operations maintain the authentication metadata for the part of the media originated from the service provider.

   a) The inserted content (such as an inserted ad) does not impact the authentication metadata nor verification of the main content.

   b) Each inserted content can include its own authentication information.

   c) If the inserted content causes failure in the verification of the main content, it either:

      1) removes signalling from the manifest to avoid confusing the player, or

      2) adds new authentication metadata for the combined content.

7) The player uses the authentication verifier function (AIF-3) for media verification through AIF-5.

   a) The verification may occur during the playback of media.

The media authentication interfaces are a subset of the ones identified for the streaming workflow. All interfaces are the same except AIF-2c, which does not exist in the file-based workflow.

## 5.4 Cross-authentication workflow

Figure 3, based on the above file-based workflow, highlights where cross-authentication (x-auth) mechanisms may be applied.

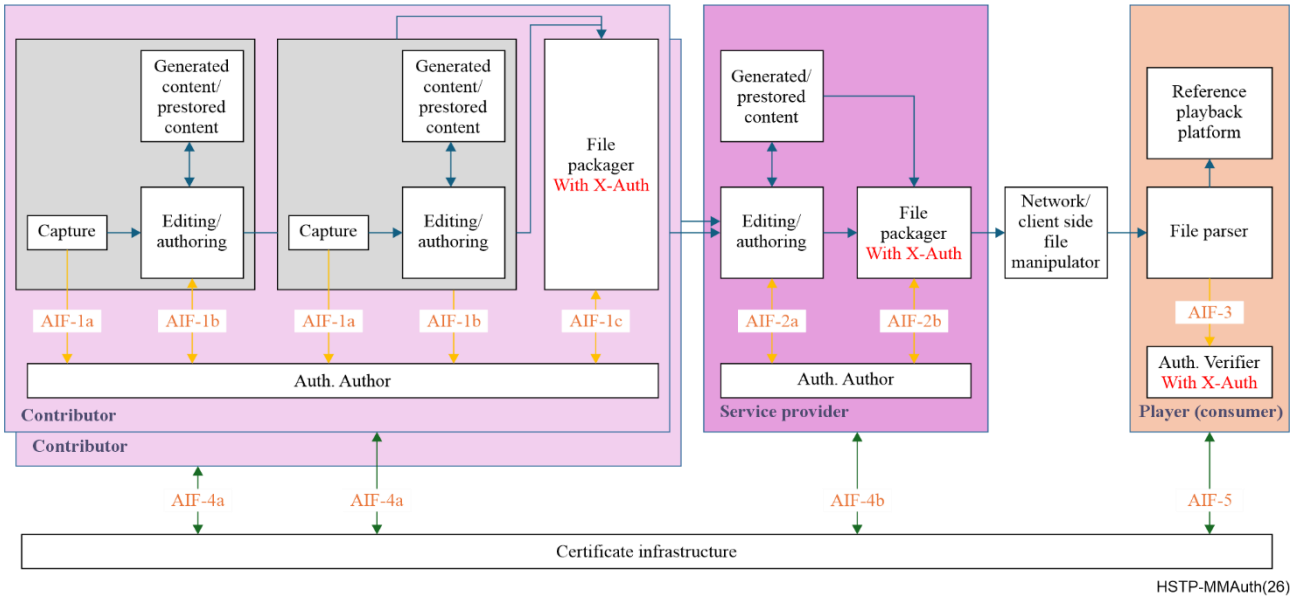



**Figure 3 – File-based workflow with cross-authentication (x-auth) of different media types**

On the contributor side, media components, possibly with different media types (e.g., video, audio tracks, subtitles, etc.) of a media asset are captured (original content), retrieved or generated. Each component is authenticated individually through the AIF-1a and AIF-1b interfaces. Once authenticated, all media components with different media types building the media asset are packaged with cross-authentication performed through the AIF-1c interface. The resulting packaged file is then made available to the service provider. There can be multiple contributors providing media components with different variants or different media types to the service provider, e.g., different audio tracks, etc.

On the service provider side, the packaged file can be edited by modifying existing media types, reusing prestored content or incorporating new ones (possibly from multiple contributors). Similar to contributors, the service provider ensures cross-authentication of the new packaged file, handled through the AIF-2a and AIF-2b interfaces.

## 5.5 Broadcast workflow

Figure 4 describes the workflow for broadcast applications.

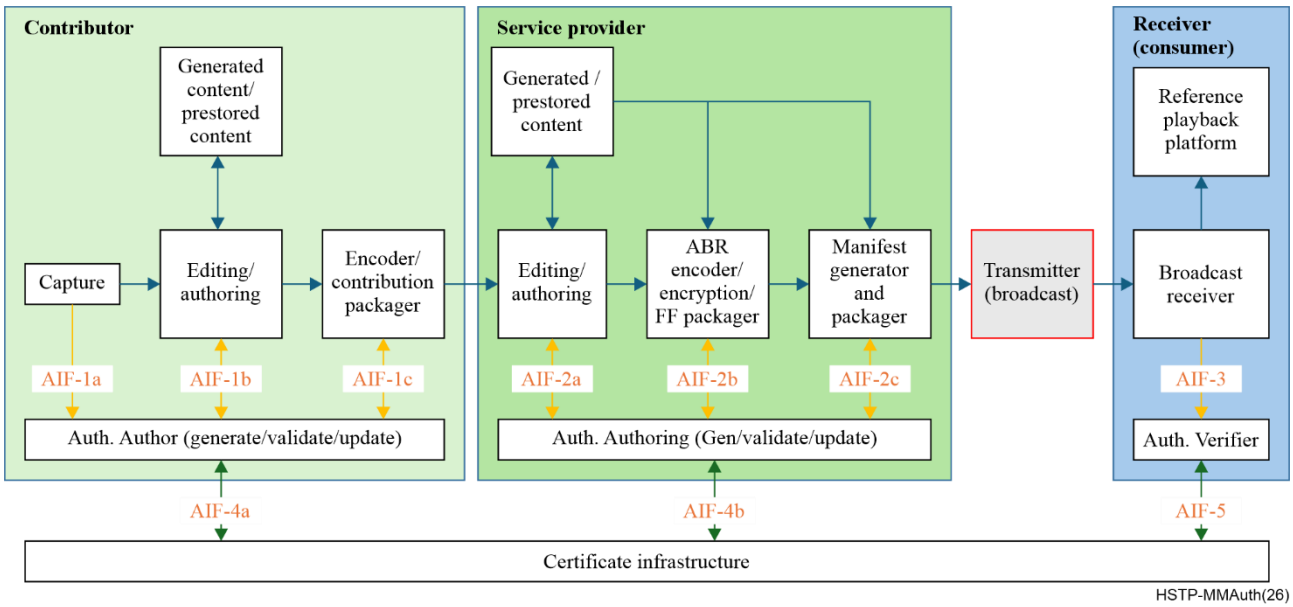



**Figure 4 – The media authentication workflow for broadcast**

As shown in Figure 4, the broadcast media authentication workflow is very similar to the streaming workflow. The major change is the distribution that is achieved through broadcast compared to the network distribution. Note that it is assumed that a local broadcaster is a part of the service provider functionality and therefore in the case of broadcast, the content is not manipulated during the distribution. It is also assumed that the receiver is a connected device, i.e., it can connect to the certificate infrastructure to retrieve certification data such as required keys and signatures.

The authentication interfaces in this workflow are identical to the interfaces in the streaming workflow.

## 5.6 General considerations

The following are considered for the streaming workflow:

- The content is produced by the contributor and/or service provider.
- The receiver is the main consumer that validates the authenticity of the content.
- The service provider may also be a consumer when receiving the contribution, i.e., it wants to validate the received content before editing/repurposing/publishing.
- The certificate infrastructure includes the signature store, the certificate authority and other possible functionalities (such as watermarking validation).
- The workflow covers on-demand, time-shift, live and low-latency content.

## 5.7 Content properties

The following content properties are considered:

1) The content may be produced for on-demand, live or low-latency live consumption.
2) The content may be produced as single- or multi-period [ISO/IEC 23009] content by the contributor and further be spliced into multi-period content by the provider.
3) The content may be stored in a file format such as ISOBMFF [ISO/IEC 14496], or in a packaging format such as CMAF [ISO/IEC 23000] or DASH [ISO/IEC 23009].
4) Time-based events such as ID3 tags [ID3], SCTE 214 [ANSI/SCTE], and DASH events [ISO/IEC 23009] can be added by the contributor or service provider to the content.

5) The content may be manipulated by the provider before delivery or at the client to be spliced with other content (such as ads) including dynamic content insertion and early termination.

### 5.8 Authentication properties

The following authentication properties are considered:

1) The authentication metadata provides information to verify the content for specific verification periods, i.e., each time interval of the content has authentication metadata.
   a) Since the content may be produced on-demand, live or in the low-latency case, the media verification periods are defined to enable each case accordingly.
   b) If authentication verification requires insertion of period transition (i.e., changing the period structure) [ISO/IEC 23009], the resulting content needs to remain conforming to the original content format, including not losing the ad insertion opportunities.
   c) Adding ad insertion opportunities needs to maintain the verification of the content for each verification period intended by the service provider.
   d) A pass-through verifiable content is only possible, if the content is contained in one or more time intervals, marked as "unchangeable".
   e) Cross-media authentication, i.e., authentication between different tracks or representations of media components, needs to be supported.
   f) The authentication data may include the internal or external content credentials and provenance information such as that defined by C2PA [C2PA].
2) The streaming manifest and its updates may provide:
   a) High-level information about the existence of authentication metadata and their format, and possible playback constraints.
   b) The cross-media authentication information, i.e., which tracks are expected to be authenticated together.

## 6 Authentication functions

This clause provides a functional description of the authentication-related entities utilized in the workflows defined in clause 5.

### 6.1 Authentication author (generate/validate/update)

This entity validates, creates, and updates the provenance and media authentication metadata for the media presentation. Its responsibilities include:

1) Validating the authenticity of the content if existing metadata is present.
2) Parsing and updating provenance information.
3) Calculating new hashes and generating new digital signatures.
4) Formatting and embedding media authentication information into a format suitable for integration with the media content.

The authentication author interfaces with the media delivery modules via interfaces AIF-1 and AIF-2, and with the certificate infrastructure via interface AIF-4.

### 6.2 Authentication verifier

This entity is responsible for verifying the authenticity of received media content. It receives the relevant media data along with the associated metadata to perform verification. Because multimedia content is typically time-based, verification is performed continuously at various intervals. The

frequency and boundaries of these verification periods (i.e., the specific segments of content being verified) are defined by the media authentication metadata carried within the content.

This entity interfaces with the media access function via interface AIF-3 and with the certificate infrastructure via AIF-5.

### 6.3 Certificate infrastructure

This entity represents the network or cloud-based functionality that enables the following functions:

1) For authoring (AIF-4):
   a) Registration with a certificate authority (CA) [ITU-T X.509].
   b) Provisioning of certificates and public/private key pairs [ITU-T X.509] and [IETF RFC 5280].
   c) Provisioning of signed timestamps [ISO/IEC 18014].
   d) Cloud storage for provenance information [C2PA].
2) For verification (AIF-5):
   a) Retrieval of provenance information stored in the cloud [C2PA].
   b) Verification of the certificate authority's validity [ITU-T X.509] and [IETF RFC 5280].
   c) Verification of the certificate validity and the intermediate trust chain [ITU-T X.509] and [IETF RFC 5280].
   d) Provisioning of certificate status and timestamp validation [ITU-T X.509], [ISO/IEC 18014] and [IETF RFC 5280].