ENGINEERING REPORT

Results of the SMPTE Survey on Content Provenance and Authenticity in Media

SMPTE ER 1012:2026-11

The home of media professionals, technologists, and engineers.

Copyright © 2026 by SMPTE ® - All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, with the express written permission of the publisher

SMPTE ENGINEERING REPORT

Results of the SMPTE Survey on Content Provenance and Authenticity in Media

Table of Contents

Foreword **5**
1 Scope **5**
2 Introduction **5**
3 Analysis (AI versus Human) **6**
4 Respondent Demographic **6**
5 Results Summary **8**
5.1 Introduction 8
5.2 General CPA 8
5.3 CPA in MXF 11
5.4 User Stories 14
6 Functional Requirements **15**
6.1 Content Acquisition and "First-Mile" Trust Requirements 15
6.1.1 Hardware-Based Cryptographic Signing at Origin 15
6.1.2 Embedding Geospatial, Temporal, and Environmental Context 16
6.1.3 Support for External Planning and Assignment Metadata 17
6.1.4 Offline Metadata Generation and Synchronization 17
6.2 Post-Production, Editorial, and AI Workflow Requirements 17
6.2.1 Management of Ingredient and Derivative Relationships 17
6.2.2 Mandatory Disclosure of AI and Generative Tools 19
6.2.3 Signing of Editorial Operations and Accountability 19
6.2.4 Inclusion of Usage Rights and Consent Metadata 19
6.3 Distribution, Packaging, and Real-Time Workflow Requirements 20
6.3.1 Shot-by-Shot Granularity in Live Streaming 20
6.3.2 Interoperability Across Mezzanine and Distribution Formats 21
6.3.3 Verification of Incomplete or Broken Trust Chains 22
6.3.4 Platform Independence for Delivery 22
6.4 Ingest, Categorization, and Real-Time Verification Requirements 23
6.4.1 Real-Time Ingest Verification 23
6.4.2 Automated Categorization Based on Provenance Metadata 24

Copyright © 2026 by THE SOCIETY OF MOTION PICTURE AND TELEVISION ENGINEERS
50 Main Street, Suite 1000, White Plains, NY, 10606, (914) 761-1100
Approved November 11, 2026

6.4.3 Detection of AI Manipulation in External Content 24
6.5 Archival Integrity and Long-Term Stewardship Requirements 25
6.5.1 Validation of Expired Certificates and Re-Signing 25
6.5.2 Alignment with Preservation Metadata Standards (Library Standards) 25
6.5.3 Embedding Provenance in Digital Birth Workflows for Analog Media 25
6.6 Privacy, Redaction, and Identity Management Requirements 26
6.6.1 Selective Redaction of Metadata for Source Protection 26
6.6.2 Institutional "Vouching" and Trust Anchors 26
6.6.3 Differentiation of Actor Identity Levels 26
6.7 Binding Mechanisms, Watermarking, and Resilience Requirements 27
6.7.1 Soft-Binding via Invisible Watermarking 27
6.7.2 Frame/Track Level Integrity Checksums 28
6.7.3 Resilience Against "Metadata Washing" 28
6.8 User Experience and Consumer Trust Signaling Requirements 29
6.8.1 Implementation of Progressive Disclosure (Levels 1-4) 29
6.8.2 Integration of Provenance in Media Management Systems 29
6.9 CPA Metadata for Material Exchange Format (MXF) 29
6.9.1 Introduction 29
6.9.2 No MXF Revision 29
6.9.3 Frame Accuracy 30
6.9.4 Multi-Step Editing 30
6.9.5 KLV, RegXML and JSON Compliance 30
6.9.6 Immediate Solution 30
6.9.7 Whole File CPA Metadata 30
6.9.8 Diverse CPA Metadata for Diverse MXF Applications 30
6.9.9 Whole File Hashes and Itemized Essence Hashes 31
6.9.10 Contributor Identity Inclusion 31
6.9.11 CPA Metadata Security 31
7 Potential Requirement Gaps 31
7.1 Existing Requirements from other organizations (JPEG Trust, C2PA, CAWG) 31
7.2 Unique Requirements identified by the SMPTE Study Group 32
7.2.1 Acquisition and Creation 32
7.2.2 Production, editing and transformation 33
7.2.3 Distribution, packaging and interoperability 33
7.2.4 Ingest, Categorization, and Real-Time Verification 33
7.2.5 Archiving and long-term preservation 33
7.2.6 Privacy, Redaction, and Identity Management 34
7.2.7 Consumer Presentation 34
7.2.8 MXF Specific Requirements 34
8 Legal Requirements 34
9 Conclusions and Recommendations 36
9.1 Urgent Need 36

 © SMPTE 2026 – All Rights Reserved

9.2 Terminology 36
9.3 Legislative Requirements 36
9.4 Holistic Solution 37
9.5 Transparency 37
9.6 Support for C2PA 37
9.7 Support for professional media editing 38
9.8 Transparent MXF encapsulation and extraction 38
9.9 Soft-binding robustness and content 38
9.10 Classification of manipulated or tampered content 39
9.11 Technology Limitation Consideration 39
10 Acknowledgments 40
ANNEX A User Stories 41
ANNEX B Demographic Survey Data 72
ANNEX C Example Categories for Manipulated or Tampered Content 75

© SMPTE 2026 – All Rights Reserved

Notice on the Use of Artificial Intelligence (AI)

Content contained in this publication may have been developed, in part, with the assistance of artificial intelligence (AI) tools used to support drafting, editorial preparation, or document structuring. Any material generated or suggested by such tools has been reviewed, validated, and authorized by appropriately qualified human experts in accordance with SMPTE's established procedures for standards development. SMPTE affirms that the final normative and informative content of this document is the result of human judgment and oversight. The use of AI tools does not diminish, replace, or alter the responsibility held by SMPTE and its duly constituted committees for the accuracy, reliability, and technical integrity of the published standard.

© SMPTE 2026 – All Rights Reserved

Foreword

The Society of Motion Picture and Television Engineers (SMPTE) is an internationally-recognized standards developing organization. Headquartered and incorporated in the United States of America, SMPTE has members in over 80 countries on six continents. SMPTE's Engineering Documents, including Standards, Recommended Practices, and Engineering Guidelines, are prepared by SMPTE's Technology Committees. Participation in these Committees is open to all with a bona fide interest in their work. SMPTE cooperates closely with other standards-developing organizations, including ISO, IEC and ITU. SMPTE Engineering Documents are drafted in accordance with the rules given in its Standards Operations Manual.

For more information, please visit www.smpte.org.

1 Scope

Identify content provenance and authenticity technologies, areas of work and activities in other professional media organizations and make recommendations where SMPTE can update existing or create new standards to support the flow of content provenance and authenticity information. Gather use cases and requirements. Summarize those findings and recommendations in one or more study group reports.

2 Introduction

For more than a century, SMPTE has brought the media industry together to address shared technical challenges through standards development, research, and collaboration. As artificial intelligence (AI) and synthetic content become increasingly integrated into professional media workflows, SMPTE's work extends to the technical frameworks needed to support interoperability, content authenticity, and trust.

The SMPTE Study Group (SG) on Content Provenance and Authenticity (CPA) in Media was established in response to the growing need for trustworthy media workflows as AI and synthetic content become more prevalent. As media professionals face mounting challenges in verifying the integrity of digital assets, the Study Group was tasked with assessing how current content provenance and authenticity technologies impact media production and distribution. Its mission includes developing use cases, gathering requirements, and recommending areas for new or updated standards, particularly in relation to the carriage of provenance metadata within professional formats such as Material Exchange Format (MXF).

This report presents the results of the Study Group’s first public survey, which was launched to collect broad industry input from individuals, companies, and professional organizations. The survey explored how authenticity and provenance metadata are used, needed, and challenged across real-world media environments. It included both a general section and an MXF-specific section, allowing respondents to share personal and organizational perspectives.

The findings summarized in this report aim to:

- Identify gaps in CPA requirements.
- Explore interoperability with emerging technologies such as the Coalition for Content Provenance and Authenticity (C2PA) specifications.
- Inform future SMPTE work that supports secure, verifiable, and trustworthy media production.

By analyzing the survey responses, this report contributes to the Study Group’s broader goal of enabling SMPTE standards to bind, carry, preserve, and extract provenance metadata throughout the media lifecycle. It also lays the groundwork for future recommendations and potential standardization efforts that will help ensure the integrity and transparency of media content in an evolving digital landscape.

© SMPTE 2026 – All Rights Reserved

3 Analysis (AI versus Human)

This engineering report was developed with the assistance of AI tools. The SG received substantial data from its media industry survey, which rendered manual analysis challenging and time intensive. The raw survey data was processed through a Large Language Model (LLM), generating an AI report that informed the subsequent preparation of the engineering report by human experts. All content from the AI report used in the engineering report underwent thorough human review prior to inclusion. Figure 1 outlines the high-level workflow for producing the engineering report and specifies the stages at which AI tools were utilized.

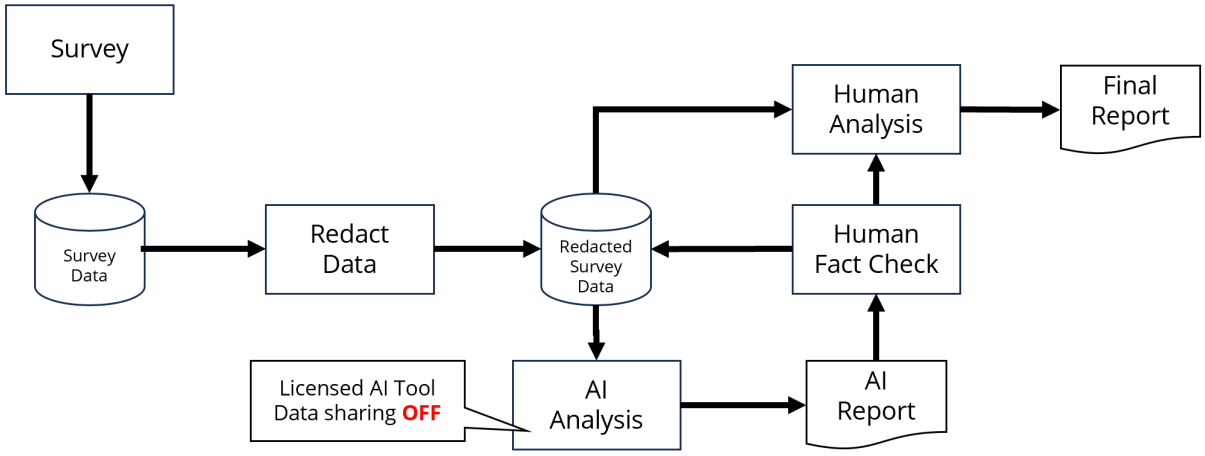


Figure 1 – High-level report creation workflow

The following LLM was used in the creation of this report: Google Gemini 3, Deep Research, Thinking Mode

4 Respondent Demographic

The validity of any standardization effort rests on the breadth and depth of the stakeholders it engages. The demographic data collected in the survey, specifically through the columns "What is your current role in media production or distribution workflows?" and "What types of media workflows are you involved in?", offers a critical view into the segments of the industry that are currently mobilized around the issue of content provenance. Table 1 shows the main responses to both questions in abbreviated and summarized form. The full and unabbreviated list of survey responses to both questions can be found in ANNEX B Demographic Survey Data.

What is your current role in media production or distribution workflows?	What types of media workflows are you involved in?
CTO	Live Events
Developer	News
Screen Producer	Sport
Director Broadcast Engineering	Entertainment
Content Authenticity Lead	Distribution
VFX Supervisor	Film Production
Cinematographer	Postproduction
Director, Solutions & Sustainment	Education
Head of Education	Archival
AI Artist	Research and Development

© SMPTE 2026 – All Rights Reserved

Camera Maker	Content Protection
Technical Director	Streaming
Manufacturer	Advertising
Software Engineer	Broadcast
Software Vendor	Syndicated Programming
Researcher	TV Production
Product Manager	Innovation
Network Line Producer	Quality Control
Material Exchange Department	
Director R&D	
Managing Director	
Audio Specialist	
Standards Developer	
Director Studio Engineering	
Supplier	
Director of Production System Architecture	
Colorist	
Head of Competence Center Production & Infrastructure	
VP, Enterprise Metadata Management	
Lead Architect	
SVP Engineering	
Consultant	
Director, Advanced Content Production	

Table 1 – Abbreviated survey responses for two demographic questions

Responses to the survey came from all parts of the media ecosystem and survey participants work in roles across the industry. This suggests that any discussion about CPA needs to address the whole ecosystem of professional media from acquisition to postproduction, distribution and archival. Survey answers also included feedback from streaming providers with considerations for downstream services like online streaming and broadcasting. This points at the daring task to have a holistic discussion about the implementation of CPA across the whole media ecosystem and possess a complex challenge for any work in standardization to define interoperable solutions.

In addition, the survey responses show that approximately 57% of responses identify as individuals while 43% identify themselves as responding on behalf of their organization. The prevalence of individual respondents may suggest that the expertise in content provenance is currently decentralized. It may reside heavily within specialized technologists who operate across multiple clients or projects, rather than being solely concentrated within the monolithic policy departments of major corporations. At the same time, the organizational responses carry strategic weight due to the market power of the entities represented. The identity of organizations who participated in this survey will not be revealed in this report due to confidentiality requirements.

The roles of those responding to the survey indicate that they are mostly active in the technical field (e.g. Technical Distribution, Systems Engineering, Software Development). Only a few responses from creatives and others were received (e.g. AI Artist, VFX Supervisor, Head of Education). This is not surprising given the technical field SMPTE is active in and in which it conducted this survey.

© SMPTE 2026 – All Rights Reserved

Furthermore, SMPTE received survey replies to both sets of questions, live and non-live, which indicates that the interest in addressing the challenges to enable CPA solutions exists in both types of workflows.

The survey replies come from industry professionals working with video, audio, data and metadata. They bring feedback about the use of compression system, transcoding, editing, metadata annotation, packaging audio, image sequences, intra and inter frame compression formats for distribution, and mezzanine compression formats.

5 Results Summary

5.1 Introduction

The survey opened on September 3, 2025, and was conducted over multiple months. On January 12, 2026, about 4.5 months after the survey opened, the Study Group members decided not to consider any more responses for this report. At that point about 127 responses were received. This report is based on these 127 responses. The tables below show the raw data collected by the survey including comments by respondents in free form text fields.

About 80 unique user stories were collected, either through the survey or from CPA efforts already underway in SMPTE.

The survey remains open to allowing more responses to be submitted. These responses may be considered at a later point or in subsequent reports of this group.

5.2 General CPA

For live workflows, which of these categories describe your interaction with media streams in general?

Type of interaction with media streams (live)	Number of Responses
Receive media streams created by other production steps	53
Deliver media streams to other production steps	51
Develop software to create, store, retrieve or modify media streams	39
Work on operations metadata, such as playlists, rundowns etc.	38
Work with business metadata, such as rights, transactions etc.	37
Distribute media streams to consumers	35
Develop hardware to create, store, retrieve or modify media streams	21

For non-live workflows, which of these categories describe your interaction with media streams in general?

Type of interaction with media streams (non-live)	Number of Responses
Receive media streams created by other production steps	65
Deliver media streams to other production steps	65
Work on operations metadata, such as playlists, rundowns etc.	47
Develop software to create, store, retrieve or modify media streams	46
Distribute media streams to consumers	37
Work with business metadata, such as rights, transactions etc.	35
Develop hardware to create, store, retrieve or modify media streams	20

Which of the following use cases are relevant to your work?

© SMPTE 2026 – All Rights Reserved

Use case	Number of Responses	%
Verifying source integrity of incoming footage	61	74
Confirming provenance of incoming footage	55	66
Authenticating final deliverables for syndication, live broadcast, and/or distribution	54	65
Ensuring essence integrity (e.g., picture, sound)	51	61
Embedding human-generated content provenance	46	55
Embedding AI-generated content provenance	46	55
Tracking editorial changes across production stages	46	54
Ensuring metadata integrity (e.g., geolocation, timestamps)	45	54

Note: 83 respondents answered this question, % figure is of those who provided an answer

Which of the following use cases are relevant to your work (Comments field)?

Comments
While I've not selected "tracking editorial changes across production stages", we still view it as useful, and have included use cases around it.
Ownership (Business License, Consumer Purchase)
Process for determining whether media is AI-generated
Our focus is mainly on metadata in production workflows. Strong authentication is not always needed.
Speech to text from AI, subtitling insertion from AI.
Embedding source and audit information into final deliverables for distribution, and verifying it.
The integrity of the information, picture or sound essence delivered is of utmost importance.
In news programs and across all other genres, ensuring the reliability of source materials and the transparency of editing histories is essential to maintaining trust with viewers. When producing programs that incorporate AI-generated content, we are considering appropriate methods for embedding provenance information.

In your media workflows, where do you see the greatest need for verifying content authenticity?

Workflow	Responses	%
Distribution	58	72
Ingest	50	62
Acquisition	49	62
Editing	46	57
Archiving	45	67
Packaging	27	33
Audit	24	30
Annotation	22	28

© SMPTE 2026 – All Rights Reserved

In your media workflows, where do you see the greatest need for verifying content authenticity?

Comments
We view "editing" and "packaging" as important too, but have highlighted those which we see as highest priority.
We provide DRM for security and now C2PA for provenance
Enrichment (Encoding, Transcoding, Watermarking, Closed Captioning, Subtitling)
Determining whether it is synthetic media
Original production audio is often lost and replaced with data reduced/damaged copies
Not sure about question. "Greatest" sounds like a select one. Verifying content authenticity must be done for all content as soon in the chain as is possible. So while I selected "Distribution" as in before it goes out the door. Verifying Authenticity should be done as soon as possible and if needed more than once.
Two types of Trust/authenticity required 1- B2C, provide trustworthy content to our audiences 2- B2B, ensure the content available in our production systems is trustworthy to use by our production teams
Audio
Consumer viewing
Reception
I appreciate that authenticity markers will impact the whole chain from Acquisition through archiving, but the largest need in my opinion is actually in Archiving.
(Acquisition includes Ingest in our view) Overall C2PA strategy still under discussion
To ensure reliability as news content, verification at the acquisition and ingest stages is essential. Authenticity must also be maintained during editing, distribution, and storage to prevent tampering and to manage provenance records.
While acquisition may be seen as an initial priority, I believe for C2PA to achieve its goals, the whole production chain, historically described as glass-to-glass must support verification of content authenticity
During media consumption
AI augmentation and validation
We would especially call out the nature of the content itself (photographic? AI-augmented? Art illustration? Deep fake?) and also add security of added metadata and provenance such as IPR and licensing content.
User agent(s)
RAW transcoding, metadata extraction
Needs to be available at all stages of the media lifecycle

How important are the following characteristics of provenance metadata?

Characteristics of provenance metadata	Absolutely essential	Very important	Moderately important	Slightly important	Not important
Survives format conversions	46 (62.2%)	21 (28.4%)	4 (5.4%)	1 (1.4%)	2 (2.7%)
Machine-readable and automatable	49 (64.5%)	23 (30.3%)	4 (5.3%)	0 (0.0%)	0 (0.0%)
Cryptographically secure	46 (61.3%)	18 (24.0%)	9 (12.0%)	0 (0.0%)	2 (2.7%)
Human-readable	13 (17.3%)	18 (24.0%)	27 (36.0`%)	10 (13.3%)	7 (9.3%)

Characteristics of provenance metadata	Absolutely essential Very important	Absolutely essential Very important Moderately important
Survives format conversions	90.5%	95.9%
Machine-readable and automatable	94.7%	100.0%
Cryptographically secure	85.3%	97.3%
Human-readable	41.3%	77.3%

© SMPTE 2026 – All Rights Reserved

Note: 77 respondents answered this question

Note: % figure is of responses to each of the characteristics

5.3 CPA in MXF

How familiar are you with MXF?

Types of metadata	Responses
Very familiar/actively working	61
Somewhat familiar	39
Not familiar	19
No reply	7

Note: 119 respondents answered this question.

In your media workflows, where do you use MXF?

Workflow	Responses	%
Ingest	37	65
Editing	33	58
Packaging	31	54
Distribution	31	54
Archiving	30	53
Shooting	29	51
Audit	10	18
Annotation	8	14

Note: 57 respondents answered this question, % figure is of those who provided an answer.

Which MXF wrapping do you use in your media workflows?

	Wrapping	Responses	%
1	Clip	22	63
1	Frame	22	63
1	GoP	22	63
2	Field	8	23

Note: 35 respondents answered this question, % figure is of those who provided an answer.

© SMPTE 2026 – All Rights Reserved

Which MXF operational pattern (OP) do you use?

Operational Pattern	Responses
OP1a	36
Atomic AVID Media Files	21
Atomic IMF files	7
Atomic DCP OP Atom	6
Other SMPTE ST 377-1 (OP2a … OP3c)	3

Note: 40 respondents answered this question.

What type(s) of metadata are included within MXF files?

Types of metadata	Responses
Descriptive Metadata scheme 1 (DMS1)	14
Other standard metadata	11
Proprietary metadata	11
Other descriptive metadata	10
Other SMPTE metadata	9
Dynamic metadata in body partition	5
ST 377-2 KXS	3

Note: 29 respondents answered this question

Which media formats in addition to MXF do you use?

Format	Responses
MP4	39
JPEG	34
TIFF	25
DPX	11
ISOBMFF	10
OpenEXR	10
JUMBF	5
DNG	4
Proprietary	9
Other	16

© SMPTE 2026 – All Rights Reserved

What are your expectations for compatibility between provenance metadata embedded within MXF files and in other media formats?

Comments
I expect that MXF files will behave in the same way as other container formats in C2PA behave: they can be used to embed C2PA provenance, they can be referenced as "ingredients" from non MXF files, and MXF files can use C2PA provenance to reference non-MXF files as "ingredients".
Maintaining the continuity and integrity on the authenticity and provenance of media content through each system, application, service, and function of the media supply-chain.
One hopes it could all work
Must be absolutely transportable
Compatibility and Interoperability
Interoperable
They should be cross-compatible, if possible.
High compatibility
Ensuring interoperability with provenance information from other file formats, such as MXF structure metadata and description metadata, is likely challenging. However, C2PA is already gaining traction in formats like MP4 and MOV, and workflows involving container conversion with MXF are easily conceivable. Therefore, we would appreciate your careful consideration of interoperability as well.
The provenance should be added when the format is changed.
I hope that an environment will be established in which technical information and other data can be carried over to other media formats.
In the content production workflow, I want provenance metadata to be preserved when integrating and converting media formats, such as from mp4 and wav to MXF, and from MXF to other formats like mp4.
Ideally all metadata would be transferrable between MXF and other formats. We use other formats as integrally to our workflows, so provenance metadata not moving to other formats will make any effort in this area pointless.
We expect that provenance metadata embedded within MXF files should remain intact and verifiable when content is converted or exported to other media formats
Full compatibility
Improved interoperability between MXF and common formats like MP4 ・Retention of provenance during format conversion ・Adoption of standards like C2PA and W3C PROV Additional Note: Consistency in authenticity management is crucial for reliability and tamper prevention across formats.
Not loosing the quality during conversion of formats. Security.
The authenticity of clips or content should be guaranteed by the person who last edited them, therefore compatibility of provenance information between each process stage is not important. Rather, attention must be paid to the risk that provenance information added in upstream processes may be arbitrarily misused.
I want the history to be properly preserved when something that was handled in MXF is converted to MP4. It should maintain consistency regardless of the media format.
My expectation is that provenance metadata should maintain a hard binding to the media, regardless of format. Ideally, any processing step in the workflow—rundown, video mixer, MAM, transcoding—should forward the full provenance chain intact, preserving the end-to-end cryptographic trust. Alternatively, if full chain forwarding is not feasible in practice, we could agree on a hardware-attested binding at each step, where each processing node independently signs its contribution and appends it as an assertion to the manifest. This would still preserve verifiable provenance without requiring the entire chain to move physically through every workflow step.
Enable to convert MXF metadata from other media formats
You would hope they would have the same taxonomy
Should be compatible in every workflow (container-agnostic)

Note: 23 respondents answered this question

© SMPTE 2026 – All Rights Reserved

5.4 User Stories

The study group survey asked participants to submit user stories detailing their needs and requirements for CPA in media workflows. Additionally, several user stories were collected from SMPTE internal groups working on content provenance and authenticity solutions or from outside organizations engaged in SMPTE.

Around 80 distinct user stories were collected, reviewed and categorized. These are listed in ANNEX A User Stories at the end of this document.

Initial analysis identified five overall categories or ‘buckets’ of user stories, indicated below. Further analysis subsequently led to more detailed categorization and to the extraction of the functional requirements listed in clause 6.

Bucket A: Acquisition and Creation (The Root of Trust)

This bucket encompasses the initiation of the "glass-to-glass" trust chain. The primary objective here is to bind physical reality (light hitting a sensor) to a cryptographic assertion.

Key Takeaways for Bucket A:

The primary requirement is hardware-based signing and offline capability. A standard must define how an acquisition system’s secure element interacts with the file system (MXF/MP4) to write provenance metadata with minimum latency. Additionally, a standardized protocol for pushing editorial metadata into the acquisition system’s signing environment is required.

Bucket B: Production, Editing, and Transformation (The Chain of Custody)

This bucket addresses the "messy middle" where content is ingested, transcoded, edited, and composited. The challenge is maintaining the chain of trust when the essence is altered.

Key Takeaways for Bucket B:

The central theme is Transformation vs. Preservation. A solution must preserve hashes where the essence is unchanged. Where the essence is transformed, for example by transcoding or color grading, the transformation must be recorded in signed metadata identifying the operation and the trusted party that performed it (see 6.3.2). Edited content is assembled from sub clips of source content. Source metadata must pass accurately to the output, so a system must be able to extract portions of the source CPA metadata and compose them into the final product.

Bucket C: Distribution, Packaging, and Interoperability (The Last Mile)

This bucket covers the final stage where content leaves the professional environment (MXF) and is prepared for consumer delivery (DASH, HLS, MP4, Web delivery).

Key Takeaways for Bucket C:

The requirements here focus on persistence across transcoding. The standard must define how CPA metadata maps from MXF (KLV) to ISO BMFF (Boxes) and other transport formats such as MPEG-TS. Soft Binding (Watermarking) is identified as a critical fail-safe for when metadata is stripped. Ad-Tech Interoperability requires specific schema extensions.

Bucket D: Archiving and Long-Term Preservation (The Long Tail)

© SMPTE 2026 – All Rights Reserved

This bucket focuses on the durability of the provenance data over decades, often involving format migration and the expiration of cryptographic keys.

Key Takeaways for Bucket D:

The primary requirement is metadata alignment and format agnosticism. A solution must define how a CPA instance maps to archival standards. Legacy format support dictates that SMPTE should define CPA carriage for broadcast wave format (BWF or RIFF chunks), beside other formats. A technical solution to address the expiration of certificates is required.

Additional comments from SG:

See: subclauses 6.3.3 and 6.5.1 for additional comments and use cases dealing with certificates and Certificate Authorities.

Bucket E: Ad-Tech and Originator Profile (The Commercial Trust Layer)

This bucket represents a specific, highly organized effort to use provenance for commercial identity and brand safety.

Key Takeaways for Bucket E:

The Originator Profile (OP) is a parallel trust framework that should be interoperable with other CPA technologies. SMPTE standards should allow for OP-defined identity assertions (e.g., Verified Credentials) to be carried within the CPA metadata structure in MXF files to satisfy market requirements.

6 Functional Requirements

User stories from the survey were reviewed, consolidated, and systematically analyzed by an AI model (Google Gemini 3, Deep Research, Thinking Mode) to identify common themes and workflow needs. It then derived an initial set of functional requirements which were discussed and annotated by the members of the Study Group. Each requirement represents one or more user stories.

These functional requirements have been used by the SG members as the basis for forming the Study Group’s conclusions, identifying key findings across the media lifecycle. The functional requirements are listed in the following subclause 6.1 to 6.9. Study Group members added comments based on their discussion of each functional requirement.

In addition, the DMS-II Drafting Group which works on carriage of content provenance, identity, and authenticity metadata in MXF contributed functional requirements to this report (see subclause 6.9). This ensures alignment with ongoing standards development in SMPTE.

6.1 Content Acquisition and "First-Mile" Trust Requirements

The "first-mile" problem represents the most critical vulnerability in the provenance chain: ensuring that the record begins at the very moment of capture. Without secure, in-camera signing, the link between the physical world and the digital file remains unverified.

6.1.1 Hardware-Based Cryptographic Signing at Origin

The system must provide the capability for capture devices, including professional cinema cameras, news cameras, audio recorders, and mobile devices, to generate, sign, and embed a CPA metadata at the moment of recording. This CPA metadata must include an immutable "Origin" assertion that represents the software or device that initially created the asset.

© SMPTE 2026 – All Rights Reserved

- **Associated Story Numbers:** 018, 039, 040, 051, 052, DMS-II-2, Vendor-2.
- **Context and Implications:** Journalists and field reporters require that their mobile-recorded clips contain device signatures and equipment details to prove the video is authentic and has not been intercepted or altered over untrusted transport. Camera manufacturers emphasize that this data must be traceable to a specific camera and author. In the future, this "first-mile trust" will be the primary defense against "camera-to-cloud" intercept attacks, where synthetic content is injected into a newsroom feed.

Additional comments from SG:

Professional recording devices may be less susceptible to manipulation from the outside of the camera than consumer recording devices. Professional recording device output may be subject to redaction to ensure journalist safety.

See: subclause 6.1.4 and 6.6.1 for additional comments and use cases concerning journalist safety in conflict/war zones, etc.

6.1.2 Embedding Geospatial, Temporal, and Environmental Context

Beyond simple identity, the acquisition device must capture and bind high-integrity metadata regarding the physical circumstances of the recording, including GPS location, wall clock time, lens/sensor characteristics.

- **Associated Story Numbers:** 018, 039, 042, 050, 057, DMS-II-2, Vendor-2.
- **Context and Implications:** A Field Reporter or News Camera Operator needs this data available throughout the production workflow to allow downstream consumers to verify the video's authenticity. This requirement ensures that the "where" and "when" of news reporting are as verifiable as the "what." Additionally, VFX supervisors, forensic analysts and others require precise lens distortion and sensor characteristics to be embedded. They can aid for example in physically accurate lighting and photoreal integration during post-production.

Additional comments from SG:

In some use cases it is important to also record the point of view of a camera which would include information such as field of view, lens axis/tilt etc. if it is available.

In the UK and EU, more use is being made of Galileo for timing references and location, so we would prefer to see the use of the generic term GNSS rather than the specific GPS (which is the US system). In the UK and EU due to interference, there is also a renewed interest in terrestrial timing systems, such as NPLtime, so timing may be derived from non-GNSS systems in the near future.

There may be a use case to insert location data into the camera output. Whilst the SG agrees that this is preferred for most circumstances, there are specific use cases where we cannot add location data to a video stream. Selective redaction or omissions in conflict zones may be required (see subclause 6.6.1). For example, a journalist embedded with a military unit reporting from a war zone, warship etc. There may be exceptions required for national security, security of personnel etc.

© SMPTE 2026 – All Rights Reserved

6.1.3 Support for External Planning and Assignment Metadata

Capture devices may facilitate the embedding of external metadata not generated by the device itself, such as story assignments, unique project IDs, or technical contact information, received from a Newsroom Computer System (NRCS).

- **Associated Story Numbers:** 012, 015, 025, 031, DMS-II-1, Vendor-1.
- **Context and Implications:** A News Director or Shooting Staff member needs to durably insert production planning metadata into story assignments so that all crew members can work smoothly on show creation. Furthermore, technical staff contact details (company name, contact person) may be included to allow for the verification of issues with source material at later stages. This requirement effectively bridges the gap between organizational planning and physical acquisition.

6.1.4 Offline Metadata Generation and Synchronization

Provenance systems must support the creation of metadata in environments with no network connectivity. This "offline" metadata must be capable of secure synchronization with organizational trust lists and metadata management systems once connectivity is restored.

- **Associated Story Numbers:** 018.
- **Context and Implications:** Journalists in conflict zones or remote locations often lack access to the internet. The system must capture device signatures and metadata locally, ensuring the chain of trust remains intact even if the file is not transmitted until hours or days later.

Additional comments from SG:

Some consumer cameras allow for pre-requisition of CPA credentials for later use which need to be synchronized at a later point if network connectivity is not available. This may be a point-to-point network between two devices used to combine metadata. Some CPA specifications allow for augmenting of metadata at a later point if network connectivity is temporally not available. Contributors in content creation may believe they are synchronized while they are actually out-of-sync. These contributors need to be synchronized at a later point (post-sync). Furthermore, the local (wristwatch) time for a contributor may be different to Studio time, System time, Wall-clock time, UTC, etc. requiring a re-sync. Such sync changes need to be recorded in content metadata along with the identity of the contributor who made the sync change.

See: subclause 6.1.1 and 6.6.1 for additional comments and use cases concerning journalist safety in conflict/war zones, etc.

6.2 Post-Production, Editorial, and AI Workflow Requirements

Once an asset enters the post-production phase, the functional requirements shift toward managing "ingredients" and documenting the transformations applied by editors and AI tools.

6.2.1 Management of Ingredient and Derivative Relationships

The system must document the parent/child relationships between primary and derivative files. This includes maintaining the "ingredient" metadata of every asset used in a composition, ensuring that the history of every sub-component remains traceable.

- **Associated Story Numbers:** 004, 026, 043, Vendor-9.

© SMPTE 2026 – All Rights Reserved

- **Context and Implications:** A Repository Manager or Video Editor needs to maintain complete object entities as defined by library standards to ensure long-term preservation. In a VFX-heavy shot, it is vital to have markers pointing back to every single asset used in generating that shot, including proxy and editorial media. This prevents "provenance loss" during complex layering where multiple sources are merged into a single output.

Additional comments from SG:

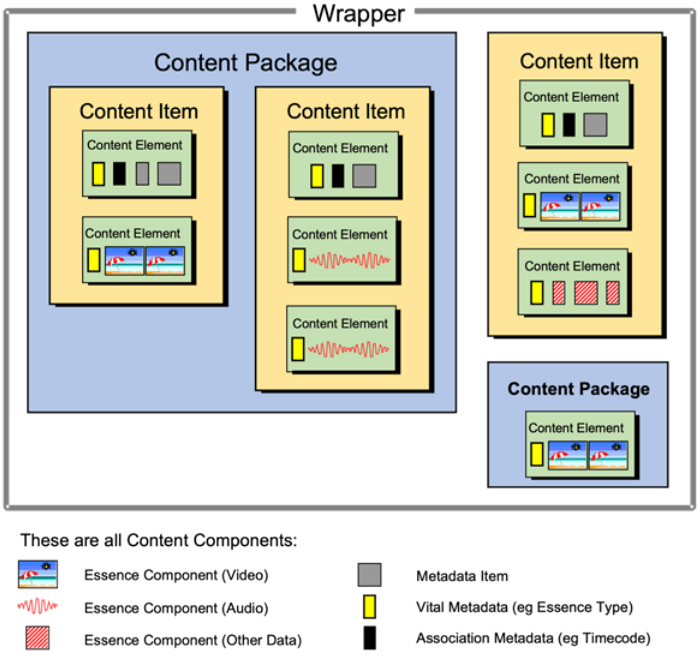
The word "ingredient" is a specific term used by C2PA. In the C2PA Implementation Guidance (version 2.4) Ingredients are defined as follows:

3.3. Ingredients

Ingredients are key to the establishment of the provenance of an asset, by serving as a listing of what other assets went into the creation of the current asset. Each ingredient that is used can itself contain its provenance, thus creating a rich provenance for the current asset and all of its ingredients.

Each ingredient can either be documented as the parentOf the current asset, a componentOf that asset, or as inputTo the creation of an asset. The value of parentOf is used in the common case where one asset is opened in an editing application, modified, and then saved or exported as another asset. That original version is the parentOf the final (now current) asset. Alternatively, when one asset is created from a series of other assets (such as audio and video clips), those sources are identified as componentOf ingredients. inputTo ingredients are used when describing information that was provided to a generative AI model, such as a prompt or seed image.

This contrasts in SMPTE with the somewhat similar terms "Content Item", "Picture Elements", "Content Packages", "Items", "Elements" etc. The C2PA term "Ingredients" might not correspond completely to a particular term listed above.



013

© SMPTE 2026 – All Rights Reserved

6.2.2 Mandatory Disclosure of AI and Generative Tools

The system must explicitly document and communicate when AI-enabled tools were used to generate content (e.g., text-to-video), modify images, or extract discovery metadata (e.g., name and place extraction).

- **Associated Story Numbers:** 006, 022, 030, 035, 037, 049, Vendor-9.
- **Context and Implications:** A Digital Archivist or News Manager needs to understand which tools were used for transparency, trust, and traceability. Viewers increasingly demand to know when subtitles, audio, or visual elements have been generated by AI. In the context of "Misinformation and disinformation," identifying whether a video depicts real life or is an AI rendering that mimics real life is a critical factor in consumer decision-making.

Additional comments from SG:

The C2PA specification already provides mechanisms for the recording of AI tools and the particular non-editorial AI enhancements to video or audio. These are features which are mandatory for media technology professionals.

6.2.3 Signing of Editorial Operations and Accountability

Editors must have the ability to insert their own digital signature into the CPA metadata, thereby taking responsibility for the editing results and proving that the clip has not been tampered with after the edit.

- **Associated Story Numbers:** 023, 024, 028, Vendor-4, Vendor-9.
- **Context and Implications:** A Video Editor or On-site Editor needs to inherit original provenance information, add new provenance reflecting their changes, and re-sign the output file. This creates a "chain of accountability" where every person who touches the content is cryptographically recorded as an actor in its history.

Additional comments from SG:

This requirement does not only apply to editors but also applies to every function in a media workflow such as VFX operator, Master Control, Audio Mixer etc. Each content change needs to be traceable in a chain of trust.

It may be required to modify content to meet broadcast standards and practices, for example obfuscation of nudity, bleeping strong language, or removal of product placement, or changing program duration for station format. Each such change needs to be recorded in the CPA metadata, and thus be traceable.

6.2.4 Inclusion of Usage Rights and Consent Metadata

The system must support the insertion of metadata defining the authorized scope of use, contributor consent, and rights evidence to streamline legal and editorial checks downstream.

- **Associated Story Numbers:** 016, 017, 019, 054.
- **Context and Implications:** A News Desk Editor wishes to insert contributor consent and risk flags to minimize manual checks by editorial staff. Post-production editors want downstream

© SMPTE 2026 – All Rights Reserved

users to be aware of usage restrictions based on the source material's provenance. This is essential for preventing the illegal use of AI-generated content or copyright-protected material.

Additional comments from SG:

This requirement is mandatory for content users. While this is an overlap with Digital Rights Management (DRM) it is helpful to have a flag indicating the right of use and consent. DRM and Content Provenance are going hand-in-hand, and this should be further discussed elsewhere.

6.3 Distribution, Packaging, and Real-Time Workflow Requirements

As content moves toward delivery, the requirements focus on maintaining the provenance chain across diverse platforms and in high-velocity live environments.

6.3.1 Shot-by-Shot Granularity in Live Streaming

For live sports and news workflows, the system must support the package, sign, and transmission of provenance metadata at a per-shot level of granularity in real time.

- **Associated Story Numbers:** 008, 042.
- **Context and Implications:** A Software Development Company building dynamic packagers requires the ability to achieve real-time authenticity for live streaming where trust in every individual shot is critical. An OB (Outside Broadcast) engineer needs the outgoing feed to securely contain both the host broadcaster's provenance and their own provenance at a shot-by-shot level as the program switches between sources.

Additional comments from SG:

This functional requirement specifically addresses outside broadcast being streamed live and OnDemand live streaming. There may be no value or opportunity to add frame-by-frame provenance metadata in live streaming from an OB truck. Shot-by-shot provenance insertion in the camera can be a regulatory requirement. For example, recently passed state and soon federal regulation in the USA and in Europe. The integrity hashing of the content can optionally still be performed frame-by-frame and folded into that per-shot signature, so the signature covers every frame, and tampering inside a shot remains detectable. Incremental hashing keeps this within live latency limits.

Ideal scenario:

Provenance is bound once per shot, not once per frame. *A provenance assertion names the accountable source of a segment and attests to its authenticity. That value changes only when the source changes. Within a single shot, the source and signer are constant, so per-frame provenance would repeat one attribution at added cost, with no added meaning. Shot-by-shot provenance insertion at the camera should be a requirement.*

The content is still checked frame-by-frame for tampering, folded into that one signature. *Integrity hashing of the content may be performed per frame and folded into the per-shot signature. When performed, the signature covers every frame, and tampering inside a shot remains detectable. Signing the shot boundary alone leaves the interior unprotected: a frame swapped or inserted mid-shot would still verify. Incremental hashing, computed as frames arrive, keeps the process within live latency.*

© SMPTE 2026 – All Rights Reserved

The signature has to say who is responsible. *The signature is attributable to a named accountable party, distinct from the device or software. A passed-through shot carries both the originating host broadcaster and the retransmitting broadcaster. An own-source shot carries the transmitting broadcaster alone.*

We are not asking the system to figure out when a shot changes. The switcher already knows. *No shot-boundary detection is required in the live feed. Shot boundaries are declared. The switcher already reports each cut and its source, and the provenance layer consumes that signal.*

Finding the exact altered frame can wait until later. Catching that a shot was altered cannot. *Locating the specific altered frame is deferred downstream. A per-shot signature shows that a shot was altered, without necessarily identifying which frame. Frame-level localization is a forensic capability for a mezzanine or archive pass, addressed by the frame-accurate binding work in SMPTE or by others, and is not required in the live feed.*

6.3.2 Interoperability Across Mezzanine and Distribution Formats

The system must ensure that provenance metadata maintains interoperability when content is converted from professional formats like MXF to distribution formats like MP4 or fMP4.

- **Associated Story Numbers:** 013, 034, Vendor-5, Vendor-9.
- **Context and Implications:** Broadcasters currently face a gap where CPA is adopted for MP4, but provenance is lost during conversion with MXF. For advertising and commercial content, it is required that provenance information survives the transition from the mezzanine file to the consumer-facing MP4 so viewers can verify authenticity.

Additional comments from SG:

A conversion may leave the essence data unchanged or alter it, and the two cases are handled differently.

Where a file is rewrapped and the essence data is unchanged, for example a change of container without transcoding, the content hash computed over the essence data remains valid and may be reused. The provenance of the original is carried forward and re-attached to the new asset.

Where the essence data is re-encoded, for example compression or transcoding, the hash over the original essence data no longer matches the new essence data. The new asset therefore carries two things: a new hash computed over the re-encoded essence data, and a signed reference to the original's provenance metadata and hash. The original lineage is preserved by reference, since a hash of the changed essence data can no longer match the original.

In either case the conversion is recorded as a provenance event that identifies when and where the encoding occurred and the party that performed it.

This applies to all content modifications.

© SMPTE 2026 – All Rights Reserved

6.3.3 Verification of Incomplete or Broken Trust Chains

Dynamic packagers and distribution systems must have the ability to ingest and verify CPA metadata before packaging and to detect if a trust chain has been broken or partially obscured. However, today no standard exists that clearly defines how a dynamic packager should obtain, verify, and embed CPA metadata, certificates, and signatures, especially in live and shot-by-shot workflows.

- **Associated Story Numbers:** 007, 010.
- **Context and Implications:** A Dynamic Packager delivering content to broadcasters and OTT platforms risks inserting unverified metadata if they cannot access the full metadata. This risk is heightened by proposals that "deliberately break the provenance chain for privacy reasons". The system must distinguish between an intact chain and a broken one to prevent broadcaster liability.

Additional comments from SG:

Redaction and a broken chain are distinct cases. In a recorded redaction, a named party removes sensitive content and the removal is itself recorded as a provenance event. The chain remains intact and auditable while the sensitive content is protected, which is the case for a journalist protecting a confidential source. In a broken chain, no record is present and no party is named, and a verifier cannot distinguish a protective removal from an unauthorized one.

The best practice for dynamic packagers is therefore the detection of unrecorded gaps rather than the detection of removals as such. This is consistent with the treatment of soft-binding lifecycle events in subclause 9.8, where a change to a soft binding should be recorded as a provenance event identifying the party that performed it and the time of the action.

Because provenance is relied upon after delivery, including for archival purposes, such records should remain resolvable for the archival life of the asset rather than only at the moment of packaging.

See: subclause 6.5.1 and Bucket D for additional comments and use cases dealing with certificates and Certificate Authorities.

6.3.4 Platform Independence for Delivery

Content provenance must be distributed independently of the platform, ensuring that the consumer receives the material without alteration regardless of whether it is consumed on a streaming site, social media, or a personal distribution platform.

- **Associated Story Numbers:** 002.
- **Context and Implications:** Broadcasters want to ensure their "content comes from me," independently of the third-party intermediary, to maintain brand integrity and audience trust.

Additional comments from SG:

Alteration of content and survival of provenance are two different concerns. One is whether the content itself is modified. The other is whether provenance survives.

© SMPTE 2026 – All Rights Reserved

Content is transcoded and repackaged many times between acquisition and consumption, and embedded provenance may not survive (Story 030). The requirement is that provenance remain verifiable and resolvable by the receiving party after these transformations, rather than that content pass through intermediaries unaltered.

No single binding survives every transformation. A content hash breaks on any transcode. A watermark survives transcoding but not regeneration. An embedded reference survives transcoding but is lost when metadata is stripped. Provenance therefore survives by being re-established at each transformation, as described in subclause 6.3.2: the original provenance is carried forward and new signed metadata records the operation, the responsible party, and the time (see subclause 9.9). A vendor survey response states the same requirement: generate, sign, and embed new provenance metadata inheriting the original when transcoding. A recorded transformation is then distinguishable from an unrecorded gap (see subclause 6.3.3).

Within professional pipelines, the transforming parties cooperate so that re-establishment of provenance history can be verified. At delivery, several jurisdictions now require platforms to detect and preserve provenance and to make it available for inspection (see subclause 9.9). Provenance should therefore remain resolvable independently of the delivery platform.

6.4 Ingest, Categorization, and Real-Time Verification Requirements

At the receiving end, be it a newsroom ingest server or a master control room, the focus is on analyzing the incoming signal to determine its reliability.

6.4.1 Real-Time Ingest Verification

Master control and ingest systems must have the ability to verify the provenance of incoming feeds and storage media (e.g., SD cards from the field) in real time.

- **Associated Story Numbers:** 033, 055, DMS-II-3, Vendor-3, Vendor-7.

- **Context and Implications:** Context and Implications: A content recipient, such as a Master Control Engineer, needs to confirm the provenance of incoming footage, especially from end users, which is currently "both critical and difficult". Ingest staff require tools that can warn of inconsistencies or unexpected data corruption in provenance information before the file is distributed to production staff. These inconsistencies or unexpected data corruption in provenance information could be due to accidental corruption or due to tampering.

Additional comments from SG:

Accidental corruption and tampering cannot be distinguished from the asset alone. The asset is compared against the recorded lifecycle of its provenance: a change recorded with a responsible party and time (see subclause 6.3.2, 6.3.3, 9.9) is a documented change, and an unrecorded gap indicates loss or tampering requiring review. Because verification occurs at ingest in real time, these records must be resolvable at the time of verification, rather than only at the time of packaging.

© SMPTE 2026 – All Rights Reserved

6.4.2 Automated Categorization Based on Provenance Metadata

The system must provide the ability to automatically categorize source materials (video, audio, text) based on their metadata assertions—specifically identifying camera-original footage, AI-generated content, or tampered media.

- **Associated Story Numbers:** 030.
- **Context and Implications:** A Media Coordinator collecting material from audiences and news agencies needs to verify materials before assigning them to editors to ensure only authorized, authentic clips are used in news production.

Additional comments from SG:

This functional requirement is closely related to subclause 6.4.1, but is distinct because it addresses the categorization of tampered content. Such categorization could support analysis and measurement where appropriate metrics are available. A separate effort should be considered to discuss the topic and to develop a suitable classification system.

6.4.3 Detection of AI Manipulation in External Content

The system must include functionality to analyze externally collected content that may lack CPA metadata to estimate whether it is AI-generated or has areas potentially altered by AI.

- **Associated Story Numbers:** 037, 038.
- **Context and Implications:** As AI-generating tools evolve, it is increasingly difficult for human operators to distinguish real from fake. Broadcast engineers need automated tools to analyze User Generated Content (UGC) and trailers created as "mashups" of legitimate and illegitimate content.

Additional comments from SG:

Looking at content alone to decide whether AI made it does not work well, and it works less well every year as the models improve.

A detector only gives an estimate, and answers are not certain. It is wrong in both directions, and an estimate no one can reproduce or stand behind is a challenge to use in news, in court, or in a rights dispute.

So this capability should route material for human review. It should not decide whether something is authentic.

(Milliman's 2025 study of AI fraud in motor insurance tested 925 people on real versus AI-generated damage photos. The average score was 46.4%, worse than a coin flip. Some AI images fooled 77% of viewers. Milliman's own summary puts human detection at 50% accurate and notes that even highly trained experts struggle.)

When content arrives with no record, the honest statement is that its origin cannot be established. Say unknown. Do not guess. The durable answer is a record that travels with the content.

© SMPTE 2026 – All Rights Reserved

6.5 Archival Integrity and Long-Term Stewardship Requirements

Archival workflows present unique challenges regarding the preservation of cryptographic trust over time.

6.5.1 Validation of Expired Certificates and Re-Signing

The system must provide a mechanism to validate provenance information even when original certificates have expired and to re-sign the content against a modern, trusted Certificate Authority (CA) for long-term archival integrity.

- **Associated Story Numbers:** 009, 029.
- **Context and Implications:** Archives Repackagers require clear rules on how to handle expired claims when redistributing historical content decades after its creation. An Archive Manager needs to verify original provenance and add new, signed provenance as content is converted for long-term storage.

Additional comments from SG:

See: subclause 6.3.3 and Bucket D for additional comments and use cases dealing with certificates and Certificate Authorities.

6.5.2 Alignment with Preservation Metadata Standards (Library Standards)

Provenance data must be capable of documenting the statute, rule, or stewardship events that explain why content was changed or redacted, ensuring that researchers can understand the relationship between a redacted derivative and the original.

- **Associated Story Numbers:** 005, DMS-II-11, Vendor-12.
- **Context and Implications:** For sensitive records (e.g., 9/11 Commission), a CPA specification must document *why* a redaction happened to maintain transparency. Archivists need produced packages and b-roll to be tagged with unique identifiers that aid in storage, retention, and retrieval within a CMS that keeps a record of all provenance changes.

Additional comments from SG:

While some CPA systems (e.g. C2PA) currently limited adding additional metadata items, other systems (e.g. CAWG, JPEG Trust) do allow it.

6.5.3 Embedding Provenance in Digital Birth Workflows for Analog Media

The system must support the creation of CPA metadata during the digitization of analog masters to establish an authoritative record of unaltered content from the point of its digital inception.

- **Associated Story Numbers:** 003.
- **Context and Implications:** Audio digitization technicians at Libraries wish to embed metadata into the CPA custom chunk of a Broadcast Wave file to establish provenance for digitized magnetic tape.

Additional comments from SG:

© SMPTE 2026 – All Rights Reserved

Libraries have already published guidelines on CPA for digitized tapes (e.g. https://www.digitizationguidelines.gov/guidelines/tcr4cap/FADGI-TCR4CAP-v02-PublicCommentDraft.pdf).

6.6 Privacy, Redaction, and Identity Management Requirements

The requirement for transparency must be balanced against the need for privacy and the protection of sensitive sources.

6.6.1 Selective Redaction of Metadata for Source Protection

The system must allow for the redaction of specific metadata fields—such as precise location or identity—to protect journalists in conflict zones or sources whose personal information must be shielded.

- **Associated Story Numbers:** 005, 021, 023, 024, 045, 056.
- **Context and Implications:** Public service providers need to protect sources in war regions. Editors need to remove or redact the signatures of individual editors to protect personal information before the content is distributed to the public. In conflict zones, removing or redacting specific provenance metadata is vital to prevent vulnerable subjects from being put at risk of harm.

Additional comments from SG:

See: subclause 6.1.1 and 6.1.4 for additional comments and use cases concerning journalist safety in conflict/war zones, etc.

6.6.2 Institutional "Vouching" and Trust Anchors

The system must support an "Override" or "Institutional Stamp" model where a trusted organization (e.g., a Broadcaster) can vouch for the provenance of a source when that source's metadata is missing or broken.

- **Associated Story Numbers:** 010, 047.
- **Context and Implications:** An MCR (Master Control Room) engineer may need to vouch for metadata when an important source lacks it, ensuring that consumers can continue to verify the media based on the broadcaster's reputation. This addresses the risk of "chain breaks" in privacy-driven workflows.

Additional comments from SG:

A mechanism is required to un-vouch the already vouched content if it is found inappropriate at a later stage.

6.6.3 Differentiation of Actor Identity Levels

Identity assertions should clearly differentiate between verified organizational identities (e.g., backed by a CA) and self-declared or unverified information.

- **Associated Story Numbers:** 048.

© SMPTE 2026 – All Rights Reserved

- **Context and Implications:** Users must be able to verify both the authenticity of the creator and the integrity of the composition through validation of the signature. This requires a hierarchy of trust signals within the user interface.

Additional comments from SG:

SMPTE CPA must identify each participating party in a production and post-production chain and bind it to the specific point at which it handled the asset, in a signed assertion attributable to that party, distinct from the software or device that produced the underlying CPA metadata. The term organizational identities is not sufficient to cover everyone who may be backed by a Certificate Authority (CA). It may boil down to one natural or fictional person.

Additional user story from SG: *A movie file goes from the studio to a visual effects company, to a sound company, to a subtitling company, in four different countries. At each stop, CPA metadata proves a piece of software touched the file. What it does not cleanly prove is which company was responsible at each stop, in a way that holds up later.*

Right now, the record says, "software X touched this, software Y touched this." It does not firmly say "A VFX Company was the accountable party here, and a vendor in Bulgaria was the accountable party there."

The tools are identified through their assertions. The accountable companies are not, at least not in a strong, standardized, signed form and connected to the asset.

With assets now arriving from anywhere, with AI-generated elements, labeling laws, and digital replica consent laws, that gap carries real liability.

6.7 Binding Mechanisms, Watermarking, and Resilience Requirements

Metadata is fragile and can be stripped by non-compliant tools or social media platforms. Functional requirements for resilience focus on "soft-binding" mechanisms.

6.7.1 Soft-Binding via Invisible Watermarking

The system must support the embedding of invisible watermarks during content creation or modification. These watermarks must act as a soft-binding to the CPA metadata, allowing for provenance metadata recovery even if the CPA metadata is stripped or the media is no longer in the professional container (e.g. MXF).

- **Associated Story Numbers:** 013, 014.
- **Context and Implications:** Media processors need to retrieve provenance when media is no longer in an MXF container. Cloud services can then use the detected watermark to recover canonical asset metadata and their associated provenance history.

Additional comments from SG:

© SMPTE 2026 – All Rights Reserved

Some information should not be bound to the asset, such as consent, terms that may change after release, or personal information. The watermark may point to that information at a registry. The watermark itself should carry only an identifier.

The watermark should survive common transformations, such as transcoding, scaling, and compression.

Metadata recovered through a watermark should be checked against the content before it is trusted, because a watermark can be copied onto other content.

When content is modified, the watermark should resolve the current provenance record, which links to earlier records.

A fingerprint can serve the same purpose for content that was never watermarked.

6.7.2 Frame/Track Level Integrity Checksums

For high-end production, the system must provide frame-level or track-level check-summing within the media to allow for the verification of specific segments of picture or sound, rather than just the file as a whole.

- **Associated Story Numbers:** 027.
- **Context and Implications:** A person in charge of ensuring an unbroken chain of custody for feature film footage requires embedded checksums to replace non-embedded sidecar methods that are easily lost or tampered with.

Additional comments from SG:

See subclause 6.9.7 and 6.9.3 for additional information.

6.7.3 Resilience Against "Metadata Washing"

The system must maintain provenance attached to the content through multiple video processing steps, even when passed over untrusted transports or through tools that do not natively support industry protocols.

- **Associated Story Numbers:** 041.
- **Context and Implications:** A Journalist in the field needs metadata to remain secure and attached through the entire newsroom workflow to ensure the final product can be verified as authentic.

Additional comments from SG:

This is a hardware and software issue which may only be solved by vendors of such products and solutions. There are already many e.g. watermarking solutions available on the market. This may also need to be addressed through legislation.

© SMPTE 2026 – All Rights Reserved

6.8 User Experience and Consumer Trust Signaling Requirements

The ultimate consumer must be able to interpret provenance data without being overwhelmed by technical complexity.

6.8.1 Implementation of Progressive Disclosure (Levels 1-4)

Consumer-facing interfaces must support at least four levels of progressive disclosure: Level 1 (Presence indicator), Level 2 (Summary), Level 3 (Full detail), and Level 4 (Forensic view).

- **Associated Story Numbers:** 020, Vendor-13.
- **Context and Implications:** Web editors need to embed provenance badges so audiences have a clear verification path. Viewers watching distributed programs need to access verification levels that help them understand the content's history without needing to be forensic experts.

6.8.2 Integration of Provenance in Media Management Systems

MAM (Media Asset Management) and CMS (Content Management System) platforms must allow for the import of provenance information and verification results, expanding them into internal metadata fields for easy traceability.

- **Associated Story Numbers:** 028, 029, Vendor-8.
- **Context and Implications:** An Editor or Archive Manager needs to specify provenance as a search condition or trace provenance to search for original files. Maintaining this within the MAM enables easy traceability if legal or authenticity issues arise years later.

6.9 CPA Metadata for Material Exchange Format (MXF)

6.9.1 Introduction

Material Exchange Format (MXF) is a foundational container for professional media workflows and therefore requires a standards-based approach for carrying content provenance and authenticity (CPA) metadata. The requirements in this subclause reflect contributions from the DMS-II Drafting Group, and identify the capabilities needed to integrate CPA metadata into the existing MXF ecosystem without disrupting established implementations. They address backward compatibility, frame-accurate association, multi-step editing, equivalent representation across KLV, XML, and JSON, near-term and comprehensive carriage mechanisms, essence binding, contributor identity, and cryptographic agility.

6.9.2 No MXF Revision

The professional media industry does not desire and will not accept revision of SMPTE ST 377-1:2019. Addition of CPA capabilities to the MXF ecosystem must be accomplished by addition of a new SMPTE ST 377-1 compliant Descriptive Metadata Schemes (herein called SMPTE CPA Metadata). Existing compliant MXF implementations conform to MXF DMS and will carry such metadata.

© SMPTE 2026 – All Rights Reserved

6.9.3 Frame Accuracy

The professional media ecosystem demands frame- and sample-accuracy at integer and fractional frame rates, especially 30000/1001 and 24000/1001. These can only be delivered via timescales that are calculated as a rational fraction of a second.

6.9.4 Multi-Step Editing

Professional media workflows require multiple steps of editing and metadata augmentation that will, in most cases, modify the MXF file essences, structural and descriptive metadata, and might invalidate the SMPTE CPA Metadata. In such cases, it must be easy to remove or update an outdated CPA Metadata. When a new CPA Metadata is generated, it must correspond to the changed essences, structural and descriptive metadata in the new MXF files.

6.9.5 KLV, RegXML and JSON Compliance

The professional media ecosystem will carry CPA metadata both in the form of MXF KLV and separately, today usually as XML and increasingly as JSON. The CPA Metadata structure, values and timing must be equivalent whatever format is used. Carriage of the CPA Metadata within MXF files must be compliant with ST336:2017 KLV .

Carriage of the CPA Metadata in XML must be compliant with ST2001 RegXML.

Carriage of the CPA Metadata in JSON requires a specification with equivalent capability.

6.9.6 Immediate Solution

It is recognized that the full KLV-based DMS-II standardization will take some time, thus there is a need for a simple immediate solution (this is being developed as ST2140-3 JUMBF Framework). It is imperative that ST2140-3 JUMBF Framework and ST2140-2 KLV Framework do not provide separate solutions for individual functional requirements.

6.9.7 Whole File CPA Metadata

Common workflow steps include creation of a whole MXF file from camera input or other ingest, and distribution of a whole MXF file, with or without rewrapping. In these cases, it is not necessary to access metadata frame by frame, and the SMPTE CPA Metadata can be provided for the whole file without reference to timing. ST 2140-3 JUMBF Framework should address such cases for its early adoption in the industry.

6.9.8 Diverse CPA Metadata for Diverse MXF Applications

MXF-based content includes media structures with multiple Tracks, multiple Packages, Framewrapped, Clipwrapped and Partitioned files, and multiple essence streams including I frame and long GOP video media, and interleaved or separate audio and data essence. The ST 2140-2 KLV Framework should address such cases; thus ST2140-3 JUMBF Framework does not need to.

© SMPTE 2026 – All Rights Reserved

6.9.9 Whole File Hashes and Itemized Essence Hashes

Many workflow steps will extract essence data from MXF files, or will insert essence data into MXF files, or will rewrap essence data to or from a non MXF wrapper; and these operations will likely be performed frame by frame. It must be possible to verify essence data hashes in all these cases without recalculation between different formats when the essence data remains unchanged. These capabilities are being developed as ST2140-4 KLV Bindings. This specification for bindings should address MXF media structures with Framewrapped, Clipwrapped and Partitioned files, multiple essence streams including I frame and long GOP media, interleaved or separate audio and data essence, and the same essence data when stored in non MXF formats.

6.9.10 Contributor Identity Inclusion

Contributor Identity must be incorporated into the CPA Metadata, and specified using standard or registered identity formats (this is being developed as SMPTE ST 2140-5 Contributor Identity). SMPTE-RA already provides some (e.g. EIDR) and can provide more (e.g. HAND). Other standards and registration authorities will also be used.

6.9.11 CPA Metadata Security

In light of continuously evolving IT security risks, CPA metadata must be designed for cryptographic agility to accommodate future threat landscape changes by taking account of the existing best practices. agility is much more important than the use of the “fixed” technology even if it is the latest one at its development stage. Governance of choice of cryptographic technology can be provided by existing registration authorities including SMPTE.

7 Potential Requirement Gaps

7.1 Existing Requirements from other organizations (JPEG Trust, C2PA, CAWG)

JPEG Trust standard and the C2PA as well as CAWG specifications set the framework for discussions by the SG. JPEG Trust provides a framework for assessing whether media can be trusted. C2PA defines how to record and sign the history of an asset and check it later. CAWG extends C2PA with assertions for who is involved, for descriptive metadata about the asset, and for consent to use of an asset or a human’s likeness and voice.

JPEG Trust (ISO/IEC 21617):

- A way to state and check whether media is authentic, built to be compatible with C2PA.
- Trust profiles: a set of conditions against which an asset is tested, producing a trust report for a specific use.
- Room for industry stakeholders to define the conditions that matter to them.

C2PA:

A conforming implementation must:

- Attach or embed a sealed record of the asset’s history that lists what was done.

© SMPTE 2026 – All Rights Reserved

- Bind that record to the content. A cryptographic hash of the content ("hard binding") is required. A watermark or a fingerprint ("soft binding") is optional and lets the record be found again if the file is re-encoded or the metadata is stripped. Sign each record, so anyone can check who made the claim and that nothing was altered.

- Support way to decide whether to trust the signer, such as a trust list.

- Keep the history add-only. A change to the asset adds a new record, and any modification to an earlier record leaves evidence.

CAWG (Creator Assertions Working Group):

CAWG assertions fill three gaps that C2PA leaves open:

- *Identity.* Names the people and organizations tied to the asset so that the record can say “who” as well as “what”. Each identity assertion sits inside the C2PA record and is signed with that party’s own credential or that of a trust registry.

- *Metadata.* The CAWG metadata assertion can carry a standard identifier for the asset, such as an EIDR ID for film and television, or an ISWC or ISRC for music. CAWG leaves open which identifier to use and where it goes.

- *Consent.* Carries a signed, machine-readable pointer from the asset to wherever the consent terms are held and permissions actually live. It keeps consent about a person separate from consent about the work, and it ties consent to a named participant.

Where all this points. Across these specifications, identity appears at two levels. The first is the identity of whoever made and/or signed the asset, C2PA and the CAWG identity work already handle this. Today, they are used mostly by organizations, and the same mechanisms extend to individuals as trust infrastructure matures. The second is the identity of the actual entities people (subjects) in the asset, the ones the people to whom consent and rights attach. That second level needs one shared, checkable way to identify participants. The current specifications point toward it and stop short. Subclause 6.2 and 6.3 and the participant-identity requirements name that shared structure as a requirement.

7.2 Unique Requirements identified by the SMPTE Study Group

This clause summarizes requirements for CPA systems for professional media uniquely identified by SG.

7.2.1 Acquisition and Creation

- Define how an acquisition system’s secure element interacts with the file system (MXF/MP4) to write provenance metadata with minimum latency (subclause 5.4, Bucket A).

- Define how a camera or recorder’s secure signing element interacts with media file systems and attaches provenance information with minimal acquisition latency (subclause 6.3.1 and 6.3.4).

- A standardized protocol for pushing planning metadata (such as Assignment IDs, Story IDs, and Production identifiers) into the acquisition system’s trusted signing environment (subclause 5.4, Bucket A).

- Support the creation of metadata in environments with no network connectivity (subclause 6.1.4).

 © SMPTE 2026 – All Rights Reserved

- "Offline" metadata to be capable of secure synchronization with organizational trust lists and metadata management systems once connectivity is restored (subclause 6.1.4).

7.2.2 Production, editing and transformation

- Preserve hashes where the essence is unchanged (clause 5.4, Bucket B).
- Where the essence is transformed, for example, by transcoding or color grading, the transformation is recorded in signed metadata identifying the operation and the trusted party that performed it (subclause 6.3.2).
- A system is able to extract portions of the source CPA metadata and compose them into the final product (subclause 5.4, Bucket B).
- For live sports and news workflows, support the packaging, signing, and transmission of provenance metadata at a per-shot level of granularity in real time (subclause 6.3.1).
- CPA metadata to support embedded integrity verification at the frame level, audio track level, and segment level (subclause 6.3.1 and 6.7.2).
- Provide provenance to utilize shot-boundary information generated by the production switcher (sub clause 6.3.1).

7.2.3 Distribution, packaging and interoperability

- Define how CPA metadata maps between MXF (KLV) and ISO BMFF (Boxes) and other transport formats such as MPEG-TS (subclause 5.4, Bucket C and subclause 6.3.2).
- Soft Binding (Watermarking) is a critical fail-safe for when metadata is stripped (subclause 5.4, Bucket C).
- Define how dynamic packagers obtain, verify, embed, and transmit provenance, certificates, and signatures during packaging (subclause 6.3.3).

7.2.4 Ingest, Categorization, and Real-Time Verification

- Support for master-control and ingest systems to verify provenance in real time upon arrival of live feeds, SD cards, contribution feeds, or incoming media (subclause 6.4.1).
- CPA systems to automatically classify incoming content as camera original, AI generated, or tampered based on provenance media assertions (subclause 6.4.2).
- Signing during packaging (subclause 6.3.3).

7.2.5 Archiving and long-term preservation

- For archived media, support validation of expired certificates, re-signing under current trusted authorities, and long-term archival trust maintenance (subclause 6.5.1).
- Generate CPA metadata during the digitization of analogue holdings to establish the first authoritative digital provenance record (subclause 6.5.3).
- Define CPA metadata carriage for broadcast wave format (BWF or RIFF chunks), beside other formats (subclause 5.4, Bucket D).

© SMPTE 2026 – All Rights Reserved

7.2.6 Privacy, Redaction, and Identity Management

- Support for trusted organizations to be able to issue or redact provenance assertions or identity on behalf of sources that must be protected or whose provenance is missing or incomplete (vouching), with previously vouched content revocable if later determined inappropriate (un-vouching) (subclause 6.6.1 and 6.6.2).

- The CPA system must be capable of identifying the accountable organization/person at every workflow stage, separately from the software or device creating provenance (subclause 5.4, Bucket E, subclause 6.2.1 and 6.2.3).

- CPA metadata to support embedded integrity verification at the frame level, audio track level, and segment level (subclause 6.3.1 and 6.7.2).

7.2.7 Consumer Presentation

- CPA systems to facilitate standardized disclosure layers consisting of (a) a presence indicator, (b) summary, (c) detailed view, and (d) forensic view (subclause 6.8.1).

7.2.8 MXF Specific Requirements

The following requirements have been identified for CPA metadata (subclause 6.9):

- Do not change SMPTE ST 377-1,
- Support CPA metadata by adding descriptive metadata schemes,
- Support frame-accurate and sample-accurate provenance timing including support for fractional frame rates (e.g., 30000/1001, 24000/1001),
- Equivalence across KLV, RegXML, and JSON with equivalent semantics, structure, and timing,
- Support whole-file mode for provenance without time references where frame access is unnecessary,
- Support diverse MXF application structures (frame-wrapped, clip-wrapped, partitioned files, long-GOP, multi-track, multi-package structures),
- Support hash reuse across wrappers to enable verification when essence remains unchanged across wrapper migrations,
- Support standardized contributor identity integration including registered industry identity schemes (EIDR, HAND, etc.) within CPA metadata,
- Support cryptographic agility governance framework for algorithm replacement and future cryptographic migration.

8 Legal Requirements

The regulatory landscape changed materially during the study period. New obligations are emerging that fall into three families:

- Those attaching to content generally
- Those triggered by generative AI
- Those attaching to the persons depicted.

© SMPTE 2026 – All Rights Reserved

All three have an impact on professional media.

Content generally. California (SB 942 as amended by AB 853, phasing in through January 2028) requires large online platforms to retain any available provenance metadata in posted content and disclose its availability, and requires capture devices sold in the state to support provenance at capture. Pending amendments (SB 1000, AB 2713) would define compliance by reference to specifications from established standards-setting bodies and would cover provenance embedded into, attached to, or otherwise associated with content. These duties are not limited to AI content. They oblige platforms to preserve the provenance a media organization attaches to its own material.

AI generation. EU AI Act Article 50 (applicable 2 August 2026) requires providers of generative AI systems to mark outputs in a machine-readable format, with feasibility measured against relevant technical standards. Assistive editing tools that do not substantially alter the input are exempt, and disclosure for artistic works is limited to a manner that does not hamper enjoyment of the work. California's provider duties (operative the same day) require a latent disclosure carrying provider name, system and version, timestamp, and a unique identifier, consistent with widely accepted industry standards, plus a free detection tool. A provider that knows a licensee has disabled the disclosure capability must revoke the license within 96 hours. The chapter currently exempts services providing exclusively non-user-generated video game, television, streaming, or movie experiences; pending SB 1000 would narrow this exemption and bring entertainment services within scope. China's Labeling Measures and mandatory national standard GB 45438-2025 (in force 1 September 2025) require metadata labels, require platforms to verify labels and categorize content as confirmed, possible, or suspected AI-generated, prohibit label tampering, and require labels to survive format conversion. India's amended IT Rules (effective 20 February 2026) require intermediaries to label synthetic content, embed provenance where technically feasible, and never remove labels, with safe harbor conditioned on compliance.

Persons depicted. Deep fake disclosure (EU), removal of nonconsensual intimate imagery (US TAKE IT DOWN Act), and right-of-publicity and digital replica statutes apply regardless of production method, with the federal NO FAKES Act and California SB 1050 (synthetic performer disclosure in advertising) pending. Each turns on who is depicted and under what authorization. Where provenance carries that information, the obligations are administrable. Where it is absent, every downstream party must re-establish it independently.

Four elements recur: machine-readable marking at creation; platform duties to detect and preserve provenance; feasibility measured against the state of the art; and compliance defined by specifications from established standards bodies. The latter gives SMPTE specifications direct regulatory significance, because conformance is how media organizations are able to demonstrate compliance.

Recommendation:

The group recommends that regulatory compliance be treated as a driver of normative requirements in subsequent engineering documents, including provenance that remains resolvable across distribution and is re-established across transformations (see subclause 6.3.2 and 6.3.4), attribution of provenance lifecycle events (see subclause 9.9), and participant-level information sufficient to support obligations attaching to the depiction of persons.

© SMPTE 2026 – All Rights Reserved

9 Conclusions and Recommendations

9.1 Urgent Need

The survey received a large number of responses from individuals and organizations as well as from across all functions and parts of the professional and consumer media ecosystem. This signals that there is great interest in the topic of CPA and an urgent need in the industry to enable and deliver CPA solutions.

Recommendation:

- Prioritize the rapid development and deployment of CPA solutions to address the industry's clear and urgent demand,
- Foster collaboration across stakeholders in the media ecosystem to ensure broad adoption and interoperability of CPA implementations.

9.2 Terminology

The Study Group found that terminology is a material interoperability issue for content provenance and authenticity (CPA). Terms such as “tampered” and “illegal” prompted substantial discussion because they can carry different technical, legal, and operational meanings depending on the context. More specialized terms, including “essence”, “metadata” and “manifest,” are likewise not used consistently across media, security, and provenance communities. Ambiguous terminology can lead to inconsistent requirements, implementations, and verification outcomes.

Recommendation:

- SMPTE should establish or adopt a CPA-specific vocabulary with clear, context-appropriate definitions.

This work could be undertaken as a dedicated SMPTE effort or through a systematic review and harmonization of terminology already defined by organizations and initiatives such as ISO, JPEG, C2PA, and CAWG. Where established definitions are suitable, they should be reused; where conflict of definitions or gaps remain, SMPTE should document the distinctions and define the CPA terms needed for professional media workflows.

9.3 Legislative Requirements

Throughout its discussion of the functional requirements, the Study Group noted that established and emerging legislation will strongly influence the design, implementation, and operation of content provenance and authenticity (CPA) solutions. Legal requirements may affect, among other matters, disclosure of synthetic or materially altered content, preservation and presentation of provenance information, identification and accountability of responsible parties, protection of privacy and confidential sources, consent and rights information, accessibility of trust signals, and retention of auditable records. These requirements may differ among jurisdictions and may continue to evolve.

CPA standards cannot by themselves determine legal compliance, nor should they encode requirements that apply only in a single jurisdiction. They should, however, provide technically neutral and adaptable capabilities that enable implementers to meet applicable obligations. This includes support for verifiable disclosure, selective and accountable redaction, traceable transformations, interoperable identity and rights assertions, durable records, and cryptographic agility.

Recommendation:

© SMPTE 2026 – All Rights Reserved

- SMPTE and the industry at large should monitor relevant legislation and regulatory guidance and consider their technical implications in all further CPA work.

- Future SMPTE standards and recommended practices should be developed in consultation with legal, policy, privacy, security, accessibility, and operational stakeholders, while remaining jurisdiction-neutral and sufficiently extensible to accommodate evolving requirements.

- CPA implementations should clearly distinguish technical evidence and trust assertions from legal determinations, and should document which capabilities are provided to support compliance.

9.4 Holistic Solution

Participants in the survey come from all parts of the media ecosystem and work in roles across the industry. This means that any discussion about CPA needs to address the whole ecosystem of media from acquisition to postproduction, distribution and archiving. It needs to include not only considerations for professional media infrastructure but also for downstream service like online streaming, cable and broadcast. Any CPA solution needs to be a holistic solution.

Recommendation:

- CPA solutions should address the entire media lifecycle, from content acquisition and post-production through distribution and archiving, ensuring end-to-end interoperability,

- CPA implementations should consider the needs of all stakeholders across the media ecosystem, including professional media infrastructure as well as downstream services such as streaming, cable, and broadcast platforms.

9.5 Transparency

A reoccurring theme among survey responses is the need for systems to be temporally accurate and to preserve CPA metadata at every step of the media workflow. They voice a need for systems to be transparent to CPA metadata and to preserve it while content is being processed. This does not mean that no new metadata can be added to a metadata record to reflect the process the content went through.

Recommendation:

- All systems are capable of preserving existing CPA metadata throughout media processing workflows, maintaining temporal accuracy and end-to-end provenance integrity,

- CPA implementations are able to transparently carry forward existing metadata while allowing the addition of new metadata that accurately records each processing step and transformation.

9.6 Support for C2PA

Many survey responses mention the C2PA specifications as a solution for CPA in media, especially for images, audio, and data. This is supported by first implementations and PoCs shown at trade shows and industry events. C2PA is emerging as a foundational technology that is increasingly being implemented within the media industry. It is actively being developed and supported by major industry organizations. It appears that many see C2PA as the best current solution to address the need for CPA and trust in media.

© SMPTE 2026 – All Rights Reserved

Recommendation:

- Develop CPA solutions that include current C2PA capabilities to address emerging media-industry requirements, maintaining full compatibility with C2PA to ensure interoperability with existing deployments and workflows,
- CPA strategies should be aligned with emerging C2PA capabilities and standards to leverage industry momentum, promote interoperability, and strengthen trust in media content.

9.7 Support for professional media editing

C2PA is not yet claimed to be a complete solution to the requirements of professional media editing although there is ongoing discussion on what is needed. For example, frame-based treatment of media is critical in professional editing environments but less critical in finished products.

Recommendation:

- CPA capabilities should be extended beyond the current scope of C2PA to address professional media workflow requirements, particularly where fine-grained and frame-level provenance tracking is needed,
- CPA solutions should support both high-precision production environments and simplified distribution use cases, enabling appropriate provenance granularity throughout the media lifecycle while maintaining interoperability with C2PA.

9.8 Transparent MXF encapsulation and extraction

Many survey answers mention that any technical solutions need to fit into the existing MXF based media ecosystem seamlessly and need to be transparent. They recommend that CPA metadata in metadata records not be stripped from media content in processing steps or altered by downstream systems. They also suggest that at the same time legitimate processes need to add their process information to the CPA metadata so that subsequent consumers receive all needed information to ensure trust.

Recommendation:

- Design CPA solutions so as to integrate seamlessly into existing MXF based media workflows, ensuring that the CPA metadata is preserved and remains transparent throughout all processing and distribution stages,
- Trusted workflow participants should be able to append process-specific provenance information while maintaining the integrity of existing CPA metadata, ensuring that downstream consumers can receive a complete and trustworthy record of content history.
- SMPTE ST 377-1 should not be changed and descriptive metadata schemes should be used.

9.9 Soft-binding robustness and content

The survey findings and discussion in the group demonstrate a clear need for provenance information that remains verifiable, interoperable, and persistent across diverse media formats and workflows.

© SMPTE 2026 – All Rights Reserved

As media assets are routinely transformed, repackaged, and redistributed, soft binding (e.g. video and audio watermarks) provides an important mechanism for maintaining the connection between content and its provenance beyond the original container.

To ensure trust and validation capabilities, soft-bindings and the contained reference should be preserved as provenance information evolves. In some cases, maintaining the trust chain may require updating a soft binding to reference a new signed provenance record associated with a transformed asset.

Conversely, there may be legitimate reasons to remove or modify a soft binding, such as redacting information to protect journalists, confidential sources, or other sensitive parties. Where a soft binding is updated or removed, the change should be recorded as a provenance event identifying the party that performed it and the time of the action, so that a legitimate update or redaction can be distinguished from an unauthorized removal.

Recommendation:

- Further study of soft-binding lifecycle management, including type of reference (e.g. URN), preservation, updating, and controlled removal,
- Attribution of soft-binding lifecycle events be included in the further study noted above.

9.10 Classification of manipulated or tampered content

The survey raised not only the topic of detecting content that has been tampered with, but also highlighted the desirability of a classification system for such content. Such a system would provide a common framework for categorizing different types of manipulation, including content fabrication, alteration, contextual misuse, impersonation, and provenance metadata tampering.

By enabling tampered content to be consistently organized and analyzed, these categories would support the development of meaningful metrics, improve understanding of emerging attack patterns, and help guide the creation of more effective prevention, detection, and mitigation measures. Ultimately, a common classification framework could contribute to greater interoperability among authenticity and provenance solutions and support future standardization efforts in this area.

One example of an existing classification specification is available on the ProofGen website (https://proofgen.app/spectrum/spec/0.3/index.html). ANNEX C Example Categories for Tampered Content provides another example of such a classification system.

Recommendation:

- SMPTE to initiate a standards effort to develop an open and interoperable classification framework for manipulated and tampered media content.

9.11 Technology Limitation Consideration

The Study Group recognizes that CPA provenance metadata does not guarantee the truth of the depicted content. For example, a certified photo could be of a staged auto accident or a synthetically generated image. Human-based fact checking is still important.

Recommendation:

© SMPTE 2026 – All Rights Reserved

- Recognize that CPA technology cannot fully substitute for human involvement and human/organizational identity, which remain crucial for trust in media.

10 Acknowledgments

SMPTE thanks all SG members for their contributions, particularly those whose drafting efforts made this report possible. The list below identifies the main participants:

Thomas Bause Mason (SG Chair)	Robert Porter
Yoshiaki Shibata	Paul Treleaven
Paul Gardiner	Walt Husak
Satoshi Oode	Mohamed Badr Taddist
Andy Rosen	James Burns
Charles J. Flynn	Erik Passoja
Go Ohtake	Wolfgang Ruppel
Frederick G Walls	
Oliver Morgan	

© SMPTE 2026 – All Rights Reserved

ANNEX A User Stories

Story # (Bucket)	Role	Who	Context	Requirements - "I want…"	Challenges	Simplified Requirements	Tags (who)	Tags (where)
001 **(B)**	Trendscout & System Engineer	As a journalist	Working with ingested material want to know if fact checking has already been done	To know whether fact checking has been done		Verify provenance	Journalist	Ingest
002 **(C)**	Trendscout & System Engineer	As a broadcaster	I want to ensure that all my media I distribute receives the customer without alteration, that he/she can be sure that my content comes from me, independently of the platform (streaming, social media, personal distribution platforms).	[Platform independence]		Platform independence Maintain provenance	Broadcaster	Distribution
003 **(D)**	Preservation and archiving	As an audio digitization technician	I want to embed C2PA metadata within the C2PA custom chunk of a Broadcast Wave file as part of the digitization workflow of a ¼" inch magnetic tape to establish an authoritative record of unaltered content and document provenance and continuity.	Embed C2PA metadata within the C2PA custom chunk of a Broadcast Wave file as part of the digitization workflow of a ¼" inch magnetic tape to establish an authoritative record of unaltered content and document provenance and continuity.		Add provenance when digitizing analogue audio	Audio engineer	Archiving
004 **(D)**	Preservation and archiving	As a repository manager	I want to use C2PA to document the parent/child/other relationships between primary and derivative files as well as multi-part packages (such as in a DCP - Digital Cinema Package) in order to maintain complete object entities as defined by PREMIS.	Maintain complete object entities as defined by PREMIS.		Add provenance Maintain complete object entities as defined by PREMIS	Archivist Repository manager	Annotation

© SMPTE 2026 – All Rights Reserved

005 **(D)**	Preservation and archiving	As a custodial unit staff member	I want to apply C2PA to document the statute or rule that explains why content was redacted for sensitive records, such as those from the 9/11 Commission records, in order to demonstrate transparency to researchers regarding any changes made to the original record following their accession into the Center for Legislative Archives' custody. Redacting information from electronic records or other similar actions, changes the date/time stamp for that in the original unredacted file. This is a new instance of the content that is derived from the unredacted original and hopefully C2PA can help demonstrate that transparency of the relationship and how it came about and why it's needed.	document the statute or rule that explains why content was redacted for sensitive records, such as those from the 9/11 Commission records		Add provenance Redact provenance	Archivist	Annotation
006 **(D)**	Preservation and archiving	As a processing digital archivist	I want to use C2PA to document and communicate which tools, especially AI-enabled tools, were used to generate discovery metadata from the content (such as name and place value entity extraction) to support transparency, trust and traceability. This also will help document workflow processes and demonstrate the use and value of specific tools.	Document and communicate which tools, especially AI-enabled tools, were used to generate discovery metadata from the content (such as name and place value entity extraction).		Add provenance Identify AI tools	Archivist	Annotation

© SMPTE 2026 – All Rights Reserved

007 **(C)**	streaming solutions manager	As a Packager Provider	The following user stories reflect challenges faced by packager providers and software developers working at the final step of media delivery. As the point where content is encrypted, signed, watermarked, and handed over to viewers, the packager is critical for maintaining provenance and authenticity. However, today no standard exists that clearly defines how a dynamic packager should obtain, verify, and embed C2PA manifests, certificates, and signatures, especially in live and shot-by-shot workflows. These user stories highlight practical requirements for enabling reliable provenance in packaging, archiving, and live streaming, as well as the risks of broken or incomplete trust chains. I deliver encrypted and signed media packages to viewers and distribution platforms. I wish to insert C2PA provenance manifests and signatures so that I may achieve trustworthy end-to-end provenance for assuring users and platforms that the content is authentic and unaltered	Ability to ingest and verify C2PA manifests and certificates before packaging. Ability to securely embed provenance information into packaged and encrypted streams.	each org in the flow has different and very confusing definitions on what things like C2PA should be and how it should be implemented	Verify provenance Add provenance Include encrypted streams	Package provider	Packaging
008 **(C)**	streaming solutions manager	As a Software Development Company building dynamic packagers	I deliver live and on-demand media workflows to broadcasters and OTT providers. I wish to insert shot-by-shot provenance metadata so that I may achieve real-time authenticity for live streaming for supporting news and sports where trust in every shot is critical.	Ability to interact with external systems that provide assertions in real time. Ability to package, sign, and transmit provenance metadata at per-shot granularity.		Add provenance Package, sign, and transmit provenance metadata at per-shot granularity Assertions from external systems in real time	Package provider	Packaging

© SMPTE 2026 – All Rights Reserved

009 **(C/D)**	streaming solutions manager	As a Packager in charge of archive repackaging	I deliver reprocessed and redistributed content to broadcasters, archives, or consumers. I wish to insert validated C2PA provenance information even when original certificates have expired so that I may achieve long-term archival integrity for historical and cultural preservation.	Ability to validate and re-sign provenance information against trusted CAs, even decades later. Clear rules on how expired certificates and claims should be handled when re-issuing or repackaging content.		Verify provenance Add provenance Rules on how expired certificates and claims should be handled	Package provider of archived content	Packaging
010 **(C)**	streaming solutions manager	As a Dynamic Packager	I deliver encrypted and signed content to broadcasters and OTT platforms. If I cannot access or verify C2PA manifests, certificates, and signatures, I risk inserting unverified or incomplete provenance metadata. This risk is amplified by current proposals (e.g., demonstrated at IBC 2025 by BBC/EBU) that deliberately break the provenance chain for privacy reasons, replacing it with a single institutional stamp (“Trust us—it’s BBC News”). Without standards or safeguards, I may unknowingly package media with a broken or partial trust chain, causing viewers to believe provenance is intact when in fact critical links are missing. Consequences: Loss of trust in provenance claims if privacy-driven chain breaks are normalized. Broadcasters and OTT platforms may face liability for delivering content with incomplete provenance while claiming the opposite End-users may lose confidence in C2PA altogether if the “verify” button cannot distinguish between intact and broken chains.	Verify C2PA manifests, certificates, and signatures.		Verify provenance C2PA manifests, certificates, and signatures.	Package provider	Packaging

© SMPTE 2026 – All Rights Reserved

011 **(C)**	Applications developer	[as a developer in D-Cinema Package (DCP) and Interoperable Master Format (IMF) environments]	The provenance of a content version is asserted via the Composition Playlist (CPL) object in the form of an enveloped digital signature. Referenced MXF elements are bound to the signature by embedded message digest values in the CPL. In cases of encrypted essence, content keys are bound to the respective CPL by reference to the content signer. Our interest in C2PA is from the point of view of supporting future provenance metadata in the DCP and IMF workflows, enabling deeper linking to content origination.	Supporting future provenance metadata in the DCP and IMF workflows.		Provenance for IMF	D-Cinema Package provider	D-Cinema packaging
012 **(C)**	ENGINEER	As the person responsible for converting television commercial content for domestic Japanese broadcasters	converting television commercial content for domestic Japanese broadcasters	I request that technical contact information (company name, contact person, and contact details) created as metadata be added to verify any issues with the source material.	The client who supplied the content does not know the exact creator. They often forward materials received from higher-level clients without sufficient information.	Verify provenance Provide technical contact details in case of queries	Package provider	Packaging Annotation
013 **(C)**	Watermark embedding and detection	As a media/content processor or consumer	I want to ensure provenance metadata can be retrieved and verified when the media is no longer in the MXF (or other professional format) container.	Embed a watermark(s) during content creation/modification as a soft-binding to the provenance metadata.	Social media platform ingest; consumer consumption	Watermark for soft-binding to provenance Essence may no longer be in MXF	Package provider	Ingest Delivery
014 **(C)**	Watermark embedding and detection	As a media/content processor or consumer	I want to retrieve or access the canonical asset(s) when the provenance metadata cannot be verified.	Embed a watermark(s) during content creation/modification. Cloud services that host canonical asset(s). Canonical content recovery based on watermark detection during verification processing.		Canonical assets in the cloud Embed watermark Provenance verification based on watermark	Package provider	Packaging Viewing

© SMPTE 2026 – All Rights Reserved

015 **(B)**	Video standards conversion	As a supplier of motion compensated video standards conversion solutions	I deliver hardware, software, services and intellectual property to large parts of the production and distribution chains including OB/MCR facilities, telco providers, content libraries and archives and CDNs. I wish to generate, sign, and embed new provenance information, inheriting the original provenance information and describing the vendor and standards converter model/version employed to achieve the conversion as authenticated credentials for the purpose of maintaining a chain of trust in the content authenticity by any downstream recipients of the content by identifying a specific standards conversion method which may be made open to independent audit/accreditation by other qualified, trusted authenticated 3rd party institutions.	Ability to verify the provenance information of the received original file. Ability to generate, sign, and embed new provenance information, inheriting the original provenance information when performing video standards conversion that, unlike transcoding, doesn't closely approximate the original pixels but necessarily synthesizes new image content with macro-scale changes.	Video standards conversion, and in particular, motion compensated frame rate conversion, by definition performs an automated, complex, multi-dimensional interpolation of the source content for which simple methods for automatically confirming content equivalence in such a converted flow/version will not function.	Verify provenance Maintain provenance Add provenance Generate, sign, embed new provenance information, inheriting the original provenance information when performing video standards conversion that, unlike transcoding, doesn't closely approximate the original pixels but necessarily synthesizes new image content with macro-scale changes	Manufacturer Video standards conversion	Production Distribution Archiving
016 **(B)**	System Support	As a Post-production Editor	I deliver an edited master to the distribution and archiving departments. I wish to insert metadata defining the authorized scope of use so that I may ensure that all downstream users are aware of the content's usage restrictions, which are based on the provenance of the original source material.	Ability to access and review the provenance information of source materials before an edit. Ability to define the scope of use (e.g., usage rights, restrictions) for the edited content based on the source material's provenance. Ability to embed this usage scope information as new, signed metadata into the final edited asset.	When editing and delivering video material provided by a client, it has become necessary for us to confirm that the material was not obtained illegally.	Verify provenance Add provenance Add usage rights	Editor	Post production Distribution Archiving

© SMPTE 2026 – All Rights Reserved

017 **(A/B)**	News Gathering , Editing , Media Exchange	As a News Desk Editor	I deliver UGC and external materials to content editors. I wish to insert metadata about contributor consent, rights, identity evidence, and risk flags so that editorial staff can minimize manual checks and publish quickly while reducing risks.	Ability to attach and share metadata on consent, rights, identity proof, and risk flags with downstream editors. Mechanism to ensure this metadata travels consistently with the content through the workflow.	Scenario: Using UGC in News Reporting When relying on user-generated content from social media, we often lose metadata that is crucial for verifying the contributor and filming circumstances. At the same time, revealing precise time and location can endanger the source. Because there are few automatically verifiable traces, assessing whether the material can be trusted takes extra time and creates uncertainty in newsroom decisions.	Verify provenance of UGC Add provenance Attach and share metadata on consent, rights, identity proof, and risk flags with downstream editors Metadata travels consistently with the content through the workflow	News desk editor	Post production
018 **(A)**	News Gathering , Editing , Media Exchange	As a Field Reporter	I deliver offline mobile-recorded clips to recording staff. I wish to insert device signatures, equipment information, and geospatial/temporal metadata so that consistent provenance can be maintained even without network connectivity."	Ability to capture and embed device signature, equipment details, and location/time at the point of recording. Support for offline embedding that synchronizes provenance once connectivity is restored.		Add provenance Device signature, equipment details, location/time at the point of recording Support for offline embedding that synchronizes provenance once connectivity is restored	Field reporter	Acquisition

© SMPTE 2026 – All Rights Reserved

019 **(C)**	News Gathering , Editing , Media Exchange	As a Program Producer	I deliver final packaged files to scheduling and playout. I wish to insert rights metadata so that long-term reuse and distribution rights management can be handled smoothly.	Ability to embed rights metadata into final program packages. Capability for downstream scheduling and playout systems to read and act on rights information.		Add provenance Add usage rights Downstream scheduling and playout systems to read and act on rights information	Producer	Packaging
020 **(C)**	News Gathering , Editing , Media Exchange	As a Web Editor	I wish to insert content credentials and provenance badges so that audiences have a clear verification path when consuming the content.	Ability to embed content credentials and provenance badges into CMS-published videos. Mechanism for viewers to access and verify provenance information at the point of consumption.		Add provenance Embed content credentials and provenance badges so that audiences have a clear verification path when consuming the content.	Web editor	Packaging
021 **(C)**	Head of Competence Center Production & Infrastructure	As a public service media provider	Public service media provider	Differentiate between technical and user-generated (organizational) metadata. Implement redactions of metadata to protect sources (e.g., journalists in war regions). Validate the incoming sources/origins including identification of potential content manipulation	Metadata stripping in tools that don't support C2PA Missing metadata in user-generated content	Differentiate between technical and organizational metadata Redact metadata Validate provenance	Public service media provider	Distribution

© SMPTE 2026 – All Rights Reserved

022 **(B)**	Formulation of facility planning, creation of specifications for procurement, and their installation and maintenance Construction of optimization for program production workflow	As a Video Footage Manager for News Program	I check video clips obtained from external sources such as content submitted by general viewers and provide them to the video editing staff. I want to check the shooting history recorded by the contributor and the editing history by AI and editing software embedded in the obtained footages so that we can prove the reliability of footages obtained from external sources.	Check the shooting history recorded by the contributor and the editing history by AI and editing software embedded in the obtained footages.		Validate provenance of UGC Shooting history Editing history Identify use of AI tools	Producer	Production
023 **(B)**	Formulation of facility planning, creation of specifications for procurement, and their installation and maintenance Construction of optimization for program production workflow	As a Video Editor	I provide the news clip to the broadcasting system. As the person responsible for the editing results, I want to insert my signature so that it can be proven that the clip has not been tampered with after I created it.	Insert my signature so that it can be proven that the clip has not been tampered with after I created it. I want to remove the provenance information that was inserted to the video footage before editing so that the confidentiality of the sources is protected.		Add provenance Insert my signature Redact metadata to protect confidentiality of sources	Video editor	Production
024 **(C)**	Formulation of facility planning, creation of specifications for procurement, and their installation and maintenance Construction of optimization for program production workflow	As a person in charge of Video Distribution	I provide web content to distribution platforms.	I want to insert the company's (copyright holder's) signature so that it can be proven that the content has not been tampered with after our company created it. I want to remove the signatures of the editors who worked on each clip that makes up the content so that the personal information of the editors is protected.		Add provenance Insert the company's (copyright holder's) signature Redact metadata	Web editor	Distribution (web)

© SMPTE 2026 – All Rights Reserved

025 **(A)**	I design and supervise these workflows for mine and other entities.	As a person in charge of acquisition	Acquisition	It would be useful to have many pieces of metadata travel along with the footage and not as easily lost sidecar info. As well, cameras and audio recorders need to facilitate the embedding of external data, not generated by that device into the acquired media. Likewise, every tool down the chain should protect and pass on this metadata transparently without user intervention.		Provenance metadata ideally bound to essence Add provenance Cameras and audio recorders need to facilitate the embedding of external data, not generated by that device into the acquired media Provenance metadata travels seamlessly	In charge of acquisition	Acquisition
026 **(A)**	I design and supervise these workflows for mine and other entities.	As a person in charge of post-production	Sometimes in editorial or other stages of post it'd be nice to be able to track / verify the source of a piece of footage used as an asset in, for example, a VFX shot.	So it'd be useful to be able to have finished shots contain markers that pointed back to every single asset used in generating that shot. And likewise for proxy and editorial media.		Able to identify all assets used to generate a shot	In charge of film post production	Film post production
027 **(A)**	I design and supervise these workflows for mine and other entities.	As a person in charge of ensuring unbroken chain of custody of footage		It would be useful to have frame/track level checksumming / metadata that allowed for verification that transferred picture, sound, and other data was authentic to the origin (as opposed to the non-embedded sidecar method currently in use)		Embedded rame/track level checksumming / metadata	Custody of unbroken footage (feature film)	Film post production

© SMPTE 2026 – All Rights Reserved

028 **(A)**		As an editor of news programs	I edit video materials received from reporting sites into news content. To ensure reliability during post-verification and archiving, I would like to embed metadata such as cameraman information, shooting date/time, and location information in the final product.	By importing the embedded provenance information into the MAM or CMS, expanding it into our own metadata, and embedding the verification results in a new form, the content can be safely used for secondary and tertiary purposes. Maintain provenance within our MAM or CMS to enable easy traceability if issues arise. Embed information and stamps of the verifying organization so recipients can confirm that the data has not been tampered with.	In some cases, video materials sent from news-gathering sites contain incomplete or missing information such as the cameraman, shooting location, and shooting date/time, requiring editors to spend considerable time verifying it. Loss of original provenance information after transcoding or editing, creating challenges for reliable archiving. Provenance cannot be inherited from screenshots or re-shot content. Difficulty managing provenance of original materials when editing processes are involved, especially when incorporating archive materials lacking provenance information.	Add provenance Embed cameraman information, shooting date/time, and location information Import embedded provenance into MAM or CMS Embed information and stamps of the verifying organization Maintain provenance within MAM or CMS	Video editor	Production News

© SMPTE 2026 – All Rights Reserved

029 **(D)**	As a member of the technical division, I am involved in the end-to-end workflow for program production across all genres covering the acquisition of video materials, editing, metadata management, playout, and archiving.	As an archive manager	I convert and register edited video files for long-term storage. I want to verify the original provenance information and, when necessary, add and sign new provenance information.	Verify the original provenance information and, when necessary, add and sign new provenance information. By importing the embedded provenance information into the MAM or CMS, expanding it into our own metadata, and embedding the verification results in a new form, the content can be safely used for secondary and tertiary purposes. Maintain provenance within our MAM or CMS to enable easy traceability if issues arise. Embed information and stamps of the verifying organization so recipients can confirm that the data has not been tampered with.		Verify provenance Import embedded provenance into MAM or CMS Add provenance Embed information and stamps of the verifying organization	Archivist	Archive
030 **(A)**	Research and development of technologies to address dis/misinformation in media production and distribution workflows including prototype development based on the C2PA specifications and feasibility studies.	As a media coordinator	I collect news source materials from audiences and news agencies and assign them to editing staff. I want to categorize and verify these materials before assigning them to editing staff so that only authorized materials are used in news production. Categories may include camera footage, AI-generated content, tampered media, and others.	Ability to categorize source materials including video, audio, and text based on provenance metadata. Categories may include camera footage, AI-generated content, tampered media, and others. Ability to verify the authenticity of the materials and their provenance data.	There is a possibility that fake videos may be included in news source materials provided by audiences and news agencies, making it difficult for human operators to determine whether the videos are authentic. - Even when provenance metadata is attached during the content production workflow, it may be removed during transcoding and other processes.	Categorize source materials including video, audio, and text based on provenance metadata Verify provenance	Media coordinator	Acquisition (UGC and external content)

© SMPTE 2026 – All Rights Reserved

031 **(B)**	Colorist/Engineer	As a producer	Responsible for television content for domestic broadcasters in Japan.	I would like to request that the metadata include information about the technical staff who created the materials (such as company name, contact person, and contact details), so that any issues with the materials can be properly verified.	I was unable to obtain accurate information about the materials provided by the client, and my inquiries only resulted in vague answers.	Include information about the technical staff who created the materials (such as company name, contact person, and contact details)	Producer	Production
032 **(B)**	Developer	As a content creator	I want to give my audience the ability to be able to understand what they see.	[Provenance information available to viewers]	Audio manipulation	Provide provenance to viewers	Content creator	Production
033 **(B)**	Research and development, broadcasting technology standardization.	As a live broadcasting master control section engineer	I receive the incoming feed from the news gathering section and transport them to the delivery section.	It is my goal to be able to verify the provenance information in real time as I receive footage.	Confirming provenance of incoming footage especially from end users, is both critical and difficult.	Verify provenance in real time	Master control engineer	Production
034 **(B/E)**	The role of research and development of new technologies within the overall production and distribution business.	[Related to advertising]	In Japan, fraudulent video ads have become a social issue in the operation of certain in-stream advertising. To address this, we aim to include advertiser information, action records proving who created the ad, as well as auditor information and action records proving that the audit was conducted, as provenance data of the ad video. This will enable viewers to verify the authenticity of the advertisement and enhance transparency regarding its origin. In addition, considering the use case where the advertisement video is delivered as a mezzanine file in MXF and then distributed to consumers in MP4 or fMP4...	It is necessary that assertion information—consisting of the advertiser's information as the actor who created the advertisement and the action record proving that creation, as well as the auditor organization's information as the actor who reviewed the advertisement and the action record proving that audit—be embedded in or linked to the advertisement video, so that consumers can verify its authenticity. It is required that provenance information maintain interoperability between MXF and MP4/fMP4.	C2PA has already been adopted for MP4 and MOV, but provenance information cannot be preserved during conversion with MXF. In C2PA v2, the operation model that treated consumers as verifiers and companies such as broadcasters, advertisers, and advertising review organizations as signers is no longer considered.	Provide provenance Detailed information about advert Provenance information maintains interoperability between MXF and MP4/fMP4	Broadcaster	Auditing Viewing
035 **(C)**	Ingest and Playout servers	end user	As end user watching content, i would like to know when my subtitles or audio have been generated by AI.	Would like to know when my subtitles or audio have been generated by AI.		Would like to know when subtitles or audio have been generated by AI	Viewer	Viewing

© SMPTE 2026 – All Rights Reserved

036 **(A/B)**	Television broadcaster and News/local programming generation, web/OTT programming distribution	As a News Manager and Producer	As a News Manager and Producer, I want to verify that video is authentic and the origins are verifiable to ensure that news stories delivered by the station are accurate, to preserve journalistic integrity and avoid legal issues.	Verify that video is authentic and the origins are verifiable to ensure that news stories delivered by the station are accurate, to preserve journalistic integrity and avoid legal issues.	Viewer contribution footage or footage from stringers.	Verify provenance of footage from stringers and UGC	News Manager and producer	Acquisition (external)
037 **(A/B)**	R & D	Broadcast engineer	As a broadcast engineer, I want to analyze externally collected content (which may lack compliant metadata or have no metadata) to understand its characteristics (e.g., whether it is AI-generated, or to estimate areas potentially altered by AI),	Functionality to determine whether image/video content collected from external sources (not broadcast professionals) is AI-generated when broadcasting such content.	The dramatic evolution of image/video-generating AI has made it increasingly difficult to distinguish whether an image is real or not.	Determine whether content from external sources (not broadcast professionals) is AI-generated or manipulated	Broadcast engineer	Acquisition (external) content)
038 **(A)**	Product Manager	Product manager	User-generated video trailers of events, TV shows, movies, etc. created as mashups of media segments from both legitimate, illegitimate, even AI generated content.		Ensuring authenticity and legitimacy of the entirety and segments thereof (thumbnails, trailers, audio, descriptors, etc.) of media content).	Verify provenance Entirety and segments thereof (thumbnails, trailers, audio, descriptors, etc.) of media content UGC and other external sources	Product manager	Acquisition (external) content) Archive

© SMPTE 2026 – All Rights Reserved

039 **(A)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Journalist	As a journalist in the field, I deliver live uncompressed video to colleagues in the newsroom. I wish to insert location, wall clock time and other context around capture so that downstream consumers can verify the video is authentic.	Insert location, wall clock time and other context around capture.	Black-box" services & products that do not use industry standards or protocols are difficult to manage as there is no simple way of adding C2PA requirements to them, and so provenance claim-check patterns have to be considers. Additionally, distribution platforms that modify content, such as social media, are an issue as we have very little individual influence.	Add provenance location, wall clock time and other context around capture	Journalist	Acquisition
040 **(A)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Journalist	As a journalist in the field, I deliver live uncompressed video over potentially untrusted transports to colleagues in the newsroom. I wish to insert location, wall clock time and other context around capture so that colleagues can verify the video is authentic.	Insert location, wall clock time and other context around capture that remain secure over untrusted transports.		Insert location, wall clock time and other context around capture Maintain provenance over untrusted transports	Journalist	Acquisition
041 **(A)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Journalist	As a journalist in the field, I deliver live uncompressed video via a number of video processing steps to colleagues in the newsroom. I wish my metadata to remain secure and attached to the content so that video can be verified as authentic.	Metadata to remain secure and attached to the content		Maintain provenance attached to the content	Journalist	Acquisition

© SMPTE 2026 – All Rights Reserved

042 **(A)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	OB engineer	As an OB engineer, I deliver a feed back to base that contains both a third-party / host broadcaster's material, as well as our own cameras. I want my outgoing feed to securely contain both the contribution source's provenance data, on a shot-by-shot level, as well as our own provenance, so that downstream consumers can understand shot-by-shot provenance as it changes during a live programme.	Outgoing feed from OB to securely contain both the contribution source's provenance data, on a shot-by-shot level, as well as own provenance.		Maintain provenance Add provenance Outgoing feed from OB to securely contain both the contribution source's provenance data, on a shot-by-shot level, as well as own provenance	OB engineer	Acquisition
043 **(B)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Video editor	As a video editor, I combine many video sources and graphics in one output video, for publication to consumers. I want all the provenance data of source material to be carried through, as well my employers "package-level" provenance, so that consumers can understand where the components of the video package came from, and if they are authentic.	All the provenance data of source material (video and graphics) to be carried through as well as employers package-level provenance.		Maintain provenance Add provenance	Video editor	Packaging
044 **(B)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Video editor	As a video editor, I combine many video sources and graphics in one output video, for publication to consumers. I want to restrict the amount of provenance data of source material that is carried through, so that consumers are not confused by many layers of irrelevant technical changes.	Restrict the amount of provenance data of source material that is carried through, so that consumers are not confused by many layers of irrelevant technical changes.		Redact provenance so that consumers are not confused by many layers of irrelevant technical changes	Video editor	Production

© SMPTE 2026 – All Rights Reserved

045 **(B)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Journalist	As a journalist, I combine many media sources and graphics in one output package, for publication to consumers. I want to remove specific provenance data from source material to prevent it being carried through, so that vulnerable sources or subjects of the material in conflict zones are not put at risk of harm.	Remove specific provenance data from source material to prevent it being carried through, so that vulnerable sources or subjects of the material in conflict zones are not put at risk of harm.		Redact provenance so that vulnerable sources or subjects of the material in conflict zones are not put at risk of harm.	Journalist	Production
046 **(B)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	Equipment manufacturer	As an equipment manufacturer, I provide equipment to consumers that applies their configurable “house look” to video. I want to propagate incoming provenance data and add the equipment’s specific edits to the history, to ensure unbroken provenance and authenticity information for the next step in the chain.	Propagate incoming provenance data and add the equipment’s specific edits to the history, to ensure unbroken provenance and authenticity information for the next step in the chain.		Maintain provenance Add provenance	Equipment manufacturer	Production
047 **(C)**	Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	MCR engineer	As an MCR engineer, I provide an outgoing feed containing as much content provenance as possible to live consumers. I wish to “vouch” for source provenance metadata when I am certain of it, in a situation where an important source does not provide provenance data, or it is broken, so that consumers can continue to verify the authenticity of media.	“vouch” for source provenance metadata when certain of it, in a situation where an important source does not provide provenance data, or it is broken, so that consumers can continue to verify the authenticity of media.		Maintain provenance Add provenance	MCR engineer	Distribution Viewing

© SMPTE 2026 – All Rights Reserved

048 **(C)**	Development of authenticity verification technology	Users, by means of a user agent such as a web browser	Creators, authors, publishers and other producers of online content generate website and we pages (hereinafter referred to as “Web Content”). Such Web Content consists of text, style, images, video and other objects, and is signed by means of a mechanism that ensures both the authenticity of the creator of the Web Content and the integrity and consistency of its composition. Users, by means of a user agent such as a web browser, are able to verify the authenticity of the creator and the integrity and consistency of the composition of such Web Content through the validation of the signature. It is envisaged that the above-mentioned mechanism and methods of verification may be realized through a combination of multiple schemes, whether existing or newly developed.	The signature shall cover: - the identity of the creator (authenticity); and - the integrity and consistency of the packaged content (no unauthorised modification). Ability to provide sufficient metadata to allow validation of both authenticity and integrity. Shall be designed to accommodate multiple signature and verification schemes. Allow for the use of both existing methods and newly developed methods in combination.		Verify	User	viewing Web

© SMPTE 2026 – All Rights Reserved

049 **(C)**	The JPEG Committee is a standardisation group that produces and maintains a range of media-based file format standards including the JPEG 1 standard (ISO/IEC 10918) which is the most used image file format online, as well as lossy/non-lossy image and video formats, such as JPEG 2000 (ISO/IEC 15444) and JPEG XS (ISO/IEC 21122), storage formats such as JPEG DNA (ISO/IEC 25508) and explorations such as JPEG XE Event-Based Vision and JPEG RF Radiance Fields 3D representation. JPEG Trust is a part of and interrelated with this ecosystem. JPEG Trust arises from an exploration in 2020 addressing requirements for mis- and dis-information in digital media. The JPEG Trust framework provides a comprehensive framework for	End user	The list of use cases JPEG Trust seeks to address is virtually unlimited. A short list of use case domains identified in our Use Cases and Requirements document; these are listed below: Misinformation and disinformation: Deep fakes, Manipulated media, Media intentionally used out of context e.g. As an end user, I consume online media. I wish to understand if the video I am watching depicts real life or is an AI rendering that is meant to mimic real life, so that I can understand what meaning I am meant to understand and weather I can trust it in my decision-making and any actionable responses. Forgery / Media forensics: Document authenticity & forgery (e.g. IDs and passports), Insurance fraud (e.g. pictures of accidents), KYC (Know Your Customer) (e.g. fake identity), Impostering (e.g. impersonating a celebrity) e.g. As an agent of an insurance company, I manage insurance claims that are evidenced by images and video. I wish to understand if the media assets I accept as evidence is authentic, so that I can process insurance payments properly and avoid being scammed. Media creation: Authenticity & integrity in photography & videography, Use of deep fakes for special effects, Media processing, AI Generated Content (AIGC), Short content bursts, UGC (User Generated Content) e.g. TikTok, Triller, Adobe Spark, Picture and movies production Media modification, Media asset editing software, Movie preservation, Film enhancement, Colorization, Restoration of old movies or photographs Media composition: Green screens, Collage or layered media assets, Augmented and	I wish to understand if the video I am watching depicts real life or is an AI rendering that is meant to mimic real life, so that I can understand what meaning I am meant to understand and weather I can trust it in my decision-making and any actionable responses.	Determine whether AI or real	Verify	Viewer	Viewing

© SMPTE 2026 – All Rights Reserved

	individuals, organizations, and governing institutions interested in establishing an environment of trust for the media that they use and supporting trust in the media they share online. The framework addresses a range of relevant aspects of trustworthiness in media assets, and is built in compliance with a range of well established JPEG standards as well as other widely adopted industry standards.		extended reality Media tokenization: Authorship attribution and rights declaration, Rights monetization, Rights remuneration Any number of user stories can be derived from these domains. For further information about JPEG Trust Use Cases and Requirements please see https://ds.jpeg.org/documents/jpegtrust/wg1n100886-104-REQ-Use_cases_and_requirements_for_JPEG_Trust_v3_0.pdf					

© SMPTE 2026 – All Rights Reserved

050 **(C)**	The JPEG Committee is a standardisation group that produces and maintains a range of media-based file format standards including the JPEG 1 standard (ISO/IEC 10918) which is the most used image file format online, as well as lossy/non-lossy image and video formats, such as JPEG 2000 (ISO/IEC 15444) and JPEG XS (ISO/IEC 21122), storage formats such as JPEG DNA (ISO/IEC 25508) and explorations such as JPEG XE Event-Based Vision and JPEG RF Radiance Fields 3D representation. JPEG Trust is a part of and interrelated with this ecosystem. JPEG Trust arises from an exploration in 2020 addressing requirements for mis- and dis-information in digital media. The JPEG Trust framework provides a comprehensive framework for	Insurance company agent	The list of use cases JPEG Trust seeks to address is virtually unlimited. A short list of use case domains identified in our Use Cases and Requirements document; these are listed below: Misinformation and disinformation: Deep fakes, Manipulated media, Media intentionally used out of context e.g. As an end user, I consume online media. I wish to understand if the video I am watching depicts real life or is an AI rendering that is meant to mimic real life, so that I can understand what meaning I am meant to understand and weather I can trust it in my decision-making and any actionable responses. Forgery / Media forensics: Document authenticity & forgery (e.g. IDs and passports), Insurance fraud (e.g. pictures of accidents), KYC (Know Your Customer) (e.g. fake identity), Impostering (e.g. impersonating a celebrity) e.g. As an agent of an insurance company, I manage insurance claims that are evidenced by images and video. I wish to understand if the media assets I accept as evidence is authentic, so that I can process insurance payments properly and avoid being scammed. Media creation: Authenticity & integrity in photography & videography, Use of deep fakes for special effects, Media processing, AI Generated Content (AIGC), Short content bursts, UGC (User Generated Content) e.g. TikTok, Triller, Adobe Spark, Picture and movies production Media modification, Media asset editing software, Movie preservation, Film enhancement, Colorization, Restoration of old movies or photographs Media composition: Green screens, Collage or layered media assets, Augmented and	I wish to understand if the media assets I accept as evidence is authentic, so that I can process insurance payments properly and avoid being scammed.	Verify authenticity	Verify	Viewer (Insurance agent)	

© SMPTE 2026 – All Rights Reserved

	individuals, organizations, and governing institutions interested in establishing an environment of trust for the media that they use and supporting trust in the media they share online. The framework addresses a range of relevant aspects of trustworthiness in media assets, and is built in compliance with a range of well established JPEG standards as well as other widely adopted industry standards.		extended reality Media tokenization: Authorship attribution and rights declaration, Rights monetization, Rights remuneration Any number of user stories can be derived from these domains. For further information about JPEG Trust Use Cases and Requirements please see https://ds.jpeg.org/documents/jpegtrust/wg1n100886-104-REQ-Use_cases_and_requirements_for_JPEG_Trust_v3_0.pdf					
051	Camera manufacturer	As a camera manufacturer	As a camera manufacturer i deliver media files and metadata to post production. I wish to insert provenance and authenticity data that can be traced to a certain camera and certain author.	I wish to insert provenance and authenticity data that can be traced to a certain camera and certain author.	None yet	Insert provenance related to specific camera and author	Manufacturer	Production
052	Camera manufacturer	As a camera manufacturer	As a camera manufacturer i deliver media files and metadata to post production. I wish to generate provenance and authenticity data that can be traced to a certain camera and certain author. This data can be inserted or transferred and stored separately in a log-file.	I wish to generate provenance and authenticity data that can be traced to a certain camera and certain author. This data can be inserted or transferred and stored separately in a log-file.	None yet	Generate provenance related to specific camera and author	Manufacturer	Production
053	Camera manufacturer	As a camera manufacturer	As a camera manufacturer I want to offer trusted software to authenticate previously recorded clips.	I want to offer trusted software to authenticate previously recorded clips.	None yet	Offer trusted software for authentication	Manufacturer	Production

© SMPTE 2026 – All Rights Reserved

054	Researcher on forthcoming media technologies that can boost creativity of filmmaking. Film production.	As a researcher on forthcoming media technologies	I want to know if content created by A.I for filmmakers can be verified whether such content is legal free to be used.	I want to know if content created by AI for filmmakers can be verified whether such content is legal free to be used.		Verify whether AI content is free and legal	Reseracher in film production	Production
055	Director of Engineering	As a facility design engineer	As a facility design engineer, I want the operators to have tools that can verify the authenticity of incoming content	I want the operators to have tools that can verify the authenticity of incoming content		Tools to verify authenticity	Facility design engineer	Production Distribution
056	Director, Solutions & Sustainment	Responible for newsroom	Newsroom content needs to be visually verified and restricted per specific requirements. That metadata needs to be editable and updatable at all stages to facilitate takedown requests.	newsroom content needs to be visually verified and restricted per specific requirements. That metadata needs to be editable and updatable at all stages to facilitate takedown requests.	At all stages	Verify metadata Redact metadata Edit metadata	Newsroom manager	Production Distribution
057	VFX supervisor Cinematographer, consultant	As a VFX Supervisor	As a VFX Supervisor, I deliver camera-accurate composites and CG elements to the Director and DI team. I wish to insert precise lens distortion, sensor characteristics, color transform, and exposure metadata so that I may achieve physically accurate lighting and comp alignment for photoreal integration and minimizing post-fixes.	I wish to insert precise lens distortion, sensor characteristics, color transform, and exposure metadata so that I may achieve physically accurate lighting and comp alignment for photoreal integration and minimizing post-fixes.	GENAI in images and movies files can be stripped of meta tags and input into packages and models without proper credit or tags	Insert camera and lens metadata	VFX Supervisor	Production
058	Lead Distribution (Programmverbreitung)	As an operator of the centralized transcoding and encoding facility	As an operator of the centralized transcoding and encoding facility I want to sign and add organisational provenance information.	I want to sign and add organisational provenance information.		Sign provenance information Add provenance information	Centralized transcoding and encoding facility	Production Distribution

© SMPTE 2026 – All Rights Reserved

DMS-II-1		News Director	As a News Director, I want to durably insert production planning metadata in story assignments, so that all crew members can work smoothly together on show creation. Note 1 to entry: The C2PA core specifications generally refer to this metadata as gathered assertion metadata. Note 2 to entry: The auto sync registration feature provided by a certain professional vendor provides one example of automatic delivery of assignment metadata to a field camera.	Insert production planning metadata in story assignments		Insert production planning metadata in story assignments	News director	Acquisition Documentary News
DMS-II-2		News camera operator	As a News Camera Operator, I want to insert geospatial, temporal and integrity metadata in each shot, so that this metadata will be available throughout the production workflow. Note 1 to entry: The C2PA core specifications generally refer to this metadata as generated assertion metadata.	Insert geospatial, temporal and integrity metadata in each shot, so that this metadata will be available throughout the production workflow.		Insert geospatial, temporal and integrity metadata	Camera operator	Acquisition Documentary News
DMS-II-3		News associate producer	As a News Associate Producer, I want to verify geospatial, temporal and integrity metadata in incoming camera storage cards, received news feeds, and pool feeds, so that editors and analysts will have confidence in source quality and authenticity. Note 1 to entry: The C2PA user experience guidance documents generally describe this verification step as a level 3 display of provenance data.	Verify geospatial, temporal and integrity metadata in incoming camera storage cards, received news feeds, and pool feeds, so that editors and analysts will have confidence in source quality and authenticity.		Verify provenance Geospatial, temporal and integrity metadata in incoming camera storage cards, received news feeds, and pool feeds	News associate producer	Acquisition Documentary News
DMS-II-4		News reporter	As a News Reporter, I want to receive verified metadata along with incoming shots, so that I can make authoritative statements as part of my reportage.	Receive verified metadata along with incoming shots		Verify provenance	News reporter	Acquisition Documentary News

© SMPTE 2026 – All Rights Reserved

DMS-II-5		News technician	As a News Technician, I want to receive edited metadata with finished shots, so that I can prepare lower thirds and teleprompter cues	Receive edited metadata with finished shots, so that I can prepare lower thirds and teleprompter cue		Verify provenance	News technician	Post production News Documentary
DMS-II-6		News analyst and anchor	As a News Analyst and Anchor, I want to preview the story, script, and shots, so I can be prepared to present well to studio camera	[preview story, script, shots]			News analyst and anchor	
DMS-II-7		News supervising producer	As a News Supervising Producer, I want to assemble packages of content and verified metadata, so I can deliver a premium quality package for broadcast and syndication.	Assemble packages of content and verified metadata		Verify provenance	Producer	Distribution News
DMS-II-8		News producer	As a News Producer, I want to make use of generative AI to add content supporting a story. Note 1 to entry: This additional content may consist of copy, figures, animation and supplemental sound effects. Note 2 to entry: This additional content may serve the needs of localization. Note 3 to entry: This additional content may serve the special presentation needs of web pages, OTT apps, and smartphone apps.	[Use generative AI to add content]		Add provenance Use Generative AI	Producer	News
DMS-II-9		News ad sales manager	As a news ad sales manager, I want to ensure that all delivered materials have been tagged with unambiguous identifiers (globally-unique and freely resolvable) identifying each program, each package within a program, and the media outlet for which it was produced so that this information can be reliably included in disseminated content for later measurement of viewership, audience demographics, content re-use, and other commercially-valuable factors.	All delivered materials have been tagged with unambiguous identifiers		Verify provenance Unique identifiers	News ad sales manager	News Distribution Viewing

© SMPTE 2026 – All Rights Reserved

DMS-II-10		News consumer (viewer)	As a news consumer, I want to be assured of the accuracy of the content and source of the news materials I view, which means a well-defined, unambiguous metadata hand-off from news content production to news media distribution including unambiguous identifiers (globally-unique and freely resolvable) for each program, each package within a program, the key people appearing in the content, and the media outlet for which it was originally produced or from which it was subsequently delivered.	Assurance of accuracy of the content		Verify provenance	Viewer	Viewing News
DMS-II-11		Archivist	As a media archivist, I want to receive produced packages and b-roll that have been tagged with unambiguous identifiers (globally-unique and freely resolvable) identifying the package itself, the program for which the content was produced, and the key people present in the material to aid in the material's storage, retention, retrieval, re-use, and re-sale. Note 1 to entry: The trust anchors provided in the C2PA Trust List only secure generated assertion metadata. Note 2 to entry: The trust anchors specified by the Creator Assertions Working Group of the address gathered assertions. Note 3 to entry: The Creator Assertions Working Group (CAWG) operates under a joint participation agreement with the Decentralized Identity Foundation and the Trust Over IP Foundation. Note 4 to entry: Archival and forensic efforts are aided equally well by CAWG gathered assertions and C2PA generated assertions.	Receive produced packages and b-roll that have been tagged with unambiguous identifiers		Verify provenance	Archivist	Archive

© SMPTE 2026 – All Rights Reserved

Vendor -1		News & documentary shooting staff	Shooting staff obtain the Story Metadata sent from the News Room Computer System, if available, and add the metadata to the C2PA manifest	Add metadata received from the newsroom to the C2PA manifest [Editor or validator to quickly and accurately check the C2PA Story Metadata] [Possible need to define Story Metadata as a C2PA embedded assertion]		Receive story metadata from newsroom Add provenance	Shooting staff	Acquisition Documentary News
Vendor -2		News & documentary shooting staff	Shooting staff conduct shooting based on the instructions provided in the Story Metadata	Embed GPS, Timestamp, and other metadata as C2PA Manifest in the shooting data. Record the provenance of processing performed within the camera. Document the use of AI-effects within the camera		Add provenance - Embed GPS, Timestamp, and camera metadata (including AI effects)	Shooting staff	Acquisition Documentary News
Vendor -3		News & documentary shooting staff	Shooting staff verify the integrity of the recorded content including the integrity of C2PA metadata after a recording has been made and also when it is copied to a mobile PC for subsequent editing or delivery to the production site.	Detect and alert unexpected data corruption of the media content and embedded C2PA metadata in the camera or on a mobile PC before distributing the file.		Verify provenance - Before distribution	Shooting staff	Acquisition Documentary News
Vendor -4		News & documentary shooting staff (on-site editing)	Shooting staff select required parts of the recorded material and edit them as needed using the camera or on a mobile PC. Adjustments are made such as adding OK/NG (Good/Bad) file integrity rating and camera rotation information for each recorded file, and the output file is prepared for delivery.	Inherit the provenance information of the original file, add new provenance, and re-sign and embed it in the output file. Ability to exclude OK/NG file integrity rating information from the hash target. Ability to reuse the hash value of the original material to speed up processing, especially when re-encoding is not performed during rough editing		Add provenance Exclude OK/NG from hash target Ability to reuse the hash value of the original material	Shooting staff On-site editing	On-site News Documentary

© SMPTE 2026 – All Rights Reserved

Vendor -5		News & documentary shooting staff (distribution)	Shooting staff directly distribute or upload urgent or digest content from the shooting site to viewers.	Ability to convert the shooting material or roughly edited material to a distribution format such as MP4. During this process, it must inherit the provenance information of the original file, be able to add new provenance, re-sign and embed it, or delete irrelevant provenance information.		Convert to distribution format (such as MP4) Redact provenance Add provenance	Shooting staff	Distribution News Documentary
Vendor -6		News & documentary shooting staff (delivery)	Shooting staff write the shooting material or roughly edited material to memory media or send it to the station/production via network.	Deliver the shooting material safely and quickly.		Preserve provenance on delivery media	Shooting staff	Delivery
Vendor -7		Station/production staff (ingest)	Staff at the station/production site save the original file sent from the shooting site to the media asset server either as is or transcoded to the native format of the station.	Ability to verify the provenance information of the original file and warn if there are inconsistencies/ Ability to generate, sign, and embed new provenance information inheriting the original provenance information when transcoding.		Verify provenance Add provenance Preserve provenance when transcoding	Production staff	Ingest

© SMPTE 2026 – All Rights Reserved

Vendor -8		Station/production staff	Staff at the station/production site search, view, and retrieve files on the content server..	Ability to specify provenance information as a search condition. Ability to specify the integrity (verification OK/NG) of provenance information as a search condition Ability to trace provenance information to search for original or derived files Ability to display provenance information and verification results when viewing files. Ability to retrieve files while deleting irrelevant provenance information		Verify provenance Search provenance Specify integrity (OK/NG) of provenance information as a search condition Trace provenance information to search for original or derived files Display provenance information and verification results when viewing files Retrieve files while deleting irrelevant provenance information	Production staff	Production

© SMPTE 2026 – All Rights Reserved

Vendor -9		Station editor	Editing staff at the station/production combine and edit multiple files, outputting the result (final package) in the specified format. Typically, re-encoding is performed during output, so hard binding (hash value) cannot be inherited. However, if smart rendering is performed, the hash can be reused except near edit points.	Ability to verify and display the provenance of sources during editing. Ability to retain or delete the provenance information of the original sources as ingredients, depending on requirements. Ability to document the use of generative AI effects. Ability to add, sign, and embed the editing operations performed into the output file. Ability to generate MXF files using MP4 files as sources. Ability to generate MP4 files using MXF files as sources. Ability to record and confirm provenance information even when using materials across formats.		Verify and display provenance of sources during editing Retain or delete the provenance information of the original sources as ingredients, depending on requirements Document the use of generative AI effects. Add, sign, and embed the editing operations performed into the output file Generate MXF files using MP4 files as sources Generate MP4 files using MXF files as sources Record and confirm provenance information even when using materials across formats	Editing staff	Production
Vendor -10		Station/production staff (check final package)	Staff at the station/production receive and verify the delivered final package.	Ability to verify the provenance of the received final package and warn if there are inconsistencies.		Verify provenance	Package provider	Packaging

© SMPTE 2026 – All Rights Reserved

Vendor -11		Station/production staff (Transmission)	Staff at the station/production convert the final package video to a transmission/distribution format and transmit/distribute it.	Ability to inherit or delete the embedded provenance information of the final package as needed. Ability to add, sign, and embed necessary provenance information during transmission/distribution		Inherit provenance Redact provenance	Production staff Transmission	Distribution
Vendor -12		Archivist	Staff at the station/production studio save the final package as is or converted to an archive format. If there is a request to trace back to the original content of the archived material, and provenance has been deleted in previous processes (e.g., editing), it must be possible to access a file within the content management system that keeps a record of changes made to provenance information.	Ability to inherit or delete embedded provenance information of the final package as needed. Ability to add, sign, and embed necessary provenance information during archiving. Must be possible to access a file within the content management system that keeps a record of changes made to provenance information.		Inherit or delete embedded provenance information of the final package Sign, and embed necessary provenance information Access a file within the content management system that keeps a record of changes made to provenance information	Archivist	Archiving
Vendor -13		Viewer	Viewers watch the broadcast/distributed program. Since MXF is unlikely to be used in distribution, the confirmation of provenance during viewing is based on the provenance information contained within the broadcast/distribution format (e.g., MP4).	Confirmation of provenance is based on information contained within the broadcast/distribution format. Ability to perform and display verification levels 1-4 as described in Section 3 of the C2PA User Experience Guidance. (https://spec.c2pa.org/specifications/specifications/2.0/ux/UX_Recommendations.html#_Levels_of_information_disclosure)		Provenance information contained within the broadcast/distribution format Display provenance verification (level 1-4)	Viewer	Viewing

© SMPTE 2026 – All Rights Reserved

ANNEX B Demographic Survey Data

The following table contains an exhaustive and unabbreviated list of responses to two survey questions. These responses were used in abbreviated and summarized form in clause 4 of this report to discuss the demographics of survey responses. Identifiable information in the table was redacted using the character "♦" to address anonymity concerns.

What is your current role in media production or distribution workflows?	What types of media workflows are you involved in? (e.g., news, sports, entertainment, live events, post-production, archival)
I oversee Content Authenticity efforts for all of ♦♦♦♦♦♦, including digital video and audio products.	
Developing related technologies	N/A
Screens producer	Live events
Live/studio technical producer, occasional director, sometime broadcast engineer	News, sport, entertainment, live events.
Lead Distribution (Programmverbreitung)	Technical Distribution of all media types namely coding, packaging, provisioning to CDN as live and on demand
CTO	Live Sports Production, Film Production & Post, Broadcast and Cinema Content Delivery
VFX Supervisor, Cinematographer, consultant	Feature film, TV (episodic) , post production, visual effects, virtual production, immersive production
Director, Solutions & Sustainment	News
Director of Broadcast Engineering	News, as well as some ♦♦♦♦♦♦♦ network distribution
Researcher on forth coming media technologies that can boost creativity of filmmaking.	Film production.
Head of education.	General post-production.
AI Artist, Advocate, Educator, Community Builder	Investigative, entertainment, educational
Camera Maker	scenic productions, documentary, sports, entertainment, live events
Technical Director Media	Post production, archival, specialty media
Research and free lance writer, author	All above
We are manufacturers of acquisition, storage and transmission equipment	All of the ones mentioned above
♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦	♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦
Advisory	All forms of media workflows
Software Engineer	live events
Development of authenticity verification technology	News, Entertainment, Archival
Technical Director - I oversee digitization of legacy media formats (small gauge film, analog video) for the organization.	Archival & post-production
Software vendor	all
Working as VC technology- we are reseller and SI. Working in ♦♦♦♦♦ from past more than 28 years	Yes to all
Development of Authenticity Verification Technology	News, Entertainment, Archival,
Broadcast Engineer, System Integrations	Live events, post productions.
	We have the whole media value chain for all content types
R&D	everything
I make technology for encoding / decoding	All

© SMPTE 2026 – All Rights Reserved

Research and development works with colleagues in media production and distribution workflows, to identify ways to deliver value and efficiency with technology.	news, sports, entertainment, live events, post-production, archival, across multiple media types
CEO / Co-Founder, and in charge of dev and product.	sports, live, entertainment, news
Research and development	Cross-industry use-cases
Develop applications to enhance live streaming events	Live Events
Network Line Provider	(Mostly) live events
Product Manager	Sports, Entertainment, Live Events, Archival
CTO	all
Researcher	Research
R & D	Content protection
Management of post production facility	Post production supervisor
Development	Most
AVP Media Management	News, sports, entertainment, live events, post, archive
Material interchange department	News, Live events, post-production
R&D Director	movie distribution
Managing director	Entertainment, post production
I am the Director of RF and Transmission Engineering for ♦♦♦♦♦.	All of the above (news, sports, entertainment, live events, post-production, archival) as well as Motion Pictures and Streaming (VOD, SVOD, FAST).
advisor and tester	sports, entertainment, post production
Director, Media Processing and Production Technology	Post Production, archival
software developer	distribution
Audio Specialist on CoE of Media Solution	news, sports news, sports, entertainment, live events, production and post-production
Setting standards and best practices.	Scripted film and TV.
none	none
Sr Director Studio Engineering	Sports
I am not involved in Production or distribution but Building and Manufacturing.	Cinema
Television broadcaster and News/local programming generation, web/OTT programming distribution	News, sports, local variety, Fox network distribution broadcasting, syndicated programming
Ingest and Playout servers	All of them
Director of production system architecture	all ♦♦♦♦♦♦♦♦ workflows
Supplier of video compression software	Any
Content Production and technical engineering	From classic television to social media
Developer	Production, QC
The role of research and development of new technologies within the overall production and distribution business.	News, Sports, Entertainment, Live Events, Post-Production, Archives, Advertising Operations, Monetization
Research and development, broadcasting technology standardization.	News, sports, entertainment, live events, post-production, archival, live broadcasting/streaming
Colorist/Engineer	POST-PRODUCTION

© SMPTE 2026 – All Rights Reserved

I had been working in a broadcaster, and involving in content production and distribution, and I also had participated in standardization activity. After that I have been researching in those fields in a university.	research and development
Research and development of technologies to address dis/misinformation in media production and distribution workflows including prototype development based on the C2PA specifications and feasibility studies.	N/A
I design and supervise these workflows for mine and other entities.	Production and post for mid-high end feature films.
Public service broadcaster – providing engineering, technical operations, and workflow management across newsroom, live production, sports, and archival operations	news, live events , arrival, sports
Head of Competence Center Production & Infrastructure	all of them, but more an a consulting-style rather than operational level
As a member of the technical division, I am involved in the end-to-end workflow for program production across all genres covering the acquisition of video materials, editing, metadata management, playout, and archiving.	• News • Entertainment • Live events (election coverage, sports broadcasts, etc.) • Post-production • Archiving
NICT does not have any role in media production nor distribution workflows. However, NICT have a role of research and development in media processing.	NICT does not involved in the content workflows.
Tv director	In all chains of production
Formulation of facility planning, creation of specifications for procurement, and their installation and maintenance Construction of optimization for program production workflow	All (news, sports, entertainment, live events, post-production, archival)
News Gathering , Editing , Media Exchange	news
Supervisor	Live News
VP, Enterprise Metadata Management	news, entertainment, live
Broadcast ♦♦♦♦, Post Sound Supervisor and Recording Mixer. Senior Architect, System and Workflow design.	all of the above.
None	None
System Support	post-production, Shooting, CGI
Engineer	POST-PRODUCTION
Product Director	Delivery of our programming to broadcast, smart TVs, streaming apps, and across the internet.
OB Engineer	sports and live productions
Media Engineer	Streaming
Video standards conversion	All of the above: news, sports, entertainment, live events, post-production, archival
Mastering and encoding	Post-production
Engineering	Production (education), post-production, live events
Watermark embedding and detection	Post-production; linear broadcast; media asset creation and distribution.
ENGINEER	POST-PRODUCTION
Establishing International Standards	Cinema
researcher	post production ,archival
I am involved in archiving and preservation of current and historic content digitization and preservation from physical media recordings.	Archiving and preservation of current and historic content digitization and preservation from physical media recordings. Post-archival workflows to reuse archived content for new distribution channels beyond the initial release period(s).

© SMPTE 2026 – All Rights Reserved

Applications developer	Cinema, other long-form
Head Outside Production Radio Consultant C2PA	live, events
Preservation and archiving	archival
Project Manager and Engineer	all kind of workflows in media production for tv, radio and online
streaming solutions manager	news, sports, entertainment, live events, archival
Researcher	Technologie and Innovation
Trend scout & System Engineer	news & sports
We collect and receive media from creators for long-term preservation and access.	Archival and Live Events
Lead Architect	
media production	post-production
SVP Engineering	Sports, live events, post, archival
system integration for programmed production	any genre
Producer and involved in all tech workflow decisions	local News editorial, podcast, post-production
Content provenance	
Composer/Post Production Audio	Entertainment, Film/TV
Post Production Executive	Post production
Consultant	Live sports, live events, entertainment
System integration of programmed production	any genre of tv programmed
Technology Development	All of the above. Focus on breaking news - where users need access to archives and shared content
Contractor Post Production	
Director, Advanced Content Production	Sports, Entertainment, Live Events, Post Production
Team lead of the team responsible for the QC of all AS-11 deliveries for ♦♦♦♦♦♦♦ and playout	Qc, short eyeball and delivery
Research	archival

ANNEX C Example Categories for Manipulated or Tampered Content

This annex provides an informative classification framework for media content that has been fabricated, altered, manipulated, or otherwise modified in a manner that may affect its authenticity, integrity, provenance, or trustworthiness. The framework distinguishes between modifications to media content, contextual information, and provenance-related metadata.

The categories are intended to support consistent description and analysis of media manipulation techniques. They are not mutually exclusive, and a single media asset may be associated with multiple categories. The classification does not imply intent, legality, or severity, but rather provides a common vocabulary for discussing media authenticity and provenance.

These categories could be extended as technology evolves.

© SMPTE 2026 – All Rights Reserved

1. Fabricated Content

Content that never existed and was entirely created artificially.

Examples

- AI-generated images
- AI-generated video
- Synthetic voices
- Fully generated news reports

2. Impersonation / Identity Manipulation

Content designed to make someone appear to say or do something they never did.

Examples

- Face swaps
- Voice cloning
- Lip-sync manipulation
- Avatar-based impersonation

3. Altered Content

Authentic content that has been modified.

Examples

- Nonexistent picture/sound object insertion
- Existing picture/sound object removal
- Background picture/sound replacement
- Image retouching
- Audio restoration/mixing
- Edited audio/video sequences
- Unfounded colorization
- Unfounded upscaling

4. Context Manipulation

Authentic media presented in a misleading context.

© SMPTE 2026 – All Rights Reserved

Examples

- Real photo/video with false caption/subtitle
- Old footage presented as current
- Newly created footage used in historical context
- Correct image/sound attributed to the wrong event

This is often called a “cheap fake” or “shallowfake” when simple editing rather than AI is used. [mdpi.com], [cnti.org]

5. Composite / Spliced Content

Multiple authentic or synthetic sources combined into one asset.

Examples

- Combining video from one source with audio from another
- Photomontages
- Audio mixing
- AI-assisted composites

6. Evidence Suppression or Concealment

Modification intended to hide information.

Examples

- Redaction of individuals
- Removal of logos or metadata
- Cropping out evidence
- Deleting sections of audio/video
- De-colorization
- downscaling/blurring

7. Misleading Transformation

The original content remains recognizable, but characteristics are changed.

Examples

- Speeding up or slowing down speech
- Voice over
- Color manipulation

© SMPTE 2026 – All Rights Reserved

- Selective video editing without context
- Re-ordering video clips

8. Metadata / Provenance Tampering

The media itself may remain untouched, but authenticity information is manipulated.

Examples

- Removal of C2PA manifests
- Modified timestamps
- Modified geographic info
- Forged creator identity
- Forged signer identity
- Altered EXIF metadata

This category is particularly relevant to provenance systems and soft-binding discussions. It concerns attacks on the trust chain rather than the media essence itself.

© SMPTE 2026 – All Rights Reserved