TECHNICAL REPORT ON AI AND MULTIMEDIA AUTHENTICITY STANDARDS

MAPPING THE STANDARDISATION LANDSCAPE

TECHNICAL PAPER
Edition 2

IEC ISO ITU

TABLE OF CONTENTS

Executive Summary 05

AI and Multimedia Authenticity Standards Collaboration (AMAS) 05

1 Introduction 06

1.1 Methodology

2 Categories of Standards 07

2.1 Content Provenance
2.2 Trust and Authenticity
2.3 Asset Identifiers
2.4 Rights Declarations
2.4.1 General Purpose
2.4.2 Opt-Out Mechanisms
2.5 Watermarking

3 Overview of Specifications 09

3.1 Content Credentials
3.2 JPEG Trust Part 1: Core foundation
3.3 JPEG Trust Part 2: Trust profiles catalogue
3.4 JPEG Trust Part 3: Media asset watermarking
3.5 CAWG Metadata
3.6 Originator Profile
3.7 Overview of trustworthiness in artificial intelligence
3.8 Framework for trust-based media services
3.9 Trust.txt
3.10 Chromium Reputation Provider Framework
3.11 ISCC: International Standard Content Code (ISCC)
3.12 Global Media Identifier (GMI)
3.13 TDM Reservation Protocol
3.14 Robots Exclusion Protocol (Robots.txt)
3.15 Vocabulary for Expressing Content Preferences for AI
3.16 Open Binding of Content Identifiers (OBID)
3.17 X.ig-dw: Implementation guidelines for digital watermarking
3.18 DRM technology for digital publications Part 1: Overview of copyright protection technologies in use in the publishing industry
3.19 IEEE Draft Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents
3.20 H.MMAUTH: Framework for authentication of multimedia content
3.21 H.274(V4): Versatile supplemental enhancement information messages for coded video bitstreams

3
3.22 H.VADS: Assessment criteria for video authenticity detection services
3.23 Credible Web
3.24 Technical and Governance Guidelines for Responsible Data Collection
3.25 Data Provenance Standards
3.26 IEEE Standard for Transparent Human and Machine Agency Identification
3.27 IPTC Photo Metadata Standard
3.28 DASH - Part 4: Segment Encryption and Authentication
3.29 Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies
3.30 CAWG Identity Assertion Specification
3.31 W3C Verifiable Credentials Data Model v2.0
3.32 NIST AI 100-4: Reducing Risks Posed by Synthetic Content
3.33 MPEG-21 Part 3: Digital Item Identification
3.34 Cybersecurity technology—Labeling method for content generated by artificial intelligence
3.35 HSTP-MMAuth: Multimedia authentication framework, workflows and procedures
3.36 ITU-T Recommendation X.2210
3.37 Open Binding of Content Identifiers - Resilient Layer (OBID-R)
3.38 Descriptive Metadata Scheme for Identity and Integrity (DMS-II)
3.39 Descriptive Metadata Scheme for Identity and Integrity JUMBF approach
3.40 Journalism Trust Initiative

4 **Standardization Map** 23
4.1 Standards & Specification Map
4.2 Media Type Support Map

5 **Related Standards** 27
Blockchain and Distributed Ledger Technologies
Identity Standards
Rights Declarations
Creative Commons
Supply Chain Integrity, Transparency, and Trust

6 **Gap Analysis** 28

7 **Conclusion and next steps** 29

Annex A: Table of Standard & Specification Categorization 30

Annex B: Table of Media Type Support 33

EXECUTIVE SUMMARY

This technical paper is an update to the original version published in 2025. It provides a comprehensive overview of the current landscape of standards and specifications related to digital media authenticity and artificial intelligence. It categorizes these standards into five key clusters: content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking. The report provides a short description of each standard along with link for further details. It also identifies gaps in the ecosystem that still need standardization efforts.

By mapping the contributions of various Standard Development Organizations (SDOs) and groups, we aim to identify gaps and opportunities for further standardization. This could serve as a valuable resource for stakeholders seeking to navigate the complex ecosystem of standards at the intersection of artificial intelligence and authenticity in digital media and to implement best practices to safeguard the authenticity of digital assets and the rights assigned to them. The findings underscore the critical role of robust specifications and standards in fostering trust and accountability in the evolving digital landscape.

AI and Multimedia Authenticity Standards Collaboration (AMAS)

The AI and Multimedia Authenticity Standards Collaboration is a global initiative advancing standardization in the rapidly evolving field of AI-generated and altered media. By identifying gaps and driving the development of new standards, we support transparent, privacy-conscious, and rights-respecting practices. Our work also aims at informing policy and regulatory frameworks to promote legal compliance and safeguard public trust.

Led by the World Standards Cooperation, the collaboration serves as a vital forum for dialogue among standards developers, civil society organizations, technology companies, and other key players.

Convened by ITU under the auspices of the World Standards Cooperation, the collaboration was launched at the AI for Good Global Summit in 2024.

Learn more at **https://aiforgood.itu.int/multimedia-authenticity/**, including a full list of members, or contact the Secretariat at **amas-secretariat@itu.int**

Section **01**

INTRODUCTION

This technical paper provides a comprehensive overview of various standards and specifications related to digital media, focusing on content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking. These standards are essential for ensuring the authenticity of both synthetic and non-synthetic digital content. As generative AI continues to evolve, the need for robust standards becomes increasingly critical to protect the interests of creators, consumers, and organizations.

This technical report also contains a gap analysis categorized into governance, access, technical performance, and societal impact.

The standards discussed in this report are developed by various Standard Development Organizations (SDOs) and groups, each contributing to different aspects of AI and authenticity. By adhering to these guidelines, individuals and organizations can better maintain the trustworthiness and provenance of their digital assets, ensuring that content remains authentic and traceable throughout its lifecycle.

1.1 Methodology

The approach taken in this report involves a thorough review of known existing standards and specifications related to digital media. The focus was on identifying key areas where standards already exist, and from that, what might still be needed to support the authenticity and integrity of digital content. From that review, we have broken this report into the following categories: content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking.

In addition to the above, sessions were organized during AI for Good Summit 2025 and AI Standards Summit 2025 during which stakeholders were consulted. This resulted in a gap analysis of the landscape of the current ongoing standardization efforts and their challenges.

Section **02**

CATEGORIES OF STANDARDS

In this technical paper, we have clustered those standards and specifications in the scope of this analysis into five categories: content provenance, trust and authenticity, asset identifiers, rights declaration and watermarking. Rights declaration, in turn, is defined in two inclinations: general purpose and opt-out mechanisms. The general-purpose rights declaration addresses a broad scope while the opt-out mechanisms refer to a specific aspect of rights declaration that is of relevance to the scope of this document.

2.1 Content Provenance

Content provenance refers to information on the origin, history, and lifecycle of digital content. This is an important tool for the verification of the authenticity and integrity of digital assets. Provenance information helps in storing information about the creation, modification, and distribution of content, providing a transparent record that can be used to establish trust and authenticity. This is particularly important in use cases and applications where the authenticity and accountability of content is paramount, such as in journalism, scientific research, and digital art.

2.2 Trust and Authenticity

Trust and authenticity represent methodologies for ensuring that digital content is genuine and has not been tampered with. Such mechanisms are essential for maintaining the integrity of digital media, especially in environments where content manipulation is a significant concern. By implementing trust and authenticity measures, individuals and organizations can protect their digital assets from unauthorized alterations and help ensure that consumers can rely on the content they receive.

2.3 Asset Identifiers

Asset identifiers are unique codes assigned to digital content to ensure proper management and identification of the asset. These identifiers help in maintaining a clear and organized record of digital assets, making it easier to organize, manage and distribute content. By using asset identifiers, individuals and organizations can ensure that their digital media is properly tracked and accounted for, reducing the risk of loss or unauthorized use.

2.4 Rights Declarations

2.4.1 General Purpose

Rights declarations are formal statements that outline the rights and permissions associated with digital content. These declarations help in clarifying the ownership and usage rights of digital assets, providing a clear framework for how content can be used and shared. By establishing clear rights declarations, individuals and organizations can protect their intellectual property and ensure that their digital assets are used in accordance with their intended purpose.

2.4.2 Opt-Out Mechanisms

Opt-out mechanisms are a specialized approach to rights declarations that allow users to exclude their content from certain processes, such as data mining or AI training. These mechanisms are essential for protecting the privacy and rights of content creators, ensuring that their digital assets are not used without their consent. By implementing opt-out mechanisms, organizations can provide users with greater control over their content and ensure that their rights are respected.

2.5 Watermarking

Watermarking ensures that digital content is marked in a way that can be used to verify its authenticity, synthetic (or not) nature, and ownership. Watermarking is increasingly used to facilitate the declaration of the rights of content creators and to help ensure that their digital assets are not used without their consent. By implementing watermarking measures, organizations can provide users with greater control over their content and make sure that their rights are respected.

Section **03**

OVERVIEW OF SPECIFICATIONS

3.1 Content Credentials

- **SDO/Group:** C2PA
- **Link:** C2PA Specification
- **Status:** Published
- **Publication Date:** 2026
- **Media:** Any

Summary: This standard focuses on providing a tamper-evident provenance record, called a Content Credential, that can be embedded into digital media, watermarked or stored online. A Content Credential can include information about the creator, creation date, and any modifications made to the content. This helps in maintaining a verifiable record of the content's history.

3.2 JPEG Trust Part 1: Core foundation

- **SDO/Group:** ISO/IEC JTC 1/SC 29/ WG 1
- **Link:** ISO 21617-1:2025, second edition in progress
- **Status:** Published
- **Publication Date:** 2025
- **Media:** Any (image focused)

Summary: This standard focuses on trust and authenticity in JPEG images through provenance, detection and fact-checking. It provides a framework for embedding metadata directly into JPEG files in the form of trust indicators. This allows users to decide the degree of trust they can put on a digital asset as a function of their trust profiles. This is particularly useful in contexts where image manipulation is common, such as in social media applications.

3.3 JPEG Trust Part 2: Trust profiles catalog

- **SDO/Group:** ISO/IEC JTC 1/SC 29/ WG 1
- **Link:** ISO 21617-2
- **Status:** In progress
- **Media:** Any (image focused)

Summary: This standard introduces a series of trust profile snippets that can be used either as is or as starting points to establish profiles for use in specific workflows, use cases and applications such as broadcasting, digital cameras, AI-powered content generation services, etc.

3.4 JPEG Trust Part 3: Media asset watermarking

- **SDO/Group:** ISO/IEC JTC 1/ SC 29/ WG 1
- **Link:** ISO 21617-3
- **Status:** In Progress
- **Media Types:** Images

Summary: This standard is planned to provide an overview of mechanisms used for watermarking of media assets.

3.5 CAWG Metadata

- **SDO/Group:** Creation Assertions Working Group, as part of DIF
- **Link:** CAWG Metadata
- **Status:** Published
- **Publication Date:** 2025
- **Media Types:** Any

Summary: This specification provides a framework for expressing metadata that captures detailed information about the content, including ownership and authorship.

3.6 Originator Profile

- **SDO/Group:** Originator Profile
- **Link:** Originator Profile
- **Status:** In progress
- **Media:** Web pages

Summary: This specification provides a framework for documenting the origin of digital content. It includes guidelines for creating and maintaining profiles that capture detailed information about the content's creator and its creation process. This helps in establishing a clear and verifiable record of the content's provenance.

3.7 Overview of trustworthiness in artificial intelligence

- **SDO/Group:** ISO/IEC JTC 1/SC 42
- **Link:** ISO/IEC TR 24028:2020
- **Status:** Published
- **Publication Date:** 2020

Summary: This standard offers an overview of trustworthiness in artificial intelligence. It provides guidelines for assessing the reliability and integrity of AI systems, ensuring that they produce trustworthy results. This is crucial in applications where AI is used to generate or manipulate digital content, as it helps in maintaining the authenticity of the output.

3.8 Framework for trust-based media services

- **SDO/Group:** ITU-T
- **Link:** ITU-T Y.3054
- **Status:** Published
- **Publication Date:** 2018

Summary: is framework provides guidelines for trust-based media services. In particular, it includes methods for establishing and maintaining trust in digital media platforms, ensuring that users can rely on the content they access. This is particularly important in contexts where media services are used to distribute sensitive or high-value content.

3.9 Trust.txt

- **SDO/Group:** JournalList
- **Link:** Trust.txt
- **Status:** Initiated
- **Media:** Web pages

Summary: This specification outlines methods for establishing trust in digital content. It includes guidelines for creating and maintaining trust.txt files, which can be used to document the trustworthiness of digital assets. This helps in ensuring that users can verify the authenticity of the content they receive.

3.10 Chromium Reputation Provider Framework

- **SDO/Group:** Google's Chrome Team
- **Link:** Chromium Reputation Provider Framework
- **Status:** Initiated
- **Media:** Web pages

Summary: This framework provides guidelines for reputation management of digital content. It includes methods for assessing and maintaining the reputation of digital assets, ensuring that users can trust the content they access. This is particularly important in contexts where reputation is a key factor in determining the value and reliability of digital media.

3.11 ISCC: International Standard Content Code (ISCC)

- **SDO/Group:** ISO/TC 46/SC 9
- **Link:** ISO 24138
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Any

Summary: This standard provides a unique identifier for digital content. It includes guidelines for creating and maintaining ISCC codes, which can be used to track and manage digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.12 Global Media Identifier (GMI)

- **SDO/Group:** IWA 44
- **Link:** GMI
- **Status:** Published
- **Publication Date:** 2025
- **Media:** Any

Summary: This specification offers a unique identifier for media content. It includes methods for creating and maintaining GMI codes, which can be used to track and manage media assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.13 TDM Reservation Protocol

- **SDO/Group:** W3C
- **Link:** TDMRep
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Web pages, EPub, PDF

Summary: This protocol provides guidelines for reserving content from text and data mining. It includes methods for creating and maintaining TDMRep files, which can be used to document the reservation of digital assets. This helps in ensuring that content is not used for data mining without the creator's consent.

3.14 Robots Exclusion Protocol (Robots.txt)

- **SDO/Group:** IETF
- **Link:** RFC 9309
- **Status:** Published
- **Media:** Any

Summary: This standard provides guidelines for excluding content from web crawlers. It includes methods for creating and maintaining robots.txt files, which can be used to document the exclusion of digital assets. This helps in ensuring that content is not accessed by web crawlers without the creator's consent.

3.15 Vocabulary for Expressing Content Preferences for AI

- **SDO/Group:** IETF
- **Link:** draft-ietf-aipref-vocab-06
- **Status:** In progress
- **Media:** Any

Summary: This document proposes a standardized vocabulary of use cases that can be targeted when expressing machine-readable opt-outs related to Text and Data Mining (TDM) and AI training. The vocabulary is agnostic to specific opt-out mechanisms and enables declaring parties to communicate restrictions or permissions regarding the use of their digital assets in a structured and interoperable manner.

3.16 Open Binding of Content Identifiers (OBID)

- **SDO/Group:** SMPTE
- **Link:** SMPTE ST 2112-10:2020
- **Status:** Published
- **Publication Date:** 2020
- **Media:** Audio

Summary: This standard provides guidelines for binding content identifiers to digital media. It includes methods for creating and maintaining OBID files, which can be used to document the binding of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.17 X.ig-dw: Implementation guidelines for digital watermarking

- **SDO/Group:** ITU-T SG17
- **Link:** SG17-TD42/WP4
- **Status:** Published, but temporary
- **Publication Date:** 2024
- **Media:** Images, Video

Summary: This guideline offers methods for implementing digital watermarking. It includes guidelines for creating and maintaining watermark files, which can be used to document the watermarking of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.18 DRM technology for digital publications Part 1: Overview of copyright protection technologies in use in the publishing industry

- **SDO/Group:** ISO/IEC JTC 1/SC 34
- **Link:** ISO/IEC 23078-1:2024
- **Status:** Published
- **Publication Date:** 2024
- **Media:** EPub, PDF

Summary: This standard provides an overview of DRM technologies for digital publications. It includes guidelines for creating and maintaining DRM files, which can be used to document the DRM of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.19 IEEE Draft Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents

- **SDO/Group:** IEEE
- **Link:** IEEE P3361
- **Status:** In progress
- **Media:** Any

Summary: This draft standard offers methods for evaluating the robustness of digital watermarking. It includes guidelines for creating and maintaining evaluation files, which can be used to document the evaluation of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.20 H.MMAUTH: Framework for authentication of multimedia content

- **SDO/Group:** ITU-T SG21/Q9
- **Link:** H.MMAUTH
- **Status:** In progress
- **Media:** Video

Summary: This Draft Recommendation specifies a technical solution for the verification of multimedia content integrity, enabling users to confirm the authenticity of the content by its creators, such as governments, companies, or news organizations. The solution is based on the digital signing of data streams. The content creator (encoder) uses a private key to sign the content, while the recipient (decoder) uses a corresponding public key to verify the authenticity. The public key, necessary for verification, is not derived directly from the data stream but is obtained through a trusted, independent method, such as a third-party trust center.

3.21 H.274(V4): Versatile supplemental enhancement information messages for coded video bitstreams

- **SDO/Group:** JVET (ITU-T SG21 & ISO/IEC JTC 1/SC 29/ WG5)
- **Link:** H.274(V4)
- **Status:** In progress
- **Media:** Video

Summary: This specification contains changes to the versatile supplemental enhancement information messages for coded video bitstreams (VSEI) standard to specify additional SEI messages that will be useful for the purposes of content provenance, trust and authenticity.

3.22 H.VADS: Assessment criteria for video authenticity detection services

- **SDO/Group:** ITU-T SG21/Q7
- **Link:** H.VADS
- **Status:** In progress
- **Media:** Video

Summary: This Draft Recommendation provides a comprehensive assessment framework for video authenticity detection services. It specifies the requirements, assessment categories, key metrics, and methods to evaluate the capabilities of video authenticity detection services. By establishing a structured, criteria-based approach, this Draft Recommendation would guide the development, evaluation, and selection of reliable and effective video authenticity detection services.

3.23 Credible Web

- **SDO/Group:** W3C
- **Link:** Cred Web
- **Status:** In progress
- **Media:** Web pages

Summary: The mission of the W3C Credible Web Community Group is to help shift the Web toward more trustworthy content without increasing censorship or social division. We want users to be able to tell when content is reliable, accurate, and shared in good faith, and to help them steer away from deceptive content. At the same time, we affirm the need for users to find the content they want and to interact freely in the communities they choose. To balance any conflict between these goals, we are committed to providing technologies which keep end-users in control of their Web experience.

3.24 Technical and Governance Guidelines for Responsible Data Collection

- **SDO/Group:** Alliance for Responsible Data Collection (ARDC)
- **Link:** Technical and Governance Guidelines for Responsible Data Collection
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Data

Summary: With the rapid expansion of online digital data, it is critical to establish responsible data collection standards that provide data collectors with guidance on best practices, provide third parties with a reliable means to assess whether the public web data they seek to use has been responsibly sourced, and protect public access to public data. The technical guidelines set forth below are part of a broader framework for responsible data collection that includes important guidelines for data collection governance. As such, all ARDC guidelines must be applied holistically. These standards build upon previous work by the FISD-SIA-Alternative Data Council on Web Data Collection Considerations.

3.25 Data Provenance Standards

- **SDO/Group:** Data & Trust Alliance
- **Link:** D&TA Data Provenance Standards v1.0.0
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Data

Summary: The Data Provenance Standards are a set of guidelines developed by the Data & Trust Alliance to help organizations assess dataset quality, transparency, and legal usability for AI and traditional data applications. The standards aim to provide essential metadata about a dataset's origin, creation method, and legal usage, with the goal of increasing data trust and reducing risks in AI development.

3.26 IEEE Standard for Transparent Human and Machine Agency Identification

- **SDO/Group:** IEEE
- **Link:** IEEE 3152-2024
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Images, Audio

Summary: This standard addresses recognizable audio and visual markers that assist humans in distinguishing communication with a human, a machine, or a combination of both. Therefore, the standard defines visual, textual, and auditory marks. This standard does not cover methods to determine whether an interaction is with a machine, such as Turing tests.

3.27 IPTC Photo Metadata Standard

- **SDO/Group:** IPTC
- **Link:** IPTC Photo Metadata Standard 2024.1
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Images, Video

Summary: This document specifies metadata properties with a focus on usage with photos, some of these properties are also specified by the IPTC Video Metadata Hub.

3.28 DASH - Part 4: Segment Encryption and Authentication

- **SDO/Group:** ISO/IEC JTC 1/SC 29
- **Link:** ISO/IEC 23009-4:2018
- **Status:** Published
- **Publication Date:** 2018
- **Media:** Video

Summary: This standard introduces encryption and authentication mechanisms at the segment level for adaptive video streaming, which enhances content integrity and protects against tampering during media transmission. It complements existing watermarking and trust/authenticity standards, especially for streaming use cases.

3.29 Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies

- **SDO/Group:** IEEE SA
- **Link:** P3429
- **Status:** Published
- **Publication Date:** 2023
- **Media:** Any

Summary: This recommended practice offers a structured framework for understanding and classifying Artificial Intelligence Generated Content (AIGC). It defines rules and levels of AIGC technologies, outlines recommended practices for their implementation, and provides real-world use cases. This standard is highly relevant to the trust and authenticity domain, as it supports transparent communication of the origin, nature, and reliability of AI-generated content—an increasingly critical aspect of digital media governance.

3.30 CAWG Identity Assertion Specification

- **SDO/Group:** Creation Assertions Working Group (DIF)
- **Link:** CAWG Identity Assertion v1.2
- **Status:** Published
- **Publication Date:** 2025
- **Media:** Any

Summary: This specification enables content creators to cryptographically bind their verified identity to C2PA-signed digital assets. It supports multiple identity binding methods including X.509 certificates and Identity Claim Aggregators (ICA). Ratified by the Decentralized Identity Foundation (DIF) on December 15, 2025, after CAWG formally became a DIF working group in March 2025. Directly extends and complements the C2PA Specification and CAWG Metadata specification.

3.31 W3C Verifiable Credentials Data Model v2.0

- **SDO/Group:** W3C
- **Link:** VC Data Model 2.0
- **Status:** Published
- **Publication Date:** 2025
- **Media:** Any

Summary: This W3C Recommendation (published May 15, 2025) provides a standard data model for cryptographically secure, privacy-respecting, machine-verifiable credentials. It is directly applicable to content authenticity workflows ‚Äì notably as the foundation for identity binding in CAWG Identity Assertions. The v2.0 family comprises seven interlocking specifications covering the data model, JSON-LD contexts, and securing mechanisms (ECDSA and BBS). Supersedes v1.1.

3.32 NIST AI 100-4: Reducing Risks Posed by Synthetic Content

- **SDO/Group:** NIST
- **Link:** NIST AI 100-4
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Images, Audio, Video, Any

Summary: This NIST technical report provides authoritative US government guidance on detecting, authenticating, and labeling AI-generated and synthetic content. It covers digital watermarking, metadata-based provenance, and content labeling approaches, with explicit interoperability references to C2PA and W3C PROV as recommended standards. Although a technical report rather than a normative standard, it carries significant influence on US policy and industry practice for AI content authenticity.

3.33 MPEG-21 Part 3: Digital Item Identification

- **SDO/Group:** ISO/IEC JTC 1/SC 29
- **Link:** IEEE 3152-2024
- **Status:** Published
- **Publication Date:** 2025
- **Media:** Any

Summary: This 2025 edition of MPEG-21 Part 3 replaces the original 2003 version and defines a framework for the unique identification of digital items and their components. It provides persistent, globally unique identifiers for digital content objects and is applicable across audio, video, images, and documents. Relevant to asset identifier workflows and interoperable with C2PA, ISCC, and GMI (IWA 44) identification schemes.

3.34 Cybersecurity technology—Labeling method for content generated by artificial intelligence

- **SDO/Group:** Chinese National Standard
- **Link:** GB 45438
- **Status:** Published
- **Publication Date:** 2025
- **Media:** Images, Audio, Video

Summary: This document defines the compulsory technical methods for explicit and implicit marking of AI-generated text, images, audio, and video.

3.35 HSTP-MMAuth: Multimedia authentication framework, workflows and procedures

- **SDO/Group:** ITU-T SG21
- **Link:** HSTP-MMAuth
- **Status:** In Progress
- **Media:** Video

Summary: This report will provide an end-to-end framework for multimedia authentication for various use cases such as broadcast, broadband distributions and live/low latency/on-demand streaming, real-time communication, ingesting the content for production and consumption by professional and public consumers. The framework will describe the workflows for various use cases, the role of each actor and entity, the interface requirement between various entities, and the requirements for each entity's functionalities and features.

3.36 ITU-T Recommendation X.2210

- **SDO/Group:** ITU-T SG17
- **Link:** SG17-TD308/WP4
- **Status:** In Progress
- **Media:** Images, Video

Summary: This Recommendation provides guidelines for implementation of digital watermarking through a detailed methodology approach, including watermark preparation, embedding, distribution, and extraction. It targets a wide range of digital content carriers, including images, videos, files, and emerging artificial intelligence (AI) generated content.

3.37 Open Binding of Content Identifiers - Resilient Layer (OBID-R)

- **SDO/Group:** SMPTE
- **Link:** SMPTE ST 2112-30:20xx
- **Status:** Initiated
- **Media:** Audio

Summary: This standard provides guidelines for binding content identifiers to digital media. It includes methods for creating and maintaining OBID files, which can be used to document the binding of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.38 Descriptive Metadata Scheme for Identity and Integrity (DMS-II)

- **SDO/Group:** SMPTE
- **Link:** SMPTE ST 2140-1:20xx
- **Status:** In Progress
- **Media:** Audio, Video, Data

Summary: The DMS-II develops and documents an architecture, a data model and a detailed specification to carry Identity and Integrity metadata in SMPTE ST 377 Material Exchange Format (MXF) files using the SMPTE ST 336 KLV Protocol. The specification for bindings will address the MXF media structures including I frame and long GOP media, as well as Framewrapped, Clipwrapped and Partitioned files.

3.39 Descriptive Metadata Scheme for Identity and Integrity JUMBF approach

- **SDO/Group:** SMPTE
- **Link:** SMPTE ST 2140-3:20xx
- **Status:** In Progress
- **Media:** Audio, Video, Data

Summary: This document defines the specifications for applying the JPEG Universal Metadata Box Format (JUMBF) data model for metadata to be carried in professional media files with reference to the SMPTE ST 2140-1 conceptual architecture for Identity and Integrity.

3.40 Journalism Trust Initiative

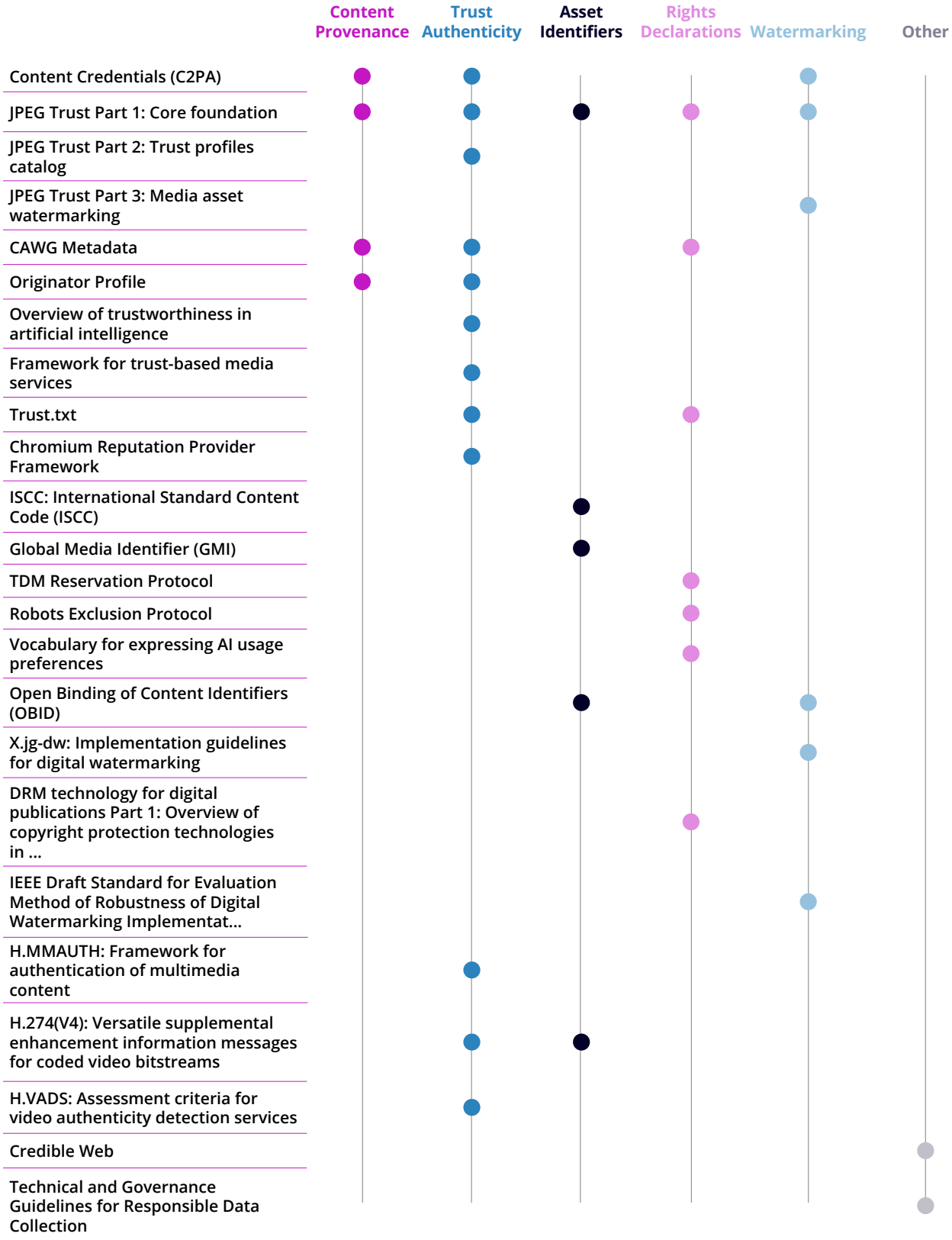
- **SDO/Group:** CEN-CENELEC
- **Link:** CWA 17493 WORKSHOP AGREEMENT
- **Status:** Published
- **Publication Date:** 2019
- **Media:** Any

Summary: This standard introduces a benchmark applicable to any type of news media outlets (television, radio, print and digital) to assess their efforts in terms of transparency, governance, editorial processes and responsibility policies, including in the usage of AI.

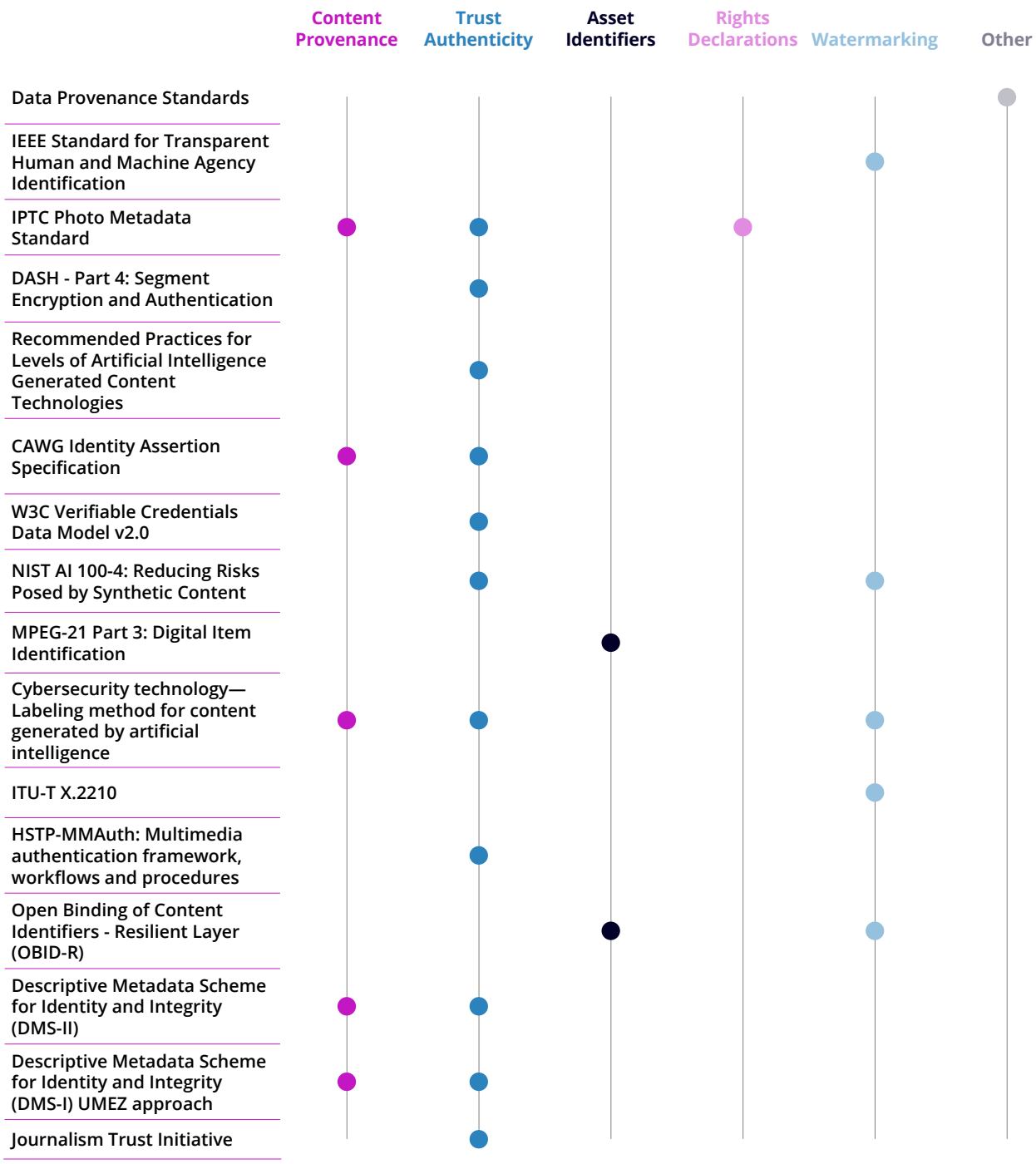
Section **04**

STANDARDIZATION MAPPING

4.1 Standards & Specification Map



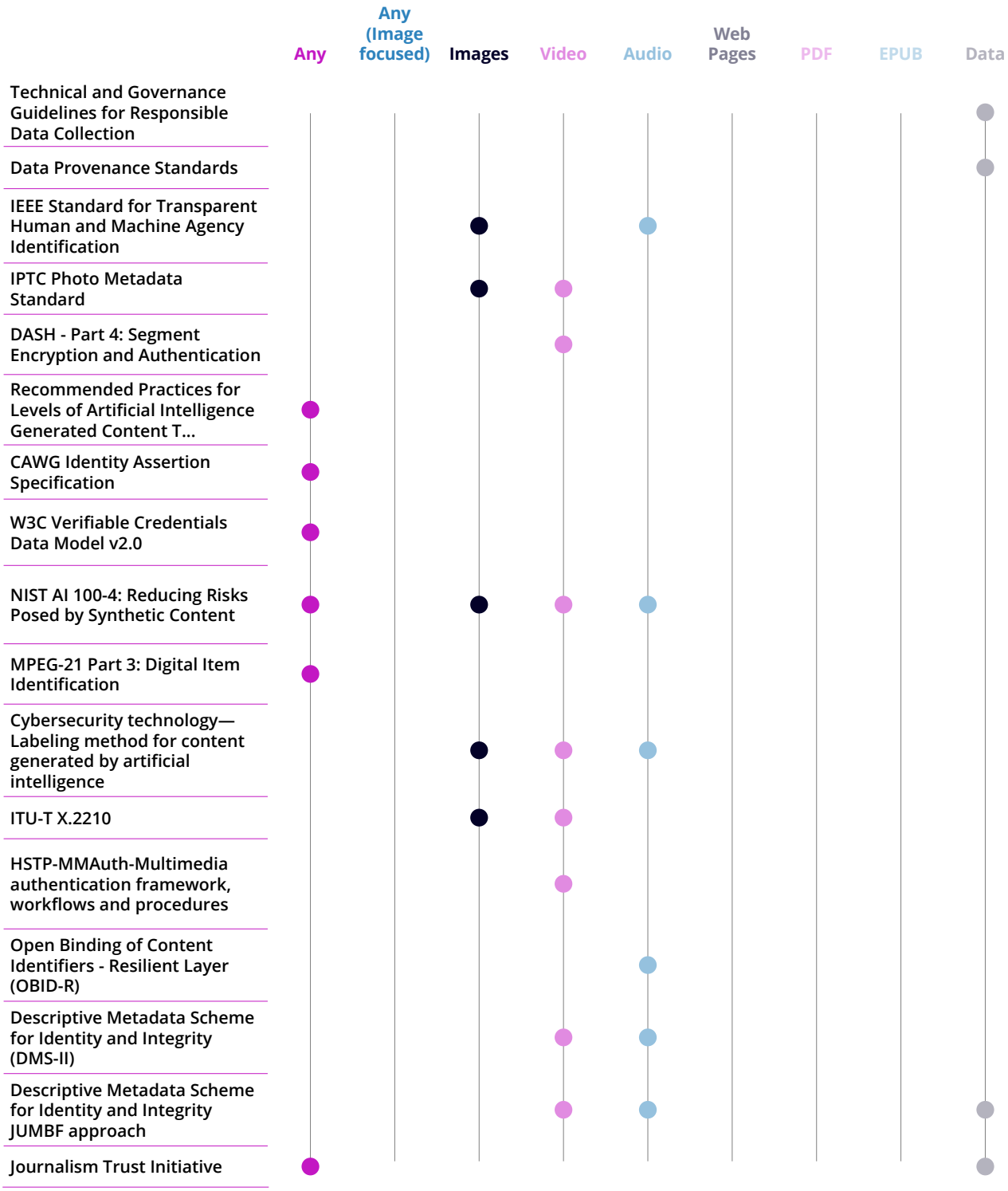
4.1 Standards & Specification Map (cont'd)



For an accessible table representation of this chart, see Annex A: Table of Standard & Specification Categorization.

4.2 Media Type Support Map

4.2 Media Type Support Map (cont'd)



For an accessible table representation of this chart, see Annex B: Table of Media Type Support.

Section **05**

RELATED STANDARDS

In addition to the core standards discussed in this report, several related areas of standardization play a significant role in supporting digital media authenticity. These standards address foundational technologies and practices that complement the main categories of content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking.

Blockchain and Distributed Ledger Technologies

Blockchain and Distributed Ledger Technologies (DLT) provide a well-established approach to decentralized, tamper-evident ledgers that can be used to record information about the provenance and integrity of digital assets. By leveraging cryptographic techniques, these technologies enable transparent and immutable records of content creation, modification, and transfer. Standards such as those from ISO TC 307 (Blockchain and distributed ledger technologies) and the W3C (e.g., Verifiable Credentials and DIDs) are increasingly referenced in digital media workflows.

Identity Standards

Robust digital identity standards are essential for establishing the authenticity of content creators, both human and organizational. Efforts emanating from organizations such as the Decentralized Identity Foundation (DIF) and its Creator Assertion Working Group (CAWG, https://cawg.io/identity/1.1/) allow for secure and privacy-preserving identification while enabling features such as attribution of digital assets.

Rights Declarations

It is important to establish a flexible, machine-readable framework for expressing permissions, prohibitions, and obligations associated with digital content. Standards such as the Open Digital Rights Language (ODRL), standardized by the W3C, enable rights holders to specify how their content may be used, shared, or restricted, supporting automated rights management and compliance across diverse platforms and services.

Creative Commons

Creative Commons (CC) licenses are widely adopted for the standardized declaration of usage rights for digital content. The CC framework provides a suite of licenses that allow creators to communicate permissions and restrictions in a clear, interoperable manner.

Supply Chain Integrity, Transparency, and Trust

Supply Chain Integrity, Transparency, and Trust (SCITT) is an emerging initiative led by the IETF, focuses on establishing standards for the secure and transparent tracking of digital assets throughout their lifecycle. SCITT aims to provide mechanisms for recording, verifying, and auditing actions taken on digital content, enhancing supply chain integrity and supporting trust in digital ecosystems. This is particularly relevant for complex media workflows involving multiple stakeholders and distribution channels.

Section **06**

GAP ANALYSIS

The standards landscape faces systemic challenges that hinder their efficacy, adoption, and societal alignment. These challenges and gaps can be categorized into governance, access, technical performance, and societal impact. High barriers to entry and non-transparent decision-making processes marginalize diverse stakeholders, while fragmented, paywalled, and IP-encumbered standards complicate implementation for SMEs and researchers. As these standards are adopted, especially at scale, they can struggle with adaptive threats, end-to-end lifecycle security, and consistent privacy protections.

The slow pace of traditional standardization fails to keep up with the rapid evolution of AI technology, leading to fragmented industry solutions. Bridging these gaps requires a move toward agile, open-access, and rights-respecting standards that include sector-specific implementation profiles and rigorous, standardized performance metrics.

Section **07**

CONCLUSION AND NEXT STEPS

Through the categorization of these existing specifications and standards into key areas, we have highlighted their critical role in fostering trust, accountability, and integrity in the digital ecosystem. The findings underscore the importance of continued collaboration among Standard Development Organizations (SDOs), industry stakeholders, and researchers to address existing gaps and emerging challenges.

As next steps, it is essential to focus on the harmonization of overlapping standards and the development of interoperable frameworks that can be widely adopted across industries. Emerging areas of work, such as the integration of decentralized technologies for enhanced provenance management and the exploration of new watermarking techniques for synthetic media, present exciting opportunities for innovation. Additionally, fostering awareness and adoption of these specifications and standards through education, advocacy, and pilot implementations will be crucial in ensuring their effectiveness and impact.

The evolving nature of digital media and AI technologies necessitates a proactive approach to standardization. By staying ahead of technological advancements and fostering a collaborative ecosystem, we can build a robust foundation for the authenticity and trustworthiness of digital content in the years to come.

ANNEX A: TABLE OF STANDARD & SPECIFICATION CATEGORIZATION

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
Content Credentials (C2PA)	X	X			X	
JPEG Trust Part 1: Core foundation	X	X	X	X	X	
JPEG Trust Part 2: Trust profiles catalog		X				
JPEG Trust Part 3: Media asset watermarking					X	
CAWG Metadata	X	X		X		
Originator Profile	X	X				
Overview of trustworthiness in artificial intelligence		X				
Framework for trust-based media services		X				
Trust.txt		X		X		
Chromium Reputation Provider Framework		X				
ISCC: International Standard Content Code (ISCC)			X			
Global Media Identifier (GMI)			X			
TDM Reservation Protocol				X		
Robots Exclusion Protocol				X		
Vocabulary for expressing AI usage preferences				X		
Open Binding of Content Identifiers (OBID)			X		X	
X.ig-dw: Implementation guidelines for digital watermarking					X	

ANNEX A: TABLE OF STANDARD & SPECIFICATION CATEGORIZATION (CONT'D)

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
DRM technology for digital publications						
Part 1: Overview of copyright protection technologies in use in the publishing industry				X		
IEEE Draft Standard for Evaluation Method of						
Robustness of Digital Watermarking Implementation in Digital Contents					X	
H.MMAUTH:						
Framework for authentication of multimedia content		X				
H.274(V4):						
Versatile supplemental enhancement information messages for coded video bitstreams		X				
H.VADS:						
Assessment criteria for video authenticity detection services		X				
Credible Web						X
Technical and Governance Guidelines for Responsible Data Collection						X
Data Provenance Standards						X
IEEE Standard for Transparent Human and Machine Agency Identification					X	
IPTC Photo Metadata Standard	X	X		X		

ANNEX A: TABLE OF STANDARD & SPECIFICATION CATEGORIZATION (CONT'D)

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
DASH - Part 4: Segment Encryption and Authentication		X				
Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies		X				
CAWG Identity Assertion Specification	X	X				
W3C Verifiable Credentials Data Model v2.0		X				
NIST AI 100-4: Reducing Risks Posed by Synthetic Content		X			X	
MPEG-21 Part 3: Digital Item Identification			X			
Cybersecurity technology—Labeling method for content generated by artificial intelligence	X	X			X	
ITU-T Recommendation X.2210					X	
HSTP-MMAuth: Multimedia authentication framework, workflows and procedures		X				
Open Binding of Content Identifiers - Resilient Layer (OBID-R)			X		X	
Descriptive Metadata Scheme for Identity and Integrity (DMS-II)	X	X				
Descriptive Metadata Scheme for Identity and Integrity JUMBF approach	X	X				
Journalism Trust Initiative		X				

ANNEX B: TABLE OF MEDIA TYPE SUPPORT

Standard	Audio	Data	EPUB	Images	PDF	Video	Web pages	Others
Content Credentials (C2PA)	X	X	X	X	X	X	X	X
JPEG Trust Part 1: Core foundation	X	X	X	X	X	X	X	X
JPEG Trust Part 2: Trust profiles catalog	X	X	X	X	X	X	X	X
JPEG Trust Part 3: Media asset watermarking				X				
CAWG Metadata	X	X	X	X	X	X	X	X
Originator Profile							X	
Overview of trustworthiness in artificial intelligence								
Framework for trust-based media services								
Trust.txt							X	
Chromium Reputation Provider Framework							X	
ISCC: International Standard Content Code (ISCC)	X	X	X	X	X	X	X	X
Global Media Identifier (GMI)	X	X	X	X	X	X	X	X
TDM Reservation Protocol			X		X		X	
Robots Exclusion Protocol	X	X	X	X	X	X	X	X
Vocabulary for expressing AI usage preferences	X	X	X	X	X	X	X	X
Open Binding of Content Identifiers (OBID)	X							

ANNEX B: TABLE OF MEDIA TYPE SUPPORT (CONT'D)

Standard	Audio	Data	EPUB	Images	PDF	Video	Web pages	Others
X.ig-dw: Implementation guidelines for digital watermarking				X		X		
DRM technology for digital publications								
Part 1: Overview of copyright protection technologies in use in the publishing industry			X		X			
IEEE Draft Standard for Evaluation Method of								
Robustness of Digital Watermarking Implementation in Digital Contents	X	X	X	X	X	X	X	X
H.MMAUTH:								
Framework for authentication of multimedia content						X		
H.274(V4):								
Versatile supplemental enhancement information messages for coded video bitstreams						X		
H.VADS:								
Assessment criteria for video authenticity detection services						X		
Credible Web							X	
Technical and Governance Guidelines for Responsible Data Collection		X						
Data Provenance Standards		X						
IEEE Standard for Transparent Human and Machine Agency Identification	X			X				
IPTC Photo Metadata Standard				X		X		

ANNEX B: TABLE OF MEDIA TYPE SUPPORT (CONT'D)

Standard	Audio	Data	EPUB	Images	PDF	Video	Web pages	Others
DASH - Part 4: Segment Encryption and Authentication						X		
Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies	X	X	X	X	X	X	X	X
CAWG Identity Assertion Specification	X	X	X	X	X	X	X	X
W3C Verifiable Credentials Data Model v2.0	X	X	X	X	X	X	X	X
NIST AI 100-4: Reducing Risks Posed by Synthetic Content	X	X	X	X	X	X	X	X
MPEG-21 Part 3: Digital Item Identification	X	X	X	X	X	X	X	X
Cybersecurity technology—Labeling method for content generated by artificial intelligence	X			X		X		
ITU-T Recommendation X.2210				X		X		
HSTP-MMAuth: Multimedia authentication framework, workflows and procedures						X		
Open Binding of Content Identifiers - Resilient Layer (OBID-R)	X							
Descriptive Metadata Scheme for Identity and Integrity (DMS-II)	X	X				X		
Descriptive Metadata Scheme for Identity and Integrity JUMBF approach	X	X				X		
Journalism Trust Initiative	X	X	X	X	X	X	X	X

ISBN 978-2-9702103-0-6