

Technical Report on AI and Multimedia Authenticity Standards *Mapping the standardisation landscape*

Version 1.0, 2025-04-28: Draft 0.4

Executive Summary

TBD

Table of Contents

Executive Summary	1
1. Introduction	4
1.1. About the AMAS initiative	4
1.2. Methodology	4
2. Categories of Standards	4
2.1. Content Provenance	4
2.2. Trust and Authenticity	5
2.3. Asset Identifiers	5
2.4. Rights Declarations	5
2.5. Watermarking	6
3. Overview of Specifications	6
3.1. Content Credentials (C2PA)	6
3.2. Content Credentials (ISO 22144)	6
3.3. JPEG Trust Part 1: Core foundation	6
3.4. JPEG Trust Part 2: Trust profiles catalogue	7
3.5. JPEG Trust Part 3: Media asset watermarking	7
3.6. CAWG Metadata	7
3.7. Originator Profile	7
3.8. PROV	8
3.9. Overview of trustworthiness in artificial intelligence	8
3.10. Framework for trust-based media services	8
3.11. Trust.txt	9
3.12. Chromium Reputation Provider Framework	9
3.13. International Standard Content Code (ISCC)	9
3.14. Unique Media Identifier (UMid)	9
3.15. TDM Reservation Protocol	10
3.16. Spawning ai.txt	10
3.17. Robots.txt	10
3.18. Vocabulary for Expressing Content Preferences for AI	11

3.19. Open Binding of Content Identifiers (OBID).....	11
3.20. X.ig-dw: Implementation Guidelines for Digital Watermarking	11
3.21. Specification of Digital Rights Management (DRM) Technology for Digital Publications	12
3.22. A Review of Medical Image Watermarking Requirements for Teleradiology	12
3.23. Evaluation Tools for Persistent Association Technologies.....	12
3.24. IEEE Draft Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents	13
4. Standardization Map.....	13
4.1. Overview	13
4.2. Graphical Representation	16
5. Conclusion and next steps.....	16

1. Introduction

This report provides a comprehensive overview of various standards and specifications related to digital media, focusing on content provenance, trust 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.

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, organizations can maintain the trustworthiness and provenance of their digital assets, ensuring that content remains authentic and traceable throughout its lifecycle.

1.1. About the AMAS initiative

TBD

1.2. Methodology

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

2. Categories of Standards

In this white 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 is in turn 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 right declaration that is of relevance to the scope of this document.

2.1. Content Provenance

Content provenance refers to information on the origin and history of digital content. This is an

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

2.2. Trust and Authenticity

Trust and authenticity measures ensure 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, organizations can protect their digital assets from unauthorized alterations and 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 their proper management and tracking. 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, 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, 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 and ownership. Watermarking is increasingly used to facilitate the declaration of the rights of content creators and ensuring 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.

3. Overview of Specifications

3.1. Content Credentials (C2PA)

- **SDO/Group:** C2PA
- **Link:** [C2PA Specification](#)
- **Status:** Published
- **Summary:** This standard provides guidelines for embedding content credentials in digital media to ensure provenance. It outlines methods for attaching metadata to digital assets, which 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. Content Credentials (ISO 22144)

- **SDO/Group:** ISO TC 171/SC 2
- **Link:** [ISO 22144](#)
- **Status:** In progress
- **Summary:** This ISO standard outlines methods for documenting content credentials to maintain provenance. It specifies the types of metadata that should be included and the formats for storing this information. By following these guidelines, organizations can ensure that their digital content is traceable and its authenticity can be verified.

3.3. JPEG Trust Part 1: Core foundation

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1 (JPEG)
- **Link:** [ISO/IEC 21617-1:2025, second edition in progress](#)
- **Status:** Published

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

3.4. JPEG Trust Part 2: Trust profiles catalogue

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1 (JPEG)
- **Status:** In Progress
- **Summary:** This standard introduces a series of Trust Profiles 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.

3.5. JPEG Trust Part 3: Media asset watermarking

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1 (JPEG)
- **Status:** Initiated
- **Summary:** This standard is planned to provide an overview of mechanisms used for watermarking of media assets.

3.6. CAWG Metadata

- **SDO/Group:** Creation Assertions Working Group, as part of DIF
- **Link:** [CAWG Metadata](#)
- **Status:** Published (new version in progress)
- **Summary:** This specification provides a framework for expressing metadata that captures detailed information about the content, including ownership and authorship.

3.7. Originator Profile

- **SDO/Group:** Originator Profile
- **Link:** [Originator Profile](#)
- **Status:** In progress

- **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.

3.8. PROV

- **SDO/Group:** Open Provenance
- **Link:** [PROV](#)
- **Status:** Published
- **Summary:** This standard offers a model for representing provenance information in digital content. It defines a set of concepts and relationships that can be used to describe the history of a digital asset, including its creation, modification, and distribution. This model can be applied across various types of digital content, providing a flexible and comprehensive approach to provenance documentation.

3.9. Overview of trustworthiness in artificial intelligence

- **SDO/Group:** ISO/IEC JTC 1/SC 42
- **Link:** [ISO/IEC TR 24028:2020](#)
- **Status:** Published
- **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.

3.10. Framework for trust-based media services

- **SDO/Group:** ITU-T
- **Link:** [ITU-T Y.3054](#)
- **Status:** Published
- **Summary:** This framework provides guidelines for trust-based media services. 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.

3.11. Trust.txt

- **SDO/Group:** JournalList
- **Link:** [Trust.txt](#)
- **Status:** Initiated
- **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.

3.12. Chromium Reputation Provider Framework

- **SDO/Group:** Google's Chrome Team
- **Link:** [Chromium Reputation Provider Framework](#)
- **Status:** Initiated
- **Summary:** This framework provides guidelines for reputation management in 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.

3.13. International Standard Content Code (ISCC)

- **SDO/Group:** ISO/TC 46/SC 9
- **Link:** [ISO 24138](#)
- **Status:** Published
- **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.

3.14. Unique Media Identifier (UMid)

- **SDO/Group:** IWA 44
- **Link:** [UMid](#)
- **Status:** Published
- **Summary:** This specification offers a unique identifier for media content. It includes methods for

creating and maintaining UMid 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.

3.15. TDM Reservation Protocol

- **SDO/Group:** W3C
- **Link:** [TDMRep](#)
- **Status:** Published
- **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.

3.16. Spawning ai.txt

- **SDO/Group:** Spawning
- **Link:** [Spawning ai.txt](#)
- **Status:** Published
- **Summary:** This specification offers a method for opting out of AI training. It includes guidelines for creating and maintaining ai.txt files, which can be used to document the opt-out of digital assets. This helps in ensuring that content is not used for AI training without the creator's consent.

3.17. Robots.txt

- **SDO/Group:** IETF
- **Link:** [RFC 9309](#)
- **Status:** Published
- **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.

3.18. Vocabulary for Expressing Content Preferences for AI

- **SDO/Group:** IETF
- **Link:** [draft-vaughan-aipref-vocab-00](#)
- **Status:** Withdrawn
- **Summary:** This draft offers a vocabulary for expressing content preferences for AI. It includes guidelines for creating and maintaining preference files, which can be used to document the preferences of digital assets. This helps in ensuring that content is used in accordance with the creator's preferences.

3.19. Open Binding of Content Identifiers (OBID)

- **SDO/Group:** SMPTE
- **Link:** [SMPTE ST 2112-10:2020](#)
- **Status:** Published
- **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.

3.20. X.ig-dw: Implementation Guidelines for Digital Watermarking

- **SDO/Group:** ITU-T SG17
- **Link:** [2413-PLN](#)
- **Status:** Published
- **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.

3.21. Specification of Digital Rights Management (DRM) Technology for Digital Publications

- **SDO/Group:** ISO/IEC JTC 1/SC 34
- **Link:** [ISO/IEC 23078-1:2024](#)
- **Status:** Published
- **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.

3.22. A Review of Medical Image Watermarking Requirements for Teleradiology

- **SDO/Group:** NIH
- **Link:** [Medical Image Watermarking](#)
- **Status:** Published
- **Summary:** This review outlines the requirements for watermarking medical images for teleradiology. It includes guidelines for creating and maintaining watermark files, which can be used to document the watermarking of medical images. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.23. Evaluation Tools for Persistent Association Technologies

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- **Link:** [ISO/IEC TR 21000-11:2004](#)
- **Status:** Published
- **Summary:** This standard provides tools for evaluating persistent association technologies. 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.

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

- **SDO/Group:** IEEE
- **Link:** [IEEE P3361](#)
- **Status:** In progress
- **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.

4. Standardization Map

4.1. Overview

Table 1. Table of Standard Categorization

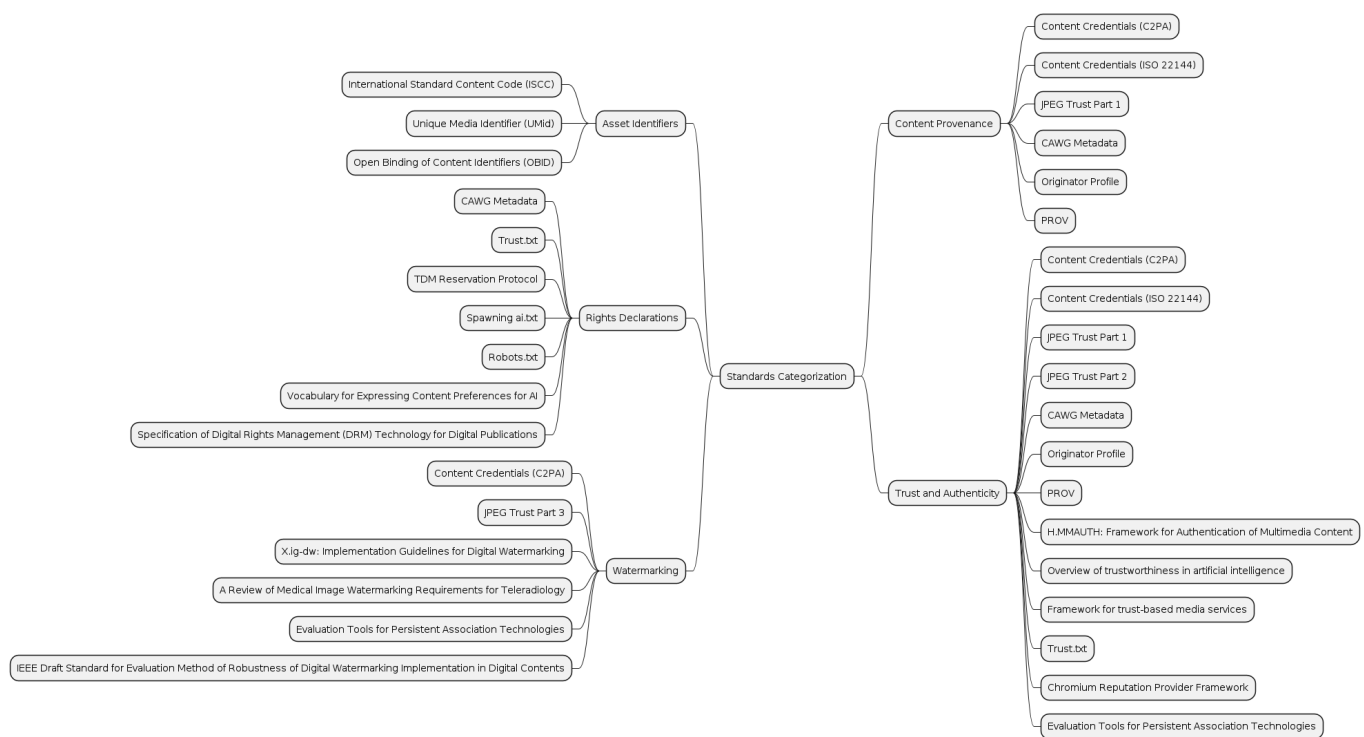
Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking
Content Credentials (C2PA)	x	x			x
Content Credentials (ISO 22144)	x	x			
JPEG Trust Part 1	x	x	x	x	
JPEG Trust Part 2		x			
JPEG Trust Part 3					x
CAWG Metadata	x	x		x	

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking
Originator Profile	x	x			
PROV	x	x			
H.MMAUTH: Framework for Authentication of Multimedia Content		x			
Overview of trustworthiness in artificial intelligence		x			
Framework for trust-based media services		x			
Trust.txt		x		x	
Chromium Reputation Provider Framework		x			
International Standard Content Code (ISCC)			x		
Unique Media Identifier (UMid)			x		
TDM Reservation Protocol				x	
Spawning ai.txt				x	
Robots.txt				x	

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking
Vocabulary for Expressing Content Preferences for AI				x	
Open Binding of Content Identifiers (OBID)			x		
X.ig-dw: Implementation Guidelines for Digital Watermarking					x
Specification of Digital Rights Management (DRM) Technology for Digital Publications				x	
A Review of Medical Image Watermarking Requirements for Teleradiology					x
Evaluation Tools for Persistent Association Technologies		x			x

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking
IEEE Draft Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents					X

4.2. Graphical Representation



5. Conclusion and next steps

TBD