Technical Report on AI and Multimedia Authenticity Standards

Leonard Rosenthol <lrosenth@adobe.com>, Touradj Ebrahimi <touradj.ebrahimi@epfl.ch>

1.0 Draft : 2025-03-28

Table of Contents

Introduction

This report provides a comprehensive overview of various standards and specifications related to digital media, focusing on content provenance, trust authenticity, asset identifiers, opt-out mechanisms, 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. Content Provenance

Content provenance refers to the documentation of the origin and history of digital content. It is crucial for verifying the 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 in contexts where the authenticity of content is paramount, such as in journalism, scientific research, and digital art.

1.1. Content Credentials (C2PA)

- **SDO/Group:** C2PA
- **Link:** C2PA Specification
- **Details:** 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.

1.2. Content Credentials (ISO 22144)

- **SDO/Group:** ISO TC 171/SC 2
- **Link:** ISO 22144
- **Details:** 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.

1.3. JPEG Trust

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1
- **Link:** ISO 21617-1:2025
- **Details:** This standard focuses on ensuring trust in JPEG images through provenance documentation. It provides a framework for embedding provenance information directly into JPEG files, allowing users to verify the authenticity and history of the images. This is particularly useful in contexts where image manipulation is common, such as in digital forensics and media.

1.4. Originator Profile

- **SDO/Group:** Originator Profile
- **Link:** Originator Profile
- **Details:** 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.

1.5. PROV

- **SDO/Group:** Open Provenance
- **Link:** PROV
- **Details:** 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.

2. Trust and Authenticity

Trust and authenticity standards ensure that digital content is genuine and has not been tampered with. These standards 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.

2.1. H.MMAUTH: Framework for Authentication of Multimedia Content

- **SDO/Group:** ITU-T/SG-13 & ISO/IEC JTC 1/SC29
- **Details:** This framework provides guidelines for authenticating multimedia content. It includes methods for verifying the integrity of digital media files and ensuring that they have not been altered since their creation. This helps in maintaining the trustworthiness of multimedia content in various applications, such as broadcasting and digital archiving.

2.2. Overview of trustworthiness in artificial intelligence

- **SDO/Group:** ISO/IEC JTC 1/SC 42
- **Link:** ISO/IEC TR 24028:2020
- **Details:** 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.

2.3. Framework for trust-based media services

- **SDO/Group:** ITU-T
- **Link:** ITU-T Y.3054
- **Details:** 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.

2.4. Trust.txt

- **SDO/Group:** JournalList
- **Link:** Trust.txt
- **Details:** 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.

2.5. Chromium Reputation Provider Framework

- **SDO/Group:** Google's Chrome Team
- **Link:** Chromium Reputation Provider Framework
- **Details:** 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. Asset Identifiers

Asset identifiers are unique codes assigned to digital content to ensure proper management and tracking. These identifiers help in maintaining a clear and organized record of digital assets, making it easier to 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.

3.1. International Standard Content Code (ISCC)

- **SDO/Group:** ISO/TC 46/SC 9
- **Link:** ISO 24138
- **Details:** 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.

3.2. Unique Media Identifier (UMid)

- **SDO/Group:** IWA 44
- **Link:** UMid
- **Details:** 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.

4. Opt-Out Mechanisms

Opt-out mechanisms 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.

4.1. TDM Reservation Protocol

- **SDO/Group:** W3C
- **Link:** TDMRep
- **Details:** 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.

4.2. Spawning ai.txt

- **SDO/Group:** Spawning
- **Link:** Spawning ai.txt
- **Details:** 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.

4.3. Robots.txt

- **SDO/Group:** IETF
- **Link:** RFC 9309
- **Details:** 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.

4.4. Vocabulary for Expressing Content Preferences for AI

- **SDO/Group:** IETF
- **Link:** draft-vaughan-aipref-vocab-00
- **Details:** 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.

5. Watermarking

Watermarking standards ensure that digital content is marked in a way that can be used to verify its authenticity and ownership. These standards are essential for protecting 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 ensure that their rights are respected.

5.1. Open Binding of Content Identifiers (OBID)

- **SDO/Group:** SMPTE
- **Link:** SMPTE ST 2112-10:2020
- **Details:** 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.

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

- **SDO/Group:** ITU-T SG17
- **Link:** 2413-PLEN
- **Details:** 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.

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

- **SDO/Group:** ISO/IEC JTC 1/SC 34
- **Link:** ISO/IEC 23078-1:2024
- **Details:** 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.

5.4. A Review of Medical Image Watermarking Requirements for Teleradiology

- **SDO/Group:** NIH
- **Link:** Medical Image Watermarking
- **Details:** 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.

5.5. Evaluation Tools for Persistent Association Technologies

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 11
- **Link:** ISO/IEC TR 21000-11:2004
- **Details:** 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.

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

- **SDO/Group:** IEEE
- **Link:** IEEE P3361
- **Details:** 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.

6. Conclusion

The standards and specifications outlined in this report are essential for ensuring the integrity, authenticity, and proper management of digital content. 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. As digital media continues to evolve, the need for robust standards becomes increasingly critical to protect the interests of creators, consumers, and organizations.