## Content Credentials

* **SDO/Group:** C2PA
* **Link:** [C2PA Specification](https://c2pa.org/specifications/specifications/2.1/specs/C2PA_Specification.html)
* **Status:** Published
* **Media:** Any
* **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.

## Content Credentials

* **SDO/Group:** ISO TC 171/SC 2
* **Link:** [ISO 22144](https://www.iso.org/standard/90726.html)
* **Status:** In progress
* **Media:** Any
* **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.

## 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](https://www.iso.org/standard/86831.html)
* **Status:** Published
* **Media:** Any (but focused on images)
* **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 assets as a function of their trust profiles. This is particularly useful in contexts where image manipulation is common, such as in social media applications.

## JPEG Trust Part 2: Trust profiles catalog

* **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1
* **Status:** In Progress
* **Media:** Any (but focused on images)
* **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.

## JPEG Trust Part 3: Media asset watermarking

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

## CAWG Metadata

* **SDO/Group:** Creation Assertions Working Group, as part of DIF
* **Link:** [CAWG Metadata](https://cawg.io/metadata/1.1/)
* **Status:** Published
* **Media:** Any
* **Summary:** This specification provides a framework for expressing metadata that captures detailed information about the content, including ownership and authorship.

## Originator Profile

* **SDO/Group:** Originator Profile
* **Link:** [Originator Profile](https://originator-profile.org/en-US/)
* **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.

## PROV

* **SDO/Group:** Open Provenance
* **Link:** [PROV](https://openprovenance.org/)
* **Status:** Published
* **Media:** Any
* **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.

## Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence

* **SDO/Group:** ISO/IEC JTC 1/SC 42
* **Link:** [ISO/IEC TR 24028:2020](https://www.iso.org/standard/77608.html?browse=tc)
* **Status:** Published
* **Media:** n/a
* **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.

## Framework for trust-based media services

* **SDO/Group:** ITU-T
* **Link:** [ITU-T Y.3054](https://standards.globalspec.com/std/13059031/itu-t-y-3054)
* **Status:** Published
* **Media:** n/a
* **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.

## Trust.txt

* **SDO/Group:** JournalList
* **Link:** [Trust.txt](https://journallist.net/reference-document-for-trust-txt-specifications)
* **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.

## Chromium Reputation Provider Framework

* **SDO/Group:** Google’s Chrome Team
* **Link:** [Chromium Reputation Provider Framework](https://docs.google.com/document/d/1wTFafdHa-o3OYCKmYzEJGROrpSoxXN6DNXPltzdiUzg/edit?pli=1&tab=t.0#heading=h.40o7mijeapa7)
* **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.

## ISCC: International Standard Content Code (ISCC)

* **SDO/Group:** ISO/TC 46/SC 9
* **Link:** [ISO 24138](https://www.iso.org/standard/77899.html)
* **Status:** Published
* **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.

## Unique Media Identifier (UMid)

* **SDO/Group:** IWA 44
* **Link:** [Umid](https://www.din.de/en/din-and-our-partners/press/press-releases/iwa-44-unique-media-identifier-umid-1189784)
* **Status:** Published
* **Media:** Any
* **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.

## TDM Reservation Protocol

* **SDO/Group:** W3C
* **Link:** [TDMRep](https://www.w3.org/ns/tdmrep/)
* **Status:** Published
* **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.

## Spawning ai.txt

* **SDO/Group:** Spawning
* **Link:** [Spawning ai.txt](https://spawning.ai/ai-txt)
* **Status:** Published
* **Media:** Any
* **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.

## Robots.txt

* **SDO/Group:** IETF
* **Link:** [RFC 9309](https://datatracker.ietf.org/doc/html/rfc9309)
* **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.

## Vocabulary for Expressing Content Preferences for AI Training

* **SDO/Group:** IETF
* **Link:** [ietf-aipref-vocab-00](https://www.ietf.org/archive/id/draft-ietf-aipref-vocab-00.html)
* **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.

## Open Binding of Content Identifiers (OBID)

* **SDO/Group:** SMPTE
* **Link:** [SMPTE ST 2112-10:2020](https://pub.smpte.org/pub/st2112-10/st2112-10-2020.pdf)
* **Status:** Published
* **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.

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

* **SDO/Group:** ITU-T SG17
* **Link:** [2413-PLEN](https://www.itu.int/md/T22-SG17-240902-TD-PLEN-2413/en)
* **Status:** Published, but temporary
* **Media:** Images, Videos
* **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.

## Information technology — Specification of digital rights management (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](https://www.iso.org/standard/84956.html)
* **Status:** Published
* **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.

## A Review of Medical Image Watermarking Requirements for Teleradiology

* **SDO/Group:** NIH
* **Link:** [Medical Image Watermarking](https://pmc.ncbi.nlm.nih.gov/articles/PMC3597963/)
* **Status:** Published
* **Media:** Images
* **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.

## Information technology — Multimedia framework (MPEG-21) — Part 11: Evaluation Tools for Persistent Association Technologies

* **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 11
* **Link:** [ISO/IEC TR 21000-11:2004](https://www.iso.org/standard/40487.html)
* **Status:** Published
* **Media:** Audio, Video
* **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.

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

* **SDO/Group:** IEEE
* **Link:** [IEEE P3361](https://standards.ieee.org/ieee/3361/11224/)
* **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.

## H.MMAUTH: Framework for authentication of multimedia content

* **SDO/Group:** ITU-T SG21/Q9
* **Link:** [H.MMAUTH](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=21141)
* **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.

## 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)](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=21058)
* **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.

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

* **SDO/Group:** ITU-T SG21/Q7
* **Link:** [H.VADS](https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=22161)
* **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.

## Credible Web

* **SDO/Group:** W3C
* **Link:** [Cred Web](https://www.w3.org/community/credibility/)
* **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.

## 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](https://responsibledatacollection.org/)
* **Status:** Published
* **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.

## Data Provenance Standards

* **SDO/Group:** Data & Trust Alliance
* **Link:** [D&TA Data Provenance Standards v1.0.0](https://dataandtrustalliance.org/)
* **Status:** Published
* **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.

## 2024—IEEE Draft Standard for Transparent Human and Machine Agency Identification

* **SDO/Group:** IEEE
* **Link:** [IEEE P3152/D4](https://store.accuristech.com/standards/ieee-p3152?product_id=2918804)
* **Status:** Published
* **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.

## IPTC Photo Metadata Standard

* **SDO/Group:** IPTC
* **Link:** [IPTC Photo Metadata Standard 2024.1](https://www.iptc.org/std/photometadata/specification/IPTC-PhotoMetadata)
* **Status:** Published
* **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.

## Dynamic Adaptive Streaming over HTTP (DASH) Part 4: Segment Encryption and Authentication

* **SDO/Group:** ISO/IEC JTC 1/SC 29
* **Link:** [DASH](https://www.iso.org/standard/73603.html)
* **Status:** Published
* **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.

## Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies

* **SDO/Group:** IEEE SA
* **Link:** [Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies](https://standards.ieee.org/ieee/3429/11490/)
* **Status:** Published
* **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.