



**International
Standard**

ISO/IEC 21617-1

**Information technology — JPEG
Trust —**

**Part 1:
Core foundation**

**Second edition
2026-08**

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 JPEG Trust framework	6
4.1 Description	6
4.2 Overview	6
4.3 Trust Record	7
4.4 Trust Manifests	8
4.4.1 General	8
4.4.2 Components of a Trust Manifest	9
4.4.3 Details of a Trust Manifest	9
4.4.4 Trust Declaration	10
4.5 Trust Indicators	10
4.5.1 General	10
4.5.2 Trust Indicator Set	10
4.6 Trust Profile	10
4.7 Trust Report	11
4.7.1 General	11
4.7.2 Trust Report generation procedure	11
4.7.3 Trust Report Assertion	12
5 Assertions	12
5.1 Introduction	12
5.1.1 Overview	12
5.1.2 Description	13
5.2 Assertion metadata	13
5.2.1 General	13
5.2.2 When (date and time)	13
5.2.3 Extent of modification(s)	14
5.3 Actions	14
5.3.1 Description	14
5.3.2 Type of modification	14
5.3.3 Region of interest	15
5.3.4 Purpose of modification(s)	15
5.3.5 How was it created	15
5.3.6 Category of modifications	15
5.4 Bindings (hashes)	16
5.4.1 General	16
5.4.2 Hard bindings	16
5.4.3 Soft bindings	16
5.5 Using existing metadata standards	16
5.5.1 Exif	16
5.5.2 IPTC	17
5.6 Intellectual property rights	17
5.6.1 General	17
5.6.2 Identity	17
5.6.3 Rights	20
5.6.4 IPR Examples	22
6 Embedding and referencing	23
6.1 Use of JUMBF	23
6.2 Embedding manifests into JPEG assets	24
6.2.1 Embedding manifests into JPEG 1 and JPEG XT	24

6.2.2	Embedding manifests into JPEG XL.....	24
6.2.3	Embedding manifests into JPEG 2000.....	25
6.2.4	Embedding manifests into JPEG XS.....	25
6.3	Embedding manifests into other asset types.....	25
6.4	External manifests.....	26
6.5	Embedding a reference to the active manifest.....	26
7	Media asset content binding.....	26
7.1	General.....	26
7.2	Cryptographic binding to content.....	26
7.3	Content hash.....	27
7.4	Use of digital signatures.....	27
7.5	Use of timestamps.....	27
7.6	Validation.....	27
8	Privacy and protection.....	28
8.1	General.....	28
8.2	Anonymization.....	28
8.2.1	Redaction.....	28
8.3	Obfuscation.....	29
8.3.1	General.....	29
8.3.2	Protecting an assertion.....	29
8.3.3	Protecting the media asset content.....	32
Annex A (normative)	Serialisation of Trust Indicator Sets.....	34
Annex B (normative)	Serialisation of Trust Profiles.....	47
Annex C (normative)	Serialisation of Trust Reports.....	60
Annex D (informative)	Using Dublin Core metadata with JPEG Trust.....	64
Annex E (informative)	Relationship between this document (JPEG Trust) and Content Credentials.....	67
Annex F (informative)	Threat vectors.....	68
Annex G (informative)	Change history.....	71
Bibliography		72

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see <https://www.iso.org/directives> or https://www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://www.iso.org/patents> and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see <https://www.iso.org/iso/foreword.html>. In the IEC, see <https://www.iec.ch/understanding-standards>.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

This second edition cancels and replaces the first edition (ISO/IEC 21617:2025), which has been technically revised.

The main changes are as follows:

- A new [Annex D](#) has been added to where details of the changes made in this edition can be found..

A list of all parts in the ISO/IEC 21617 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at <https://www.iso.org/members.html> and <https://www.iec.ch/national-committees>.

Introduction

Current technologies enable the modification or synthetic creation of media assets. Some, like deep learning methods, can create media assets that are hard for people to distinguish from natural media assets. These technologies open new, creative opportunities that are useful for business and research usage. However, these technologies can also lead to issues relating to the use of manipulated media assets to spread misinformation or disinformation. Misuse of manipulated media assets can cause social unrest, spread rumours for political gain, or encourage hate crimes.

Media modifications are not always negative as they are increasingly a normal and legal component of many production pipelines. However, in many application domains, creators need or want to declare the type of modifications that were performed on the media asset. A lack of such declarations in these situations may reveal the lack of trustworthiness of media assets or the intention to hide the existence of manipulations. To address such problems and attempt to avoid negative impacts, some companies, including social media platforms and news outlets, are developing mechanisms to clearly detect and annotate manipulated media assets when they are shared.

There is a need to have a standardized way to annotate media assets (regardless of the intent) and securely link the assets and annotations together. This document (JPEG Trust) ensures interoperability between a wide range of applications dealing with media asset creation and modification, providing a set of standard mechanisms to describe and embed information about the creation and modification of media assets.

Furthermore, a key aspect of understanding the trustworthiness of a media asset is the nature of trust itself. No single trust model can accommodate all the expressions of media asset trust in society so this document (JPEG Trust) requires a flexible architecture for accommodating diverse trust models. Through the mechanism of user-defined trust profiles, this document empowers various communities to define trust models that meet the specific demands of their trust requirements.

This document (JPEG Trust) provides a comprehensive framework for individuals, organizations, and governing institutions interested in establishing an environment of trust for the media that they use, and to support trust in the media they share online. This framework addresses aspects of providing provenance information, assertion rights, extracting and evaluating trust indicators, and handling privacy and security concerns.

This is the second edition of this document (JPEG Trust). It has been updated to reflect the latest developments in the field of media provenance and to provide a framework for the declaration of intellectual property rights. Details of the changes made in this edition can be found in [Annex G](#).

Information technology — JPEG Trust —

Part 1: Core foundation

1 Scope

This document specifies a framework for establishing trust in media. This framework includes aspects of authenticity, provenance, attribution, intellectual property rights, and integrity through secure and reliable annotation of the media assets throughout their life cycle.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18181-2:2024, *Information technology — JPEG XL image coding system — Part 2: File format*

ISO/IEC 18477-1, *Information technology — Scalable compression and coding of continuous-tone still images — Part 1: Core coding system specification*

ISO/IEC 18477-3, *Information technology — Scalable compression and coding of continuous-tone still images — Part 3: Box file format*

ISO/IEC 19566-4, *Information technologies — JPEG systems — Part 4: Privacy and security*

ISO/IEC 19566-5:2023, *Information technologies — JPEG systems — Part 5: JPEG universal metadata box format (JUMBF)*

ISO/IEC 19566-6, *Information technologies — JPEG systems — Part 6: JPEG 360*

ISO/IEC 19566-7, *Information technologies — JPEG systems — Part 7: JPEG linked media format (JLINK)*

ISO/IEC 19566-8, *Information technologies — JPEG systems — Part 8: JPEG Snack*

ISO/IEC 21122-1, *Information technology — JPEG XS low-latency lightweight image coding system — Part 1: Core coding system*

Rec. ITU-T T.81 (1992) | ISO/IEC 10918-1:1994, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*

Rec. ITU-T T.800 (v4) (07/24) | ISO/IEC 15444-1:2024, *Information technology — JPEG 2000 image coding system — Part 1: Core coding system*

IETF RFC 4648, *The Base16, Base32, and Base64 Data Encodings. RFC Series¹⁾*

IETF RFC 8141, *Uniform Resource Names (URNs). RFC Series²⁾*

W3C Recommendation JSON-LD, *JSON-LD 1.1*, <https://www.w3.org/TR/json-ld11/>

1) Available from: <https://www.rfc-editor.org/info/rfc4648>.

2) Available from: <https://www.rfc-editor.org/info/rfc8141>.

ISO/IEC 21617-1:2026(en)

ODRL INFORMATION MODEL. W3C *ODRL Information Model 2.2*, <https://www.w3.org/TR/odrl-model/>

VOCABULARY EXPRESSION ODRL, W3C *ODRL Vocabulary & Expression 2.2*, <https://www.w3.org/TR/odrl-vocab/>

C2PA Technical Specification, *C2PA Technical Specification 2.3*, Coalition for Content Provenance and Authenticity, https://c2pa.org/specifications/specifications/2.3/specs/C2PA_Specification.html

json-formula, *json-formula: A Query Language for JSON with Spreadsheet Functions*, <https://opensource.adobe.com/json-formula/>

Bibliography

- [1] ISO 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*
- [2] ISO/IEC 10918-4, *Information technology — Digital compression and coding of continuous-tone still images — Part 4: APPn markers*
- [3] ISO/IEC 14496-12, *Information technology — Coding of audio-visual objects — Part 12: ISO base media file format*
- [4] ISO 15836-1, *Information and documentation — The Dublin Core metadata element set — Part 1: Core elements*
- [5] ISO 16684-1, *Graphic technology — Extensible metadata platform (XMP) — Part 1: Data model, serialization and core properties*
- [6] ISO 24138:2024, *Information and documentation — International Standard Content Code (ISCC)*
- [7] IDENTITY ASSERTION C.A.W.G. CAWG Identity Assertion, version 1.2, <https://cawg.io/identity/1.2/>
- [8] METADATA ASSERTION C.A.W.G. CAWG Metadata Assertion, version 1.1, <https://cawg.io/metadata/1.1/>
- [9] CAWG Training and Data Mining Assertion, CAWG Training and Data Mining Assertion, version 1.1, <https://cawg.io/training-and-data-mining/1.1/>
- [10] Exif, CIPA DC- 008-Translation- 2019 Exchangeable image file format for digital still cameras: Exif Version 2.32, https://www.cipa.jp/std/documents/download_e.html?DC-008-Translation-2019-E
- [11] PRINCIPLES F.A.I.R. FAIR Principles, <https://www.go-fair.org/fair-principles/>
- [12] PHOTO METADATA STANDARD I.P.T.C. IPTC Photo Metadata Standard 2023.1, <https://www.iptc.org/std/photometadata/specification/IPTC-PhotoMetadata>
- [13] VERSIONING S. Semantic Versioning 2.0.0, <https://semver.org/spec/v2.0.0.html>
- [14] YAML. YAML Ain't Markup Language (YAML™) Version 1.2.2, <https://yaml.org/spec/1.2.2/>
- [15] IETF BCP 47, *Best Current Practice 47*. Available from: <https://www.rfc-editor.org/info/bcp47>.
- [16] IETF RFC 4514, K. ZEILENGA. *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*. RFC Series³⁾
- [17] IETF RFC 5280, D. COOPER, S. SANTESSON, S. FARRELL, S. BOEYEN, R. HOUSLEY and W. POLK. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC Series⁴⁾
- [18] IETF RFC 8152, J. SCHAAD. *CBOR Object Signing and Encryption (COSE)*. RFC Series⁵⁾
- [19] W3C Recommendation Verifiable Credentials Data Model, *Verifiable Credentials Data Model v1.1*, <https://www.w3.org/TR/vc-data-model/>
- [20] L. Zhang, L. Zhang, X. Mou and D. Zhang, "FSIM: A Feature Similarity Index for Image Quality Assessment," in *IEEE Transactions on Image Processing*, vol. 20, no. 8, pp. 2378-2386, Aug. 2011, doi: 10.1109/TIP.2011.2109730. Available at <https://ieeexplore.ieee.org/document/5705575>
- [21] Zhou Wang and A. C. Bovik, "A universal image quality index," in *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81-84, March 2002, doi: 10.1109/97.995823. Available at <https://ieeexplore.ieee.org/document/995823>

3) Available from: <https://www.rfc-editor.org/info/rfc4514>.

4) Available from: <https://www.rfc-editor.org/info/rfc5280>.

5) Available from: <https://www.rfc-editor.org/info/rfc8152>.

- [22] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861. Available at <https://ieeexplore.ieee.org/document/1284395>
- [23] IETF RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. RFC Series⁶⁾

6) Available from: <https://www.rfc-editor.org/info/rfc3161>.