International Standard

ISO/IEC 21617-1

Information technology — JPEG Trust —

Part 1: Core foundation

Second edition
2026-08

Reference number
ISO/IEC 21617-1:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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

© ISO/IEC 2026 – All rights reserved

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

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved

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 Series*[1)]

IETF RFC 8141, *Uniform Resource Names (URNs). RFC Series*[2)]

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 2026 – All rights reserved

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/

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org

3.1
actor
actors
human or non-human (hardware or software) that is participating in the media ecosystem

EXAMPLE camera (capture device), generation or editing software, cloud service or the person using such tools

3.2
anonymization
process of altering data in a media asset with the aim to protect the privacy of an *actor* (3.1) by obscuring identifiable features

3.3
assertion
data structure which represents a statement asserted by an *actor* (3.1) concerning the *media asset* (3.19)

Note 1 to entry: This data is a part of the *trust manifest* (3.40).

[SOURCE: C2PA Technical Specification]

3.4
authentic media asset
authenticity of media asset
media asset (3.19) that is *verifiable* (3.45)

3.5
author
human whose creativity led to a work being created or modified

3.6
claim
digitally signed and tamper-evident data structure that references one or more *assertion* (3.3) by one or more *actors* (3.1), concerning a *media asset* (3.19), and the information necessary to represent the content binding. If any assertion was redacted, then a declaration to that effect is included

Note 1 to entry: This data is a part of the *trust manifest* (3.40).

[SOURCE: C2PA Technical Specification]

© ISO/IEC 2026 – All rights reserved

3.7
claim signature
digital signature on the *claim* (3.6) using the private key of an *actor* (3.1)

Note 1 to entry: The claim_signature is a part of the *trust manifest* (3.40).

[SOURCE: C2PA Technical Specification]

3.8
composed media asset
media asset (3.19) composed of multiple media assets

3.9
content binding
information that associates *media asset content* (3.20) to a specific *trust record* (3.42) associated with a specific *media asset* (3.19), either as a *hard binding* (3.13) or a *soft binding* (3.36)

[SOURCE: C2PA Technical Specification]

3.11
fingerprint
set of inherent properties computable from *media asset content* (3.20) that identifies the content or near duplicates of it

[SOURCE: C2PA Technical Specification]

3.12
generative AI media asset
synthetic media asset
media asset (3.19) created by means of artificial intelligence (AI) and machine learning (ML)

3.13
hard binding
one or more cryptographic hashes that uniquely identifies either the entire *media asset* (3.19) or a portion thereof

[SOURCE: C2PA Technical Specification]

3.14
intellectual property rights
IPR
exclusive rights of the *actor* (3.1) to the intellectual work of their creation

3.15
invisible watermark
information incorporated in a substantially human imperceptible way into the *media asset content* (3.20) of an *media asset* (3.19) which can be used, for example, to uniquely identify the media asset or to store a reference to a *trust record* (3.42)

[SOURCE: C2PA Technical Specification]

3.16
JPEG 1
common image compression data format and means of reference to Rec. ITU-T T.81 (1992) | ISO/IEC 10918-1:1994

3.17
JUMBF
universal format to embed any type of metadata in any box-based JPEG file format and means of reference to ISO/IEC 19566-5:2023

© ISO/IEC 2026 – All rights reserved

3.18
manipulated media asset
manipulated media
media asset (3.19) that has been changed with the intention to induce misinterpretation

3.19
media asset
digital assets including images, videos, audio or text

3.20
media asset content
portion of a *media asset* (3.19) that represents the actual content, such as the pixel data of an image, along with any additional technical metadata required to understand or render the content (e.g., a colour profile or encoding parameters)

3.21
media asset integrity
lack of corruption of a *media asset* (3.19)

3.22
media asset metadata
portion of a *media asset* (3.19) that represents non-technical information about the media asset or its content, such as location, creator, annotations or IPR information

3.23
media asset original
media asset (3.19) produced by a device or method without any modifications

3.24
media asset provenance
set of information about a *media asset* (3.19) including the trail of modifications starting from an *actor* (3.1)

EXAMPLE The media asset origin.

Note 1 to entry: Modifications that are missing from the asset's provenance are treated the same as an invalid or unverifiable provenance chain.

3.25
media asset source
non-human *actor* (3.1) that created the *media asset original* (3.23)

3.26
modified media asset
media asset (3.19) that has been changed

3.27
natural media asset
sensor acquired media asset

3.28
obfuscation
process of altering data in a media asset with the aim to protect unauthorized access

3.29
provenance
logical concept of understanding the history of a *media asset* (3.19) and its interaction with *actor* (3.1)s and other media assets, as represented by the *provenance data* (3.30)

[SOURCE: C2PA Technical Specification]

© ISO/IEC 2026 – All rights reserved

3.30
provenance data
set of *trust record* (3.42)s for a *media asset* (3.19) and, in the case of a composed asset, its ingredients

[SOURCE: C2PA Technical Specification]

3.31
region of interest
ROI
subset within the *media asset content* (3.20) identified for a particular purpose

EXAMPLE the face portion of a portrait image, an extracted foreground object(s) or scene cuts of a video

3.33
registration
process of storing information (e.g. media asset, metadata or provenance) about a *media asset* (3.19), separate from the media asset itself

3.34
signer
actor (3.1) who digitally signs a *media asset* (3.19)

3.35
signing
process that establishes the relation between an *actor* (3.1) and a *media asset* (3.19) in a tamper-evident manner

3.36
soft binding
content identifier that is either (a) not statistically unique, such as a *fingerprint* (3.11), or (b) embedded as an *invisible watermark* (3.15) in the identified *media asset content* (3.20)

[SOURCE: C2PA Technical Specification]

3.37
trust declaration
specific type of *trust manifest* (3.40) that, when present, is always first in the *trust record* (3.42)

Note 1 to entry: It represents the *actor* (3.1) that created the *media asset* (3.19) and contains only mandatory assertions.

3.38
trust indicators
information derived from a combination of the *media asset* (3.19) and the *trust record* (3.42) that indicate a level of trustworthiness of a media asset in a given context

3.39
trust indicator set
set of *trust indicators* (3.38) that are derived from a *media asset* (3.19) and its *trust record* (3.42)

3.40
trust manifest
set of information about the *media asset provenance* (3.24) of a *media asset* (3.19)

Note 1 to entry: A trust manifest is part of a *trust record* (3.42).

3.41
trust profile
set of expressions that are used to evaluate each *trust indicators* (3.38) in an given *trust indicator set* (3.39) to indicate a level of trustworthiness for a given *media asset* (3.19)

© ISO/IEC 2026 – All rights reserved

3.42
trust record
collection of one or more *trust manifest* (3.40) that can either be embedded into a *media asset* (3.19) or be external to its media asset

3.43
trust report
result of evaluating a *trust indicator set* (3.39) against a *trust profile* (3.41)

3.44
trustworthy
able to be relied on as being what it is asserted to be

3.45
trustworthy media asset
media asset (3.19) that is *trustworthy* (3.44)

3.46
verifiable
able to be checked

4 JPEG Trust framework

4.1 Description

This document describes a framework for establishing trust in media that complies with the JPEG standards developed by ISO/IEC JTC1 SC 29 including (Rec. ITU-T T.81 (1992) | ISO/IEC 10918 (JPEG 1), Rec. ITU-T T.800 (v4) (07/24) | ISO/IEC 15444-1 (JPEG 2000), ISO/IEC 18477-1 (JPEG XT), ISO/IEC 18181-2 (JPEG XL), ISO/IEC 21122-1 (JPEG XS), ISO/IEC 19566-6 (JPEG 360), ISO/IEC 19566-7 (JLINK) and ISO/IEC 19566-8 (JPEG Snack)). The core components of the framework are built on the JPEG Universal Metadata Box Format (JUMBF), as described in 6.1. Therefore, the core principles can also be applied on other types of media that can embed JUMBF containers. The model for storing and accessing cryptographically verifiable information about a media asset is aligned with the technical aspects of Content Credentials.

NOTE For more information about the relationship between this document (JPEG Trust) and Content Credentials, see Annex E.

4.2 Overview

The JPEG Trust framework establishes that a media asset consists of the media asset content, media asset metadata, and a Trust Record. The Trust Record (4.3) consists of a one or more Trust Manifests. Each Trust Manifest is a tamper-evident unit that contains a series of statements, called assertions, that cover areas, such as asset creation, creation device details, authorship, edit actions, bindings to content and other information associated with the media asset.

A set of Trust Indicators (4.5) can be derived from the trust record as well as from other metadata or the media asset content. These Trust Indicators are gathered together into a Trust Indicator Set (4.5.2), which can be used to assess the trustworthiness of a media asset in a given context through the use of a specified Trust Profile (4.6). The result of this evaluation is documented in a Trust Report (4.7).

The framework and its core components are illustrated in Figure 1.

© ISO/IEC 2026 – All rights reserved