International Standard

ISO/IEC 21617-1

First edition
2025-01

Information technology — JPEG Trust —

Part 1: Core foundation

Reference number
ISO/IEC 21617-1:2025(en)

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 **1**
4 JPEG Trust framework **5**
4.1 Description 5
4.2 Overview 5
4.3 Trust Record 6
4.4 Trust Manifests 7
4.4.1 General 7
4.4.2 Components of a Trust Manifest 8
4.4.3 Details of a Trust Manifest 8
4.4.4 Trust Declaration 9
4.5 Trust Indicators 9
4.6 Trust Credential 9
4.6.1 General 9
4.6.2 For media asset content 10
4.6.3 For Trust Manifests 10
4.6.4 Claim 13
4.6.5 For claim signature 14
4.6.6 For verifiable credentials 15
4.6.7 For media asset metadata 15
4.6.8 Example Trust Credentials 16
4.7 Trust Profile 20
4.7.1 General 20
4.7.2 Trust Profile information 20
4.7.3 Statements 20
4.7.4 Expressions 21
4.7.5 Predefined statement IDs 21
4.7.6 Examples 22
4.8 Trust Report 27
4.8.1 General 27
4.8.2 Examples 28
4.8.3 Trust Report generation procedure 31
5 Media asset life cycle annotations **31**
5.1 Overview 31
5.2 Assertions 32
5.2.1 Description 32
5.2.2 IPR information 32
5.2.3 Using existing metadata standards 35
5.2.4 Actions 35
5.2.5 Bindings (hashes) 36
5.3 Assertion metadata 37
5.3.1 General 37
5.3.2 Actors 37
5.3.3 When (date and time) 37
5.3.4 Extent of modification(s) 37
6 Embedding and referencing **38**
6.1 Use of JUMBF 38
6.2 Embedding manifests into JPEG assets 38
6.2.1 Embedding manifests into JPEG 1 and JPEG XT 38
6.2.2 Embedding manifests into JPEG XL 39

6.2.3 Embedding manifests into JPEG 2000 ... 39
6.2.4 Embedding manifests into JPEG XS ... 40
6.3 Embedding manifests into other asset types ... 40
6.4 External manifests ... 40
6.5 Embedding a reference to the active manifest ... 40

7 Identification of actors ... 40
7.1 Identity and actors ... 40
7.1.1 Verifiable credentials ... 40

8 Media asset content binding ... 43
8.1 General ... 43
8.2 Cryptographic binding to content ... 43
8.3 Use of digital signatures ... 43
8.4 Validation ... 43

9 Privacy and protection ... 44
9.1 General ... 44
9.2 Anonymization ... 44
9.2.1 W3C Verifiable Credentials ... 44
9.2.2 Redaction ... 45
9.3 Obfuscation ... 47
9.3.1 General ... 47
9.3.2 Protecting an assertion ... 47
9.3.3 Protecting the media asset content ... 49

Annex A (informative) **Threat vectors ... 51**

Annex B (informative) **Relationship between this document (JPEG Trust) and C2PA ... 54**

Bibliography ... 55

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 www.iso.org/directives or 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 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 www.iso.org/iso/foreword.html. In the IEC, see 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*.

A list of all parts in the ISO 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 www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Current technologies permit 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 to spread misinformation or disinformation. Misuse of manipulated media 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 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. This means that the standard 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, extracting and evaluating trust indicators, and handling privacy and security concerns.

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 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 10918-1, *Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines*

ISO/IEC 15444-1:2024, *Information technology — JPEG 2000 image coding system — Part 1: Core coding system*

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*

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, available at: https://www.rfc-editor.org/info/rfc4122

W3C Recommendation JSON-LD 1.1, *A JSON-based Serialization for Linked Data*, available at: https://www.w3.org/TR/json-ld11/

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

3.3
media asset content
portion of a *media asset* (3.2) 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)

3.4
media asset metadata
portion of a *media asset* (3.2) that represents non-technical information about the media asset or its content, such as location, creator, annotations or IPR information

3.5
natural media asset
sensor acquired media asset

3.6
region of interest
ROI
subset within the *media asset content* (3.3) identified for a particular purpose

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

3.7
synthetic media asset
synthetically generated media asset
media asset (3.2) generated at least partially by a computer program

3.8
generative AI media asset
media asset (3.2) created by means of artificial intelligence (AI) and machine learning (ML)

3.9
JPEG 1
common image compression data format and means of reference to ISO/IEC 10918-1

3.10
digital master
master media asset as intended by its creator

3.11
manipulated media asset
manipulated media
media asset (3.2) that has been changed with the intention to induce misinterpretation

3.12
media asset original
media asset (3.2) produced by a device or method without any modifications

3.13
media asset provenance
set of information about a *media asset* (3.2) including the trail of modifications starting from an *actor* (3.1)

EXAMPLE 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.

3.14
media asset source
non-human *actor* (3.1) that created the *media asset original* (3.12)

3.15
modified media asset
media asset (3.2) that has been changed

3.16
assertion
data structure which represents a statement asserted by an *actor* (3.1) concerning the *media asset* (3.2)

Note 1 to entry: This data is a part of the *trust manifest* (3.19).

3.17
claim
digitally signed and tamper-evident data structure that references one or more *assertion* (3.16) by one or more *actors* (3.1), concerning a *media asset* (3.2) and the information necessary to represent the content_binding

Note 1 to entry: If any assertion was redacted, then a declaration to that effect is included. This data is a part of the *trust manifest* (3.19).

3.18
claim signature
digital signature on the *claim* (3.17) using the private key of an *actor* (3.1)

Note 1 to entry: The claim_signature is a part of the *trust manifest* (3.19).

3.19
trust manifest
set of information about the *media asset provenance* (3.13) of a *media asset* (3.3). A trust manifest is part of a *trust record* (3.23)

3.20
trust declaration
specific type of *trust manifest* (3.19) that, when present, is always first in the *trust record* (3.21). It represents the *actor* (3.1) that created the *media asset* (3.2) and contains only mandatory assertions

3.21
trust record
collection of one or more *trust manifest* (3.21) that can either be embedded into a *media asset* (3.2) or be external to its media asset

3.22
trust indicators
information derived from a combination of the *media asset* (3.2) and the *trust record* (3.21) that indicate a level of trustworthiness of a media asset in a given context

3.23
trust credential
the set of *trust indicators* (3.22) that are derived from a *media asset* (3.2) and its *trust record* (3.23)

3.24
trust profile
set of expressions that are used to evaluate each *trust indicators* (3.22) in a given *trust credential* (3.23) to indicate a level of trustworthiness for a given *media asset* (3.3)

3.25
trust report
result of evaluating a *trust credential* (3.23) against a *trust profile* (3.24)

3.26
authentic media asset
media asset (3.2) that is *verifiable* (3.27) or *trustworthy* (3.28) or both

3.27
verifiable
able to be checked

3.28
trustworthy
able to be relied on as being what it is asserted to be

3.29
media asset integrity
lack of corruption of a *media asset* (3.2)

3.30
registration
process of storing information (e.g. media asset, metadata or provenance) about a *media asset* (3.2), separate from the media asset itself

3.31
signer
actor (3.1) who digitally signs a *media asset* (3.2)

3.32
signing
process that establishes the relation between an *actor* (3.1) and a *media asset* (3.2) in a tamper-evident manner

3.33
intellectual property rights
IPR
exclusive right of the *actor* (3.1) to the intellectual work of their creation

3.34
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

3.35
obfuscation
process of altering data in a media asset with the aim to protect unauthorized access

3.36
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

4 JPEG Trust framework

4.1 Description

This document describes a framework for establishing trust in media that comply with the JPEG standards developed by ISO/IEC JTC1 SC 29 including ISO/IEC 10918-1 (JPEG 1), 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 ISO/IEC 19566-5 (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 the C2PA architecture.

NOTE For more information about the relationship between this document (JPEG Trust) and C2PA, see Annex B.

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) is a tamper-evident unit consisting of a one or more Trust Manifests. The Trust Manifests contain 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 Credential (4.6), which can be used to assess the trustworthiness of a media asset in a given context through the use of a specified Trust Profile (4.7). The result of this evaluation is documented in a Trust Report (4.8).

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

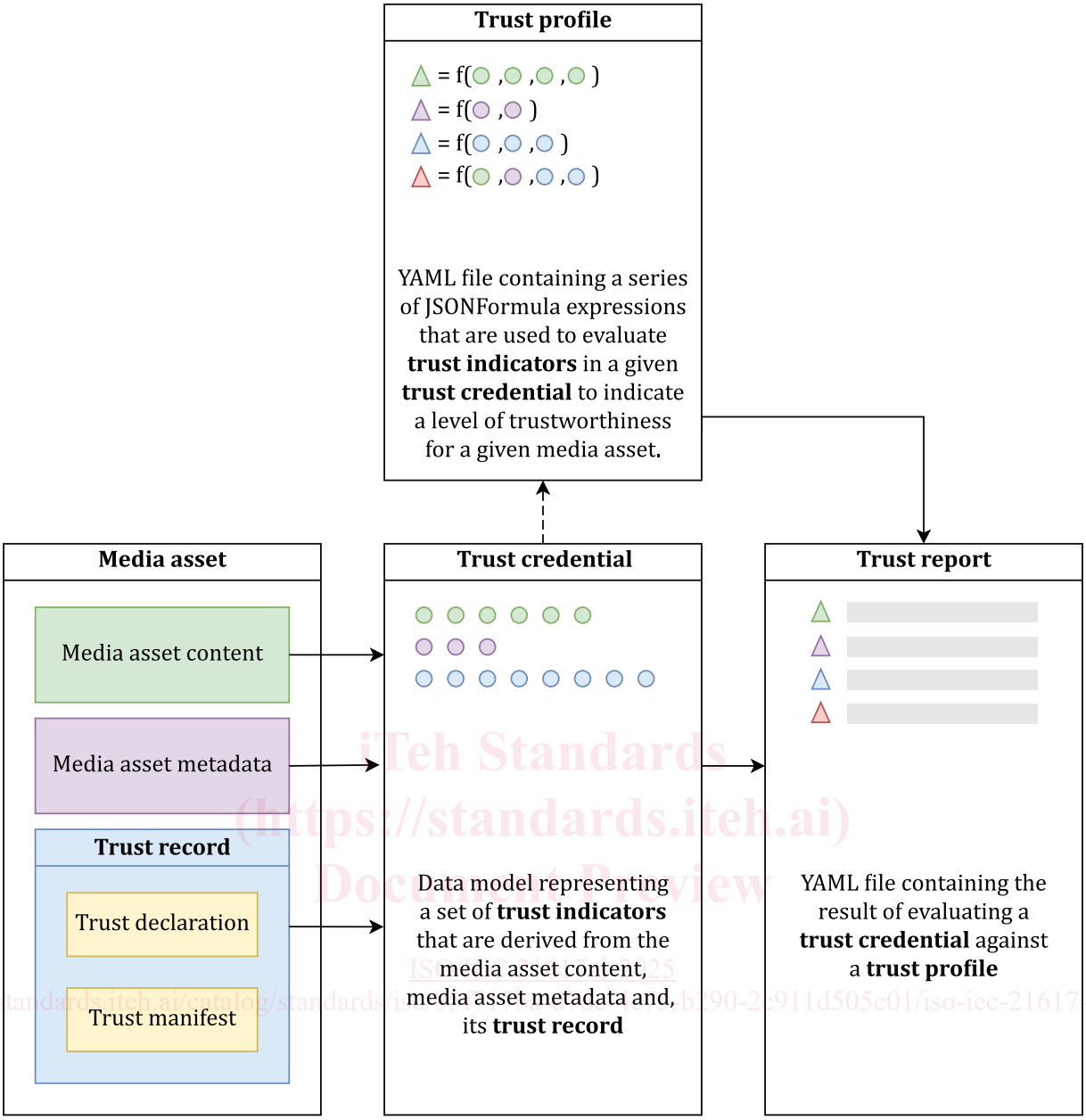

Figure 1 — Trust Framework

4.3 Trust Record

The Trust Record is a JUMBF superbox composed of a series of other JUMBF boxes and superboxes, each identified by their own UUID and label in their JUMBF Description box. The Trust Record Description box shall have a label of `c2pa`, a UUID of `0x63327061-0011-0010-8000-00AA00389B71` (`c2pa`) and shall contain one or more Trust Manifest superboxes (which may be a Trust Manifest or a Trust Declaration). The Trust Record may also contain JUMBF boxes and superboxes whose UUIDs are not defined in this document.

NOTE Allowing other boxes and superboxes enables custom extensions to this document (JPEG Trust) as well as enabling the addition of new boxes in future versions of this document without breaking compatibility.

A Trust Record (see Figure 2) shall contain at least one Trust Manifest. The set of Trust Manifests, as stored in the asset's Trust Record, represents its Media Asset Provenance.

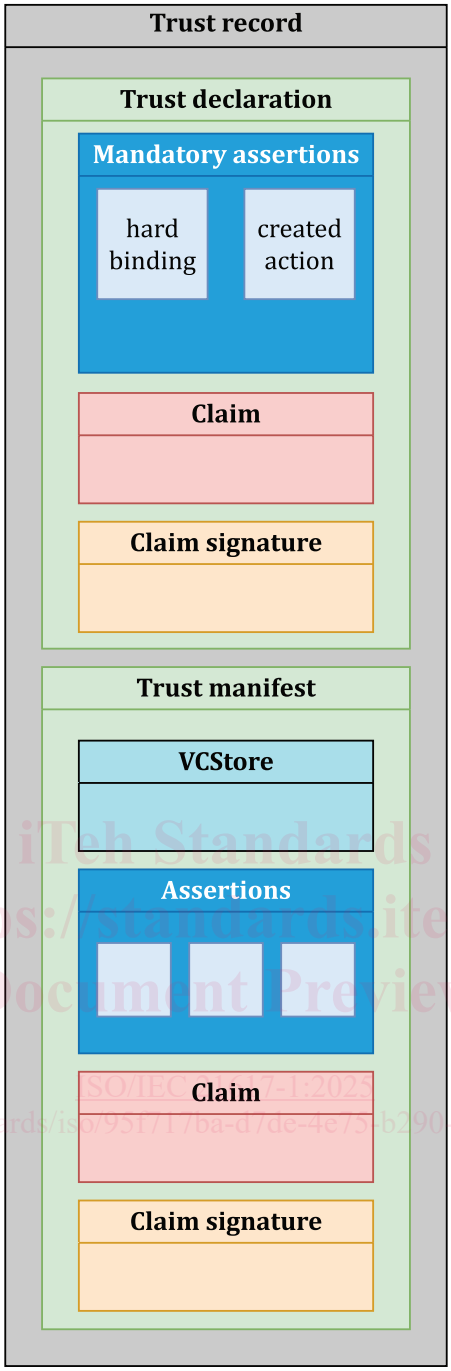

Figure 2 — A Trust Record

4.4 Trust Manifests

4.4.1 General

A Trust Manifest (see Figure 3) is the set of information about the media asset provenance, while a Trust Declaration is a special type of Trust Manifest with only mandatory assertions that always comes first in the Trust Record.

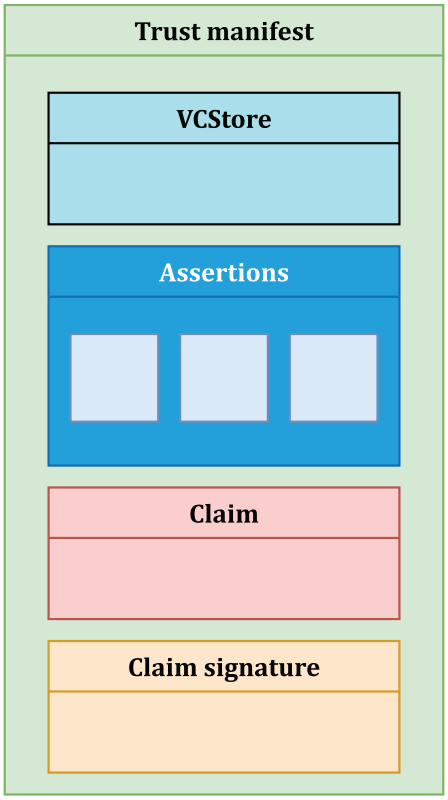

Figure 3 — A Trust Manifest

4.4.2 Components of a Trust Manifest

Each Trust Manifest may contain a Verifiable Credentials (VC) Store, Assertions, a Claim, and a Claim Signature.

Assertions (5.2) are statements about the media asset provenance of a given media asset; such as asset creation, capture device details, authorship, edit actions, and bindings to content. Assertions are wrapped up with additional information into a digitally signed entity called a Claim.

The W3C Verifiable Credentials[14] of individual actors that are involved in the creation of the Assertions can be added to the VCStore of a Trust Record to provide additional Trust Indicators concerning actors.

Together, these Assertions, Claims, Verifiable Credentials and Signatures are all bound together into the Trust Manifest by a hardware or software component called a Claim Generator.

4.4.3 Details of a Trust Manifest

The Trust Manifest is a JUMBF superbox composed of a series of other JUMBF boxes and superboxes, each identified by their own UUID and label in their JUMBF Description box. The UUID for each Trust Manifest shall be either `0x63326D61-0011-0010-8000-00AA00389B71` (`c2ma`), `0x6332636D-0011-0010-8000-00AA00389B71` (`c2cm`), `0x6332756D-0011-0010-8000-00AA00389B71` (`c2um`), or `0x63326D64-0011-0010-8000-00AA00389B71` (`c2md`) depending on the type of manifest. In order to enable uniquely identifying each Trust Manifest, they shall be labelled with a RFC 4122 (UUID) optionally proceeded by an identifier of the claim generator and a `:`.

EXAMPLE A label for the fictitious ACME claim generator might look like `acme:urn:uuid:F9168C5E-CEB2-4FAA-B6BF-329BF39FA1E4`.

NOTE More information about the JUMBF structure of Trust Manifests can be found in the C2PA specification.[6]