ISO/IEC JTC 1/SC 29/WG 1 **N100988**
105th meeting – Berlin – October 06-11, 2024

ISO/IEC JTC 1/SC 29/WG 1
(ITU-T SG16)

Coding of Still Pictures

JBIG
Joint Bi-level Image Experts Group

JPEG
Joint Photographic Experts Group

TITLE: JPEG Trust Terms and Definitions – v2.0

SOURCE: WG 1

PROJECT:

STATUS:

REQUESTED ACTION:

DISTRIBUTION: Public

Contact:
ISO/IEC JTC 1/SC 29/WG 1 Convener – Prof. Touradj Ebrahimi
EPFL/STI/IEL/GR-EB, Station 11, CH-1015 Lausanne, Switzerland
Tel: +41 21 693 2606, Fax: +41 21 693 7600, E-mail: Touradj.Ebrahimi@epfl.ch

Terms and definitions for JPEG Trust

Version 2.0, October 2024

1 Introduction

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

To ensure a correct understanding of the JPEG Trust documentation, this document defines terms and concepts as they are used in this context.

The terms and definitions come from different sources:

- [C2PA]: C2PA Technical Specifications
- [TRUST]: ISO/DIS 21617-1:2024(E) Core Foundation
- [JUMBF]: WD 19566-5:2023 AMD1 (JUMBF)
- [DUBLIN]: Dublin Core™ Metadata Element Set
- [ODRL]: ODRL terminology
- [ADD]: Additional terms and definitions that have been discussed and considered for future usage

The Dublin Core™ Metadata Element Set is a **vocabulary of fifteen properties** for use in resource description. The name "Dublin" is due to its origin at a 1995 invitational workshop in Dublin, Ohio; "core" because its elements are broad and generic, usable for describing a wide range of resources. Source: https://www.dublincore.org/specifications/dublin-core/dces/

The Open Digital Rights Language (ODRL) is a policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services. The ODRL Information Model describes the underlying concepts, entities, and relationships that form the foundational basis for the semantics of the ODRL policies. Policies are used to represent permitted and prohibited actions over a certain asset, as well as the obligations required to be meet by stakeholders. In addition, policies may be limited by constraints (e.g., temporal or spatial constraints) and duties (e.g. payments) may be imposed on permissions. Source: https://www.w3.org/TR/odrl-model/#terminology

2 Terms and definitions

In this section the terms and definitions are listed in alphabetical order with a reference to their original source.

action – an operation on an ***asset***. [ODRL]

actor (actors) – human or non-human (hardware or software) that is participating in the media ecosystem. Example: a camera (capture device), generation or editing software, cloud service or the person using such tools. [TRUST]

AI Generated Content (AIGC) – media asset created or modified by means of artificial intelligence (AI). [ADD]

anonymisation – process of altering data in a media asset with the aim to protect the privacy of an ***actor*** by obscuring identifiable features. [TRUST]

assertion – data structure which represents a statement asserted by an ***actor*** concerning the ***media asset***. This data is a part of the ***trust manifest***. [C2PA]

asset – a resource or a collection of resources that are the subject of a ***rule***. [ODRL]

authentic media asset – ***media asset*** that is ***verifiable*** or ***trustworthy*** or both. [TRUST]

author – a human whose creativity led to a work being created or modified. [ADD]

blockchain – a blockchain system is one type of distributed ledger architecture. [ADD]

box – binary structure that encapsulates an object embedded in a file. [JUMBF]

CBOR (abbreviated term) – Concise Binary Object Representation. [JUMBF]

claim – digitally signed and tamper-evident data structure that references one or more ***assertion*** by one or more ***actors***, concerning a ***media asset***, and the information necessary to represent the content binding. If any assertion was redacted, then a declaration to that effect is included. This data is a part of the ***trust manifest*** . [C2PA]

claim signature – digital signature on the ***claim*** using the private key of an ***actor***. The claim_signature is a part of the ***trust manifest***. [C2PA]

codestream – sequence of bits representing a compressed image and associated metadata. [JUMBF]

composed media asset – ***media asset*** composed of multiple media assets. [TRUST]

constraint – a boolean/logical expression that refines an ***action*** and ***party***/***asset*** collection or the conditions applicable to a ***rule***. [ODRL]

contributor – an entity responsible for making contributions to the resource. Note 1 to entry: Examples of a Contributor include a person, an organization, or a service. Typically, the name of a Contributor should be used to indicate the entity. [DUBLIN]

coordinate system – method of representing points in a space of given dimensions by coordinates. [TRUST]

coverage – the spatial or temporal topic of the resource, the spatial applicability of the resource, or the jurisdiction under which the resource is relevant. Note 1 to entry: Spatial topic and spatial applicability may be a named place or a location specified by its geographic coordinates. Temporal topic may be a named period, date, or date range. A jurisdiction may be a named administrative entity or a geographic place to which the resource applies. Recommended best practice is to use a controlled vocabulary such as the Thesaurus of Geographic Names [TGN]. Where appropriate, named places or time periods can be used in preference to numeric identifiers such as sets of coordinates or date ranges. [DUBLIN]

creator – an entity primarily responsible for making the resource. Note 1 to entry: Examples of a Creator include a person, an organization, or a service. Typically, the name of a Creator should be used to indicate the entity. [DUBLIN]

date – a point or period of time associated with an event in the lifecycle of the resource. Note 1 to entry: Date may be used to express temporal information at any level of granularity. Recommended best practice is to use an encoding scheme, such as the W3CDTF profile of ISO 8601 [W3CDTF]. [DUBLIN]

description – an account of the resource. Note 1 to entry: Description may include but is not limited to: an abstract, a table of contents, a graphical representation, or a free-text account of the resource. [DUBLIN]

digital master – master media asset as intended by its creator. [TRUST]

disinformation – information that is false and deliberately created to harm a person, social group, organisation or country[1]. [ADD]

distributed ledger – a database that spans many physical locations. [ADD]

distributed Ledger Technology (DLT) – a distributed system that enables a tamper-evident, append-only data store (ledger) . [ADD]

duty – the obligation to exercise an agreed ***action***. [ODRL]

format – the file format, physical medium, or dimensions of the resource. Note 1 to entry: Examples of dimensions include size and duration. Recommended best practice is to use a controlled vocabulary such as the list of Internet Media Types [MIME]. [DUBLIN]

fungible token – Fungible tokens or assets are divisible and non-unique. They are interchangeable and store value. [ADD]

generative AI media asset – ***media asset*** created by means of artificial intelligence (AI) and machine learning (ML) . [TRUST]

GLAM institutions – Galleries, Libraries, Archives and Museums. [ADD]

identifier – a value that uniquely refers to something, such as an asset or actor. [ADD]

identifier – An unambiguous reference to the resource within a given context. Note 1 to entry: Recommended best practice is to identify the resource by means of a string conforming to a formal identification system. [DUBLIN]

intellectual property rights (IPR) – exclusive right of the ***actor*** to the intellectual work of their creation. [TRUST]

JPEG (abbreviated term) – Joint Photographic Experts Group. [JUMBF]

JPEG 1 – common image compression data format and means of reference to ISO/IEC 10918-1:1994. [TRUST]

JSON (abbreviated term) – JavaScript object notation. [JUMBF]

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. [TRUST]

JUMBF Box – ***superbox*** containing a JUMBF Description Box, JUMBF Content Boxes and possibly a Padding Box. [JUMBF]

JUMBF Content Box – ***box*** of any type embedded in a ***JUMBF Box*** except the JUMBF Description Box or a Padding Box. [JUMBF]

JUMBF Content Type – specific set of ***JUMBF Type*** values. [JUMBF]

JUMBF Type – UUID that implies the type of content embedded in a ***JUMBF Box***. [JUMBF]

language – a language of the resource. Note 1 to entry: Recommended best practice is to use a controlled vocabulary such as RFC 4646 [RFC4646]. [DUBLIN]
ledger – a ledger is a book of accounts that contains the records of transactions. [ADD]

mal-information – information that is based on reality, used to inflict harm on a person, social group, organisation or country[1]. [ADD]

manipulated media asset – ***media asset*** that has been changed with the intention to induce misinterpretation. [TRUST]

media asset – digital assets including images, videos, audio or text. [TRUST]

media asset content – portion of a ***media asset*** 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) . [TRUST]

media asset integrity – lack of corruption of a ***media asset***. [TRUST]

media asset metadata – portion of a ***media asset*** that represents non-technical information about the media asset or its content, such as location, creator, annotations or IPR information. [TRUST]

media asset original – ***media asset*** produced by a device or method without any modifications. [TRUST]

media asset provenance – set of information about a ***media asset*** including the trail of modifications starting from an ***actor***, for example, the media asset original. Note 1 to entry: Modifications that are missing from the asset's provenance are treated the same as an invalid or unverifiable provenance chain. [TRUST]

media asset source – the non-human actor that created the media asset original. [TRUST]

media type – a standard description of the type and/or format of the data. Source: IETF RFC 2046

micro-licensing – a legal phrase to describe the difference between a standard licence and a limited licence in terms of time, purpose, channels, territories, etc. [ADD]

minter – actor who publishes an NFT. [ADD]

misinformation – information that is false but not created with the intention of causing harm[1]. [ADD]

modified media asset – ***media asset*** that has been changed. [TRUST]
natural media asset – sensor acquired media asset. [TRUST]

non-fungible token (NFT) – a unique data record containing a verifiable reference to an asset. [ADD]

obfuscation – process of altering data in a media asset with the aim to protect unauthorized access. [TRUST]

obligation – the obligation to exercise an agreed action. [ADD]

ODRL Common Vocabulary – a set of generic terms that may be re-used by ODRL Profiles. [ODRL]

ODRL Core Vocabulary – the set of terms that are represented by the ODRL Information Model. [ODRL]

ODRL Evaluator – a system that determines whether the ***rules*** of an ODRL ***policy*** expression have meet their intended action performance. [ODRL]

ODRL Profile – a community or sector specific vocabulary that extends the ***ODRL Core Vocabulary*** with new terms to express ***policies***. [ODRL]

[1] As defined by UNESCO: https://en.unesco.org/fightfakenews

ODRL Validator – a system that checks the conformance of ODRL ***policy*** expressions, including the cardinality of properties and if they are related to types of values as defined by the ODRL Information Model, and the Information Model's validation requirements. [ODRL]

parent image – image file in which a ***JUMBF Box*** is embedded. [JUMBF]

party – an entity or a collection of entities that undertake Roles in a ***rule***. [ODRL]

permission – the ability to exercise an ***action*** over an ***asset***. [ODRL]

policy – a group of one or more ***rules***. [ODRL]

prohibition – the inability to exercise an ***action*** over an ***asset***. [ODRL]

publisher – an entity responsible for making the resource available. Note 1 to entry: Examples of a Publisher include a person, an organization, or a service. Typically, the name of a Publisher should be used to indicate the entity. [DUBLIN]

region of interest (ROI) – subset within the ***media asset content*** identified for a particular purpose Example: the face portion of a portrait image, an extracted foreground object(s) or scene cuts of a video. [TRUST]

registrar – ***actor*** that performs a registration. [TRUST]
registration – process of storing information (e.g. media asset, metadata or provenance) about a ***media asset***, separate from the media asset itself. [TRUST]

relation – a related resource. Note 1 to entry: Recommended best practice is to identify the related resource by means of a string conforming to a formal identification system. [DUBLIN]

rights – information about rights held in and over the resource. Note 1 to entry: Typically, rights information includes a statement about various property rights associated with the resource, including intellectual property rights. [DUBLIN]

rule – an abstract concept that represents the common characteristics of ***permissions***, ***prohibitions***, and ***duties***. [ODRL]

signer – ***actor*** who digitally signs a ***media asset***. [TRUST]

signing – process that establishes the relation between an ***actor*** and a ***media asset*** in a tamper-evident manner. [TRUST]

smart contract – a computer program that is intended to automatically execute, control or document events and actions according to pre-specified rules. [ADD]

smart legal contract – a smart contract which creates legally binding obligations on the parties and which is wholly or partly written as a computer program. [ADD]

source – a related resource from which the described resource is derived. Note 1 to entry: The described resource may be derived from the related resource in whole or in part. Recommended best practice is to identify the related resource by means of a string conforming to a formal identification system. [DUBLIN]

statement – something that someone says or writes officially, or an action done to express an opinion. [ADD]

subject – the topic of the resource. Note 1 to entry: Typically, the subject will be represented using keywords, key phrases, or classification codes. Recommended best practice is to use a controlled vocabulary. [DUBLIN]

superbox – ***box*** that only contains other boxes. [JUMBF]

synthetic media asset – ***media asset*** generated at least partially by a computer program. [TRUST]

title – a name given to the resource. Note 1 to entry: Typically, a Title will be a name by which the resource is formally known. [DUBLIN]

tokenization – the process of encapsulating an asset's rights into a digital token. [ADD]
trust credential – the set of ***trust indicators*** that are derived from a ***media asset*** and its ***trust record***. [TRUST]

trust declaration – specific type of ***trust manifest*** that, when present, is always first in the ***trust record***. It represents the ***actor*** that created the ***media asset*** and contains only mandatory assertions. [TRUST]

trust indicators – information derived from a combination of the ***media asset*** and the ***trust record*** that indicate a level of trustworthiness of a media asset in a given context. [TRUST]

trust manifest – set of information about the ***media asset provenance*** of a ***media asset***. A trust manifest is part of a ***trust record***. [TRUST]

trust profile – set of expressions that are used to evaluate each ***trust indicators*** in an given ***trust credential*** to indicate a level of trustworthiness for a given ***media asset***. [TRUST]

trust record – collection of one or more ***trust manifest*** that can either be embedded into a *media asset* or be external to its media asset. [TRUST]

trust report – result of evaluating a ***trust credential*** against a ***trust profile***. [TRUST]

trustworthy – able to be relied on as being what it is asserted to be. [TRUST]

type – the nature or genre of the resource. Note 1 to entry: Recommended best practice is to use a controlled vocabulary such as the DCMI Type Vocabulary [DCMITYPE]. To describe the file format, physical medium, or dimensions of the resource, use the Format element. [DUBLIN]

URI (abbreviated term) – uniform resource identifier. [JUMBF]

verifiable – able to be checked. [TRUST]

XML (abbreviated term) – extensible markup language. [JUMBF]