An update on JPEG Trust

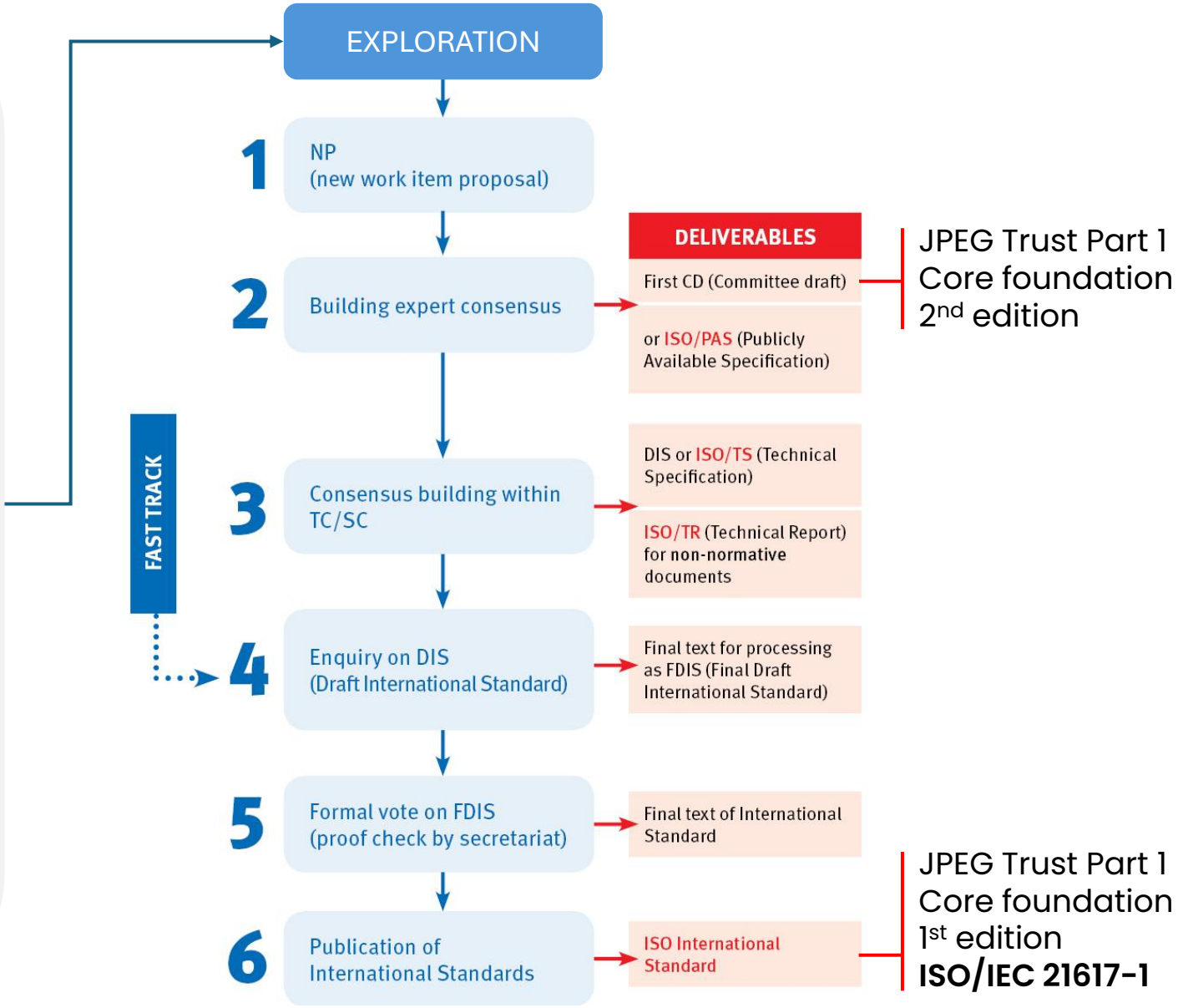
Philippe Rixhon, January 2025

prixhon@valunode.com

ISO standardisation process

JPEG Fake Media exploration

- Initiated in October 2020
- 5 workshops to engage with industry and stakeholders
- Identification of use cases and requirements
- Call for Proposals
- Completed in January 2023



Use cases

Misinformation and disinformation	Forgery/media forensics	Media creation	Media modification
• Media usage and breaking news • Deepfake detection • Content authenticity checking • Content usage tracing • Fraud in academic research • Photographic framing	• Insurance fraud • Mileage reporting photo • Photo for cost charge • Evidence of trial • Media sharing on social media • Credibility of AI training image data sets	• Movie special effects • Media transcoding • Chroma keying or silhouette extraction	• Image colorization and restoration • Photo editing

Requirements

- Media creation and modification descriptions
- Metadata embedding and referencing
- Authenticity, integrity, and trust model

Responses to the Call for Proposals on JPEG Fake Media

Adobe / Coalition for Content Provenance and Authenticity

- C2PA Specifications

Huawei

- Provenance and Right Management for Digital Contents in JPEG Fake Media

Sony Group Corporation

- Methods to keep track provenance of media asset and signing data

Vrije Universiteit Brussel / Interuniversity Microelectronics Centre (imec)

- Media revision history tracking via asset decomposition and serialization

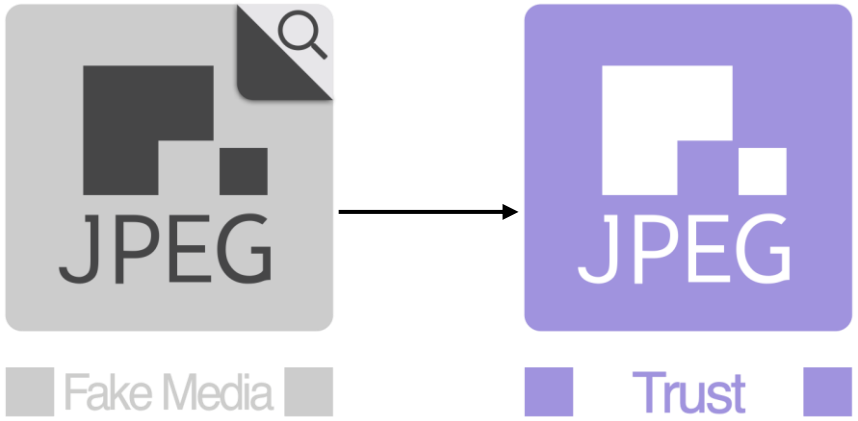
Universitat Politècnica de Catalunya

- Multimedia Information Protection And Management System (MIPAMS) Provenance module

Newcastle University

- TRusted mediA dIstribuTion (TRAIT)

Establishment of JPEG Trust



"The scope of JPEG Trust is to provide a framework for establishing trust in media. This framework includes aspects of authenticity, provenance, intellectual property rights, and integrity through secure and reliable annotation of the media assets throughout their life cycle."

Establishing trust

Tackling disinformation

Reactive approach: detection of modifications and deep fakes

Proactive approach: signaling provenance

Collaborative approach: leveraging community feedback

Trustworthiness depends on the context

“JPEG Trust does not explicitly define trustworthiness but rather provides a framework and tools for individuals, organisations, and governing institutions to establish trust in accordance with the conditions they specify.”

Trust indicators

✅ From family member

✅ Unmodified?
✅ Date
✅ Location

JPEG Trust Part 1: Core Foundation

Annotating provenance information

Extracting and evaluating trust indicators

Handling privacy and security concerns

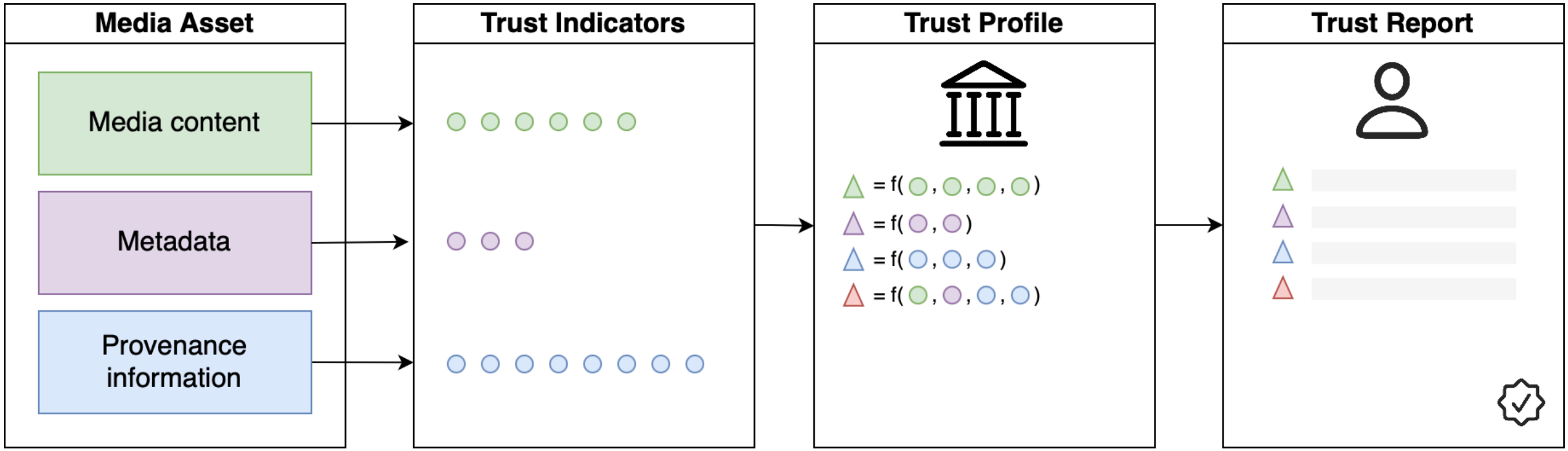
Annotating provenance information

- Embedding provenance annotations in media assets
- Securely link provenance annotations with associated media assets
- Model for expressing and embedding provenance annotations aligned with C2PA 1.4 (Coalition for Content Provenance and Authenticity) specification
- Media assets with C2PA 1.4 provenance annotations are compatible with the JPEG Trust framework
- Integrated in (upcoming) camera models of Leica, Sony and Nikon
- JPEG Trust adds additional provenance functionality such as signalling the extent of modifications

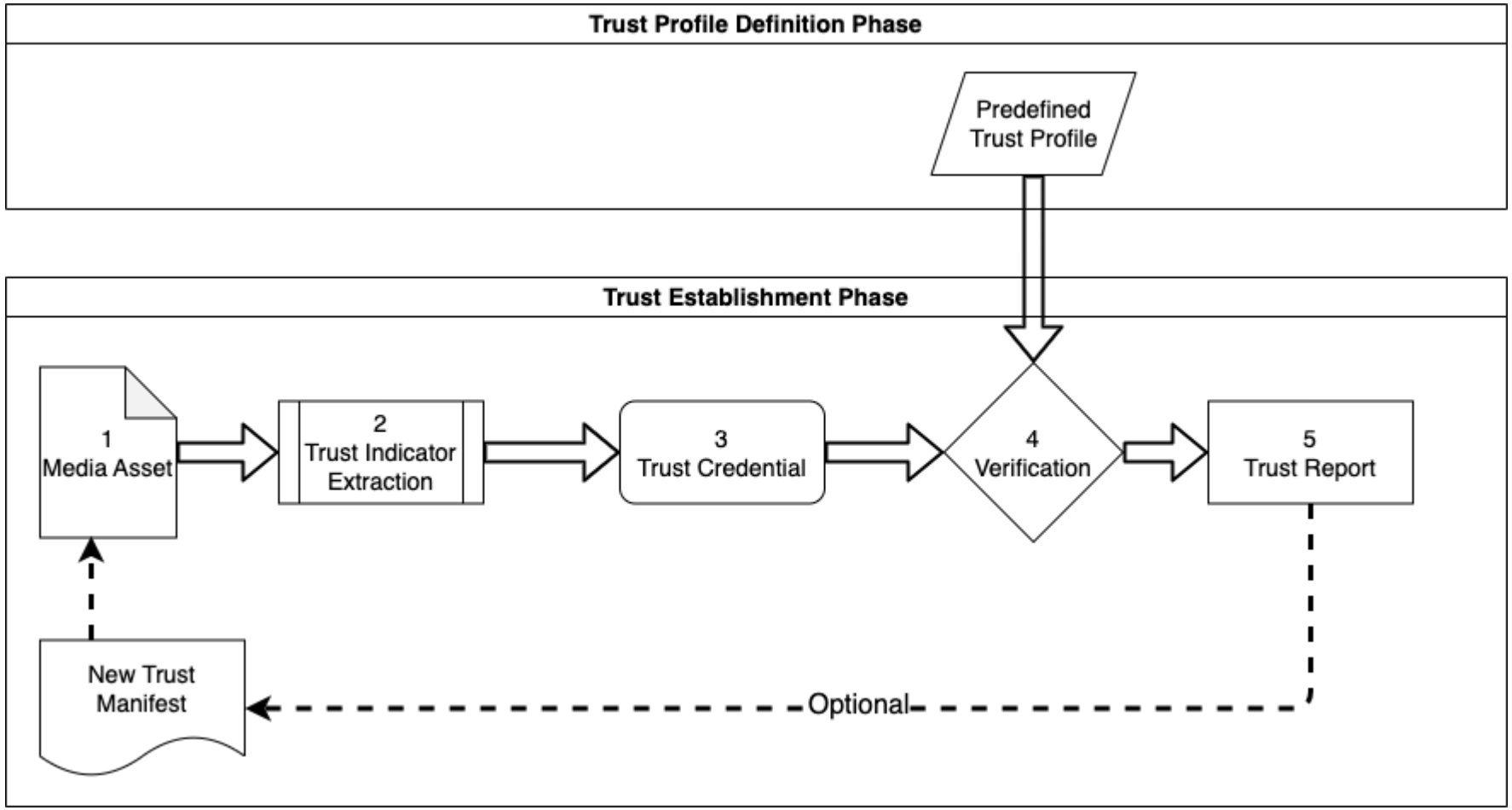
Extracting and evaluating trust indicators

- Trust Indicators can be extracted from:
  - media content
  - metadata, and
  - provenance information.
- Specific conditions for trustworthiness can be expressed in Trust Profiles.
- Trust profiles allow individuals, organizations, and governing institutions to evaluate relevant trust indicators according to the requirements for their specific usage scenarios.
- The resulting evaluation can be expressed in a Trust Report to make the information easily accessed and understood by the end user.

Extracting and evaluating trust indicators

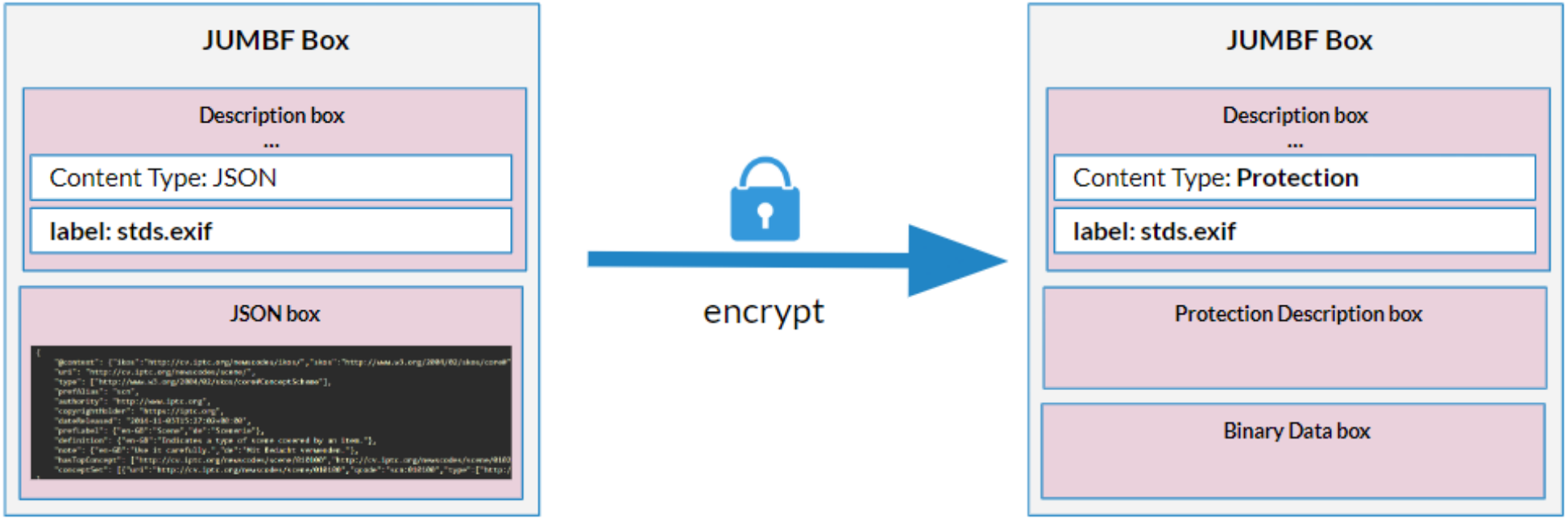


Extracting and evaluating trust indicators

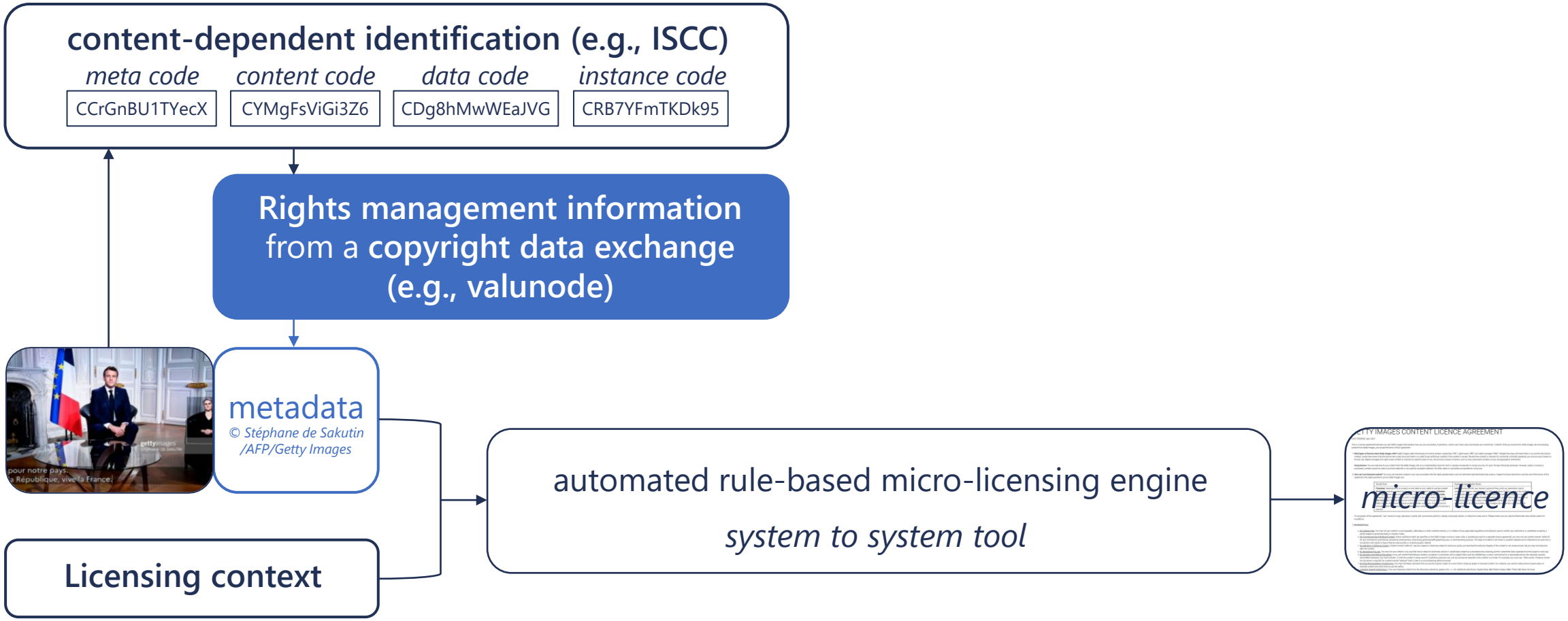


Handling privacy and security concerns

- Means to protect provenance annotations, including identification of actors
- Treated in line with JPEG Privacy and Security (ISO/IEC 19566-4)

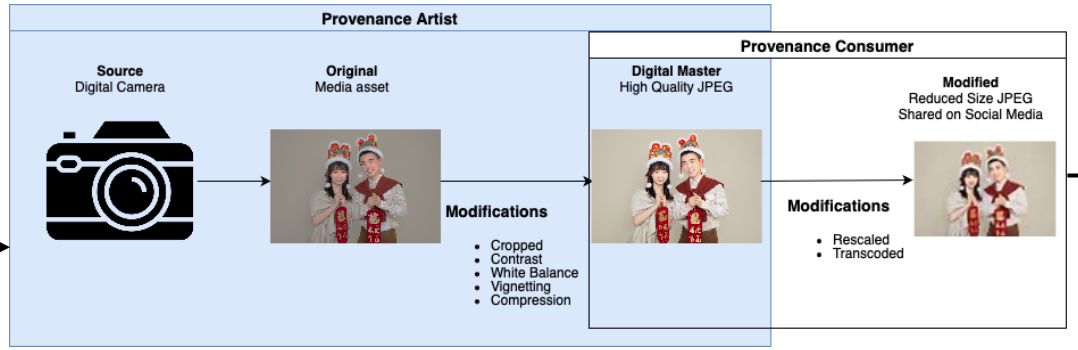


Automated micro-licensing



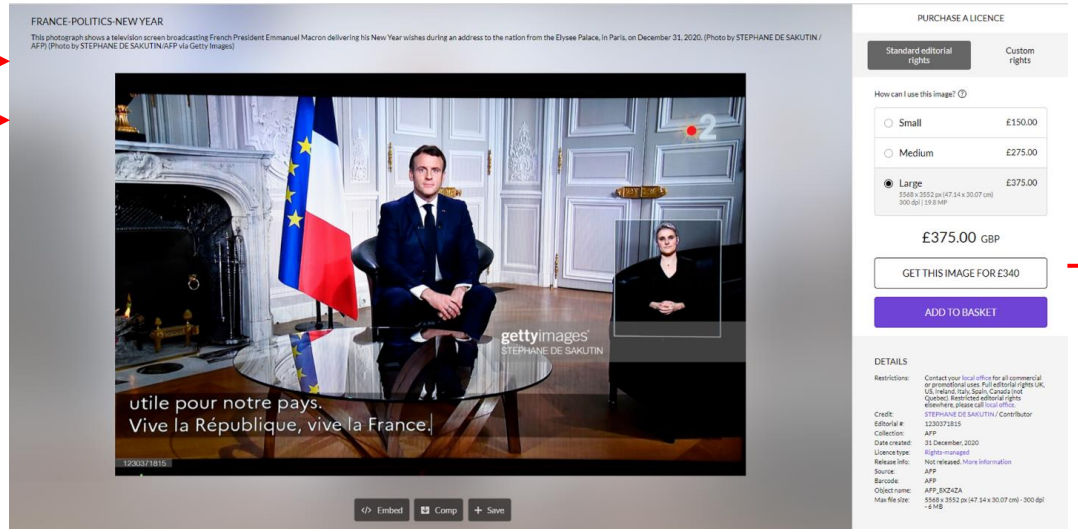
Additional use cases for JPEG Trust 2nd edition

- Misinformation and disinformation
- Forgery / Media forensics
- Media creation
- Media modification
- Media composition



Definitions of assets

- Media tokenization
  - Attribution
  - Rights declaration
  - Rights monetization
  - Rights remuneration



Definitions of actors

Additional requirements for JPEG Trust 2nd edition

Most requirements defined for media creation and modification, metadata embedding and referencing, and trust model apply equally to media tokenization.

1) Media creation and modification descriptions
2) Metadata embedding and referencing
3) Authenticity, integrity, and trust model
4) Media tokenization ⟶ The standard shall:
   - provide means to **identify**, **authenticate and describe involved actors** while considering **privacy** of individuals,
   - provide means to **identify** and **describe media assets**,
   - provide means to **signal IPR information** related to media assets,
   - provide means to **declare media assets and related tokens** while building upon existing standards of identifiers, metadata sets, and metadata exchanges, and
   - **facilitate the copyright declaration** and licensing of media assets, covering both **monetization** and **remuneration** aspects.

JPEG Trust

JPEG Trust Core Foundation, including
- Intellectual property rights, including
  - Attribution
  - Rights, including
    - TDM terms and conditions

JPEG Trust Profiles Catalogue

JPEG Trust Media Asset Watermarking

Part 1, 2nd edition

Part 2

Part 3

International organization for standardization (ISO) /IEC
Joint photographic experts' group (JPEG)
JPEG Trust (ISO/IEC 21617)

Content credentials ISO/DIS 22144

Creator assertions working group

Dublin Core™ metadata element set

Open digital rights language (ODRL)

Coalition for content provenance and authenticity (C2PA)

JPEG Trust, Part 1: Core foundation, 2nd edition

1) Scope
2) Normative references
3) Terms and definitions
4) JPEG Trust framework
    - Trust record
    - Trust manifest
    - Trust indicators
    - Trust profile
    - Trust report
5) Assertions
    - Assertion metadata
    - Actions
    - Bindings
        - Hard bindings
        - Soft bindings
    - Metadata standards
    - Intellectual property rights
        - Identity and attribution
        - Rights
6) Embedding and referencing
7) Media asset content binding
8) Privacy and protection

Normative annexes

A. Serialization of trust indicator sets
B. Examples

Informative annexes

C. Using Dublin Core metadata
D. Relationship with Content Credentials
E. Threat vectors
F. Change history

Bibliography

5.3 Actions assertion used to describe output of Generative AI

```
{
  "actions": [
    {
      "action": "c2pa.created",
      "when": 0("2023-02-11T09:00:00Z"),
      "softwareAgent" : {
          "name": "SuperAI PhotoEditor",
          "version": "2.0",
          "schema.org.SoftwareApplication.operatingSystem": "Windows 11"
      },
      "digitalSourceType": "http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia",
      "parameters" : {
        "ingredients" : [
          {
            "url": "self#jumbf=c2pa/joe-ed:urn:uuid:ABCD/c2pa.assertions/c2pa.ingredient__1",
            "alg": "sha256",
            "hash" : b64'...',
          },
          {
            "url": "self#jumbf=c2pa/joe-ed:urn:uuid:EFGH/c2pa.assertions/c2pa.ingredient__2",
            "alg": "sha256",
            "hash" : b64'...',
          }
        ]
      }
```

ACTION

GENERATOR

DEFINED BY IPTC

5.6.3.1 Obligation property with a policy

```
{
 "@context": "http://www.w3.org/ns/odrl.jsonld",
 "@type": "Agreement",
 "uid": "http://example.com/policy:42",
 "profile": "http://example.com/odrl:profile:09",
 "obligation": [{
     "assigner": "http://example.com/org:43",
     "assignee": "http://example.com/person:44",
     "action": [{
         "rdf:value": {
           "@id": "odrl:compensate“
         },
         "refinement": [
           {
            "leftOperand": "payAmount",
            "operator": "eq",
            "rightOperand": { "@value": "5.00", "@type": "xsd:decimal" },
            "unit": http://dbpedia.org/resource/Euro
           }]
         }]
       }]
}
```

CATEGORY
for example: cawg.data_mining

PARTIES

COMPENSATION

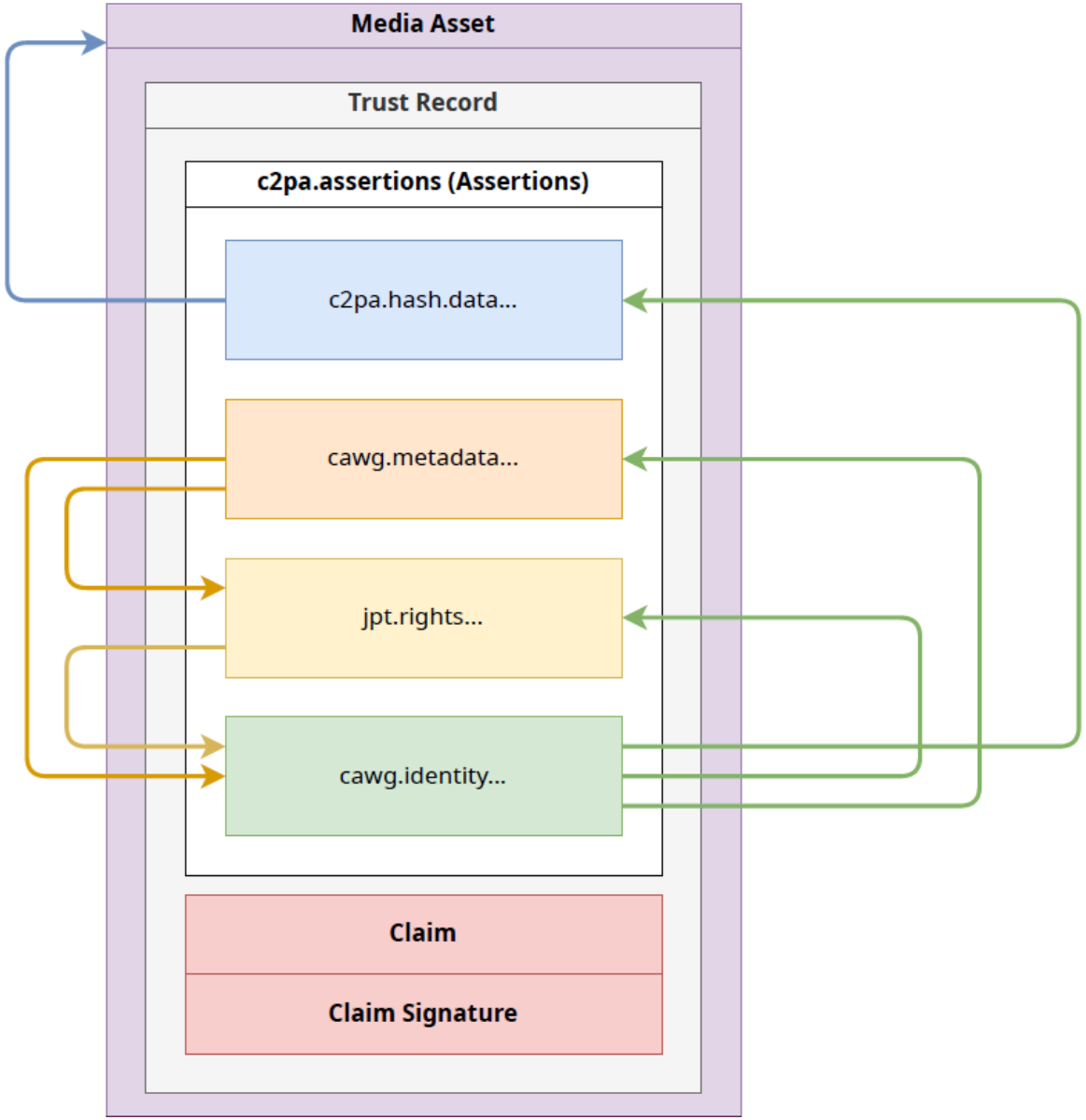
5.6.3.3 Training and data mining assertion

```
{
  "entries":
    "cawg.ai_training": {
      "use": "allowed"
    },
    "cawg.ai_inference": {
      "use": "allowed"
    },
    "cawg.ai_generative_training": {
      "use": "notAllowed"
    },
    "cawg.data_mining": {
      "use": "constrained",
      "constraint_info": "may only be mined against compensation”
    }
}
```

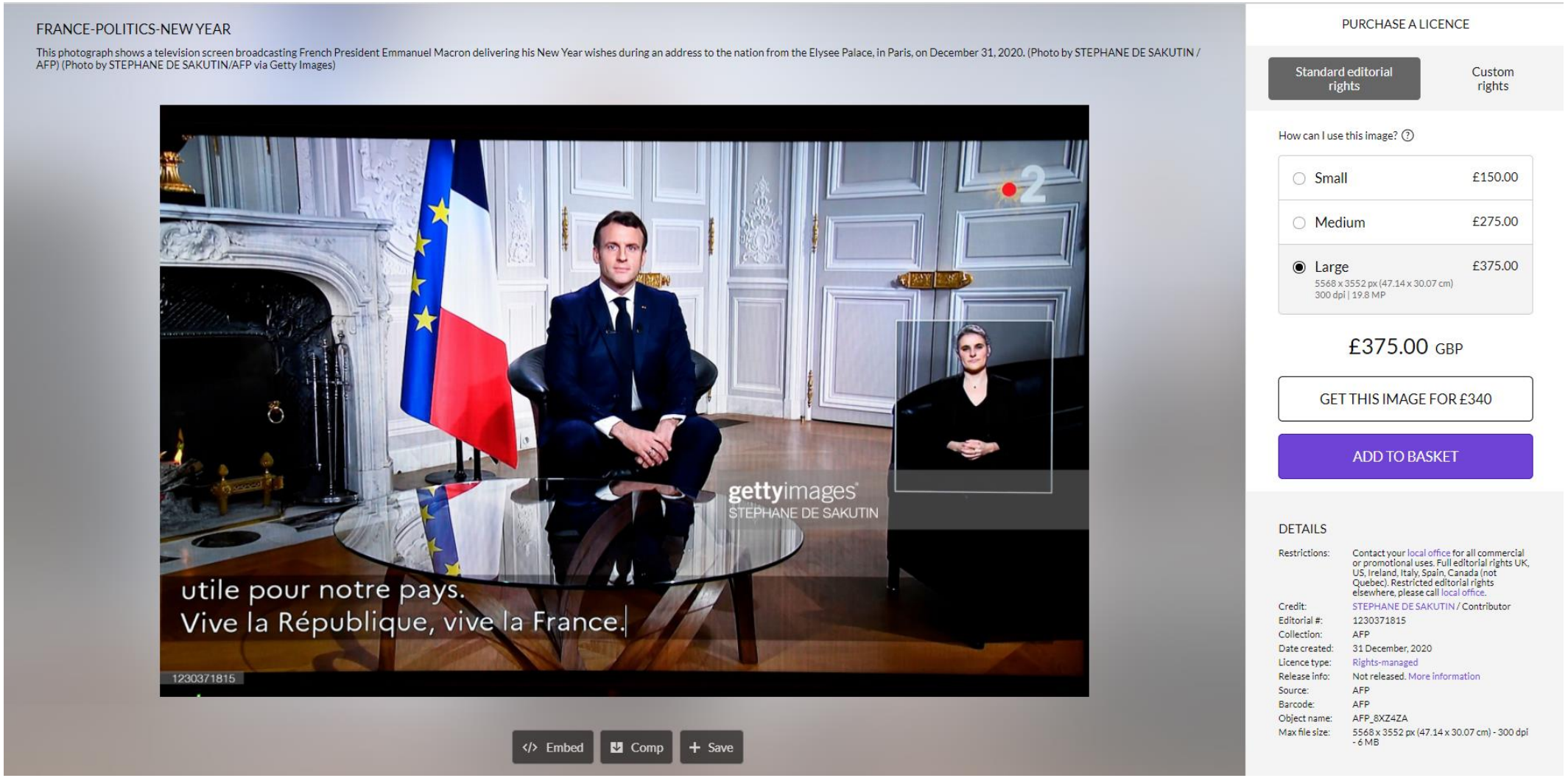
CATEGORY

VALUE

5.6.4 Attribution via the CAWG identity assertion



An example



Emmanuel Macron, © STEPHANE DE SAKUTIN, AFP, with the kind permission of Agence France-Presse

Exemplary attribution (Dublin Core™ metadata element set)


```
{
   "@context" : {
     "dc" : "http://purl.org/dc/elements/1.1/",
   },
   "dc:creator" : ["Stéphane de Sakutin", "self#jumbf=c2pa.assertions/cawg.identity"],
   "dc:identifier" : "AFP_8XZ4ZA",
   "dc:title" : "Address to the nation",
   "dc:subject" : ["France","Politics","New Year"],
   "dc:description" : "This photograph shows a television screen broadcasting French
President Emmanuel Macron delivering his New Year wishes during an address to the nation from
the Elysee Palace, in Paris, on December 31, 2020.",
   "dc:publisher" : "https://u.afp.com/5t5x",
   "dc:contributor" : ["Jeanne Parexemple", "self#jumbf=c2pa.assertions/cawg.identity_1"],
   "dc:date" : "2020-12-31T20:14:00Z",
   "dc:type" : "Image",
   "dc:source" : "France 2 broadcast",
   "dc:language" : "fr-FR",
   "dc:relation" :  ["AFP_8XZ4ZF","AFP_8XZ4YT"],
   "dc:coverage" :  ["Paris", "Elysée Palace"],
   "dc:rights" :  "self#jumbf=c2pa.assertions/jpt.rights"
}
```

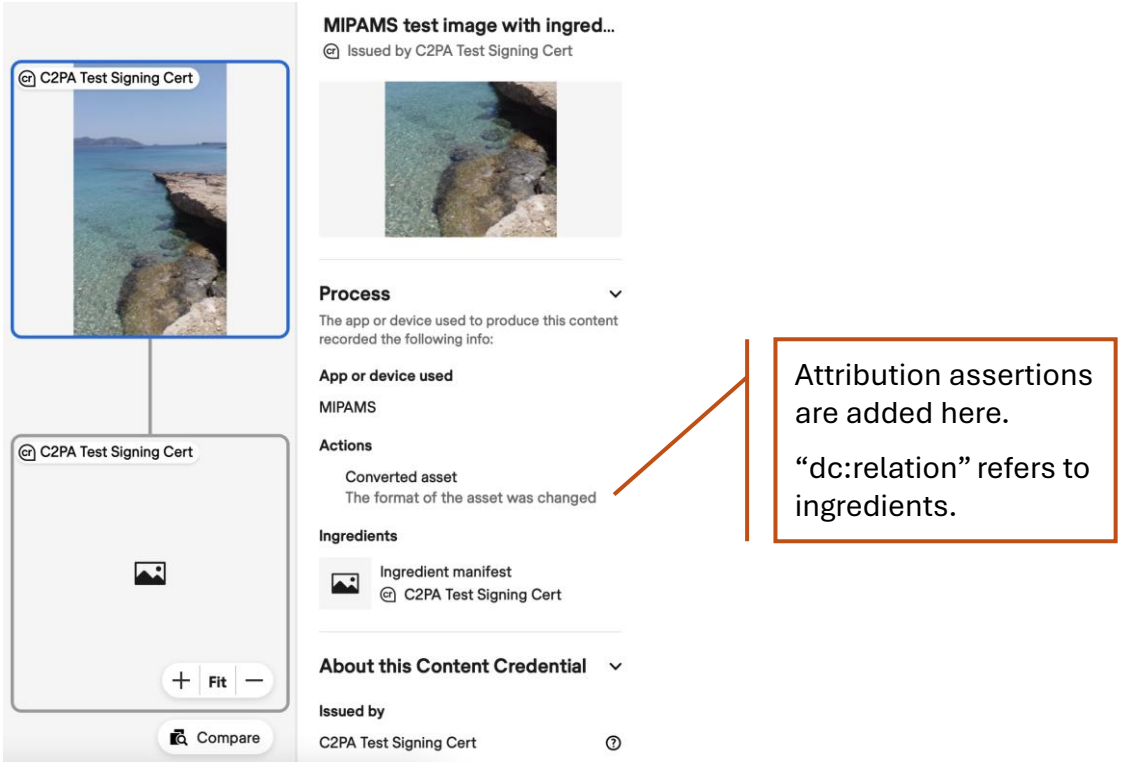

Exemplary terms and conditions (W3C® ODRL)

```
{
  "@context": "http://www.w3.org/ns/odrl.jsonld",
  "@type": "Agreement",
  "uid": "http://example.com/policy:42",
  "profile": "http://example.com/odrl:profile:09",
  "obligation": [{
    "assigner": "self#jumbf=c2pa.assertions/cawg.identity",
      "@type": "PartyCollection",
      "source": "http://example.com/org:43/rightsholders",
      "refinement": [{
        "rightsholder":"Stéphane",
        "role":"photographer",
        "percentage":"75"
                    },{
        "rightsholder":"Jeanne",
        "role":"editor",
        "percentage":"25"
                    }],
    "assignee": "http://example.com/org:44",
    "action": [{
      "rdf: value": {
        "@id": "odrl: compensate"
      },
      "refinement": [{
        "leftOperand": "payAmount",
        "operator": "eq",
        "rightOperand": { "@value": "5.00", "@type": "xsd:decimal" },
        "unit": "http://dbpedia.org/resource/Euro"
      }]
    }]
  }]
}
```

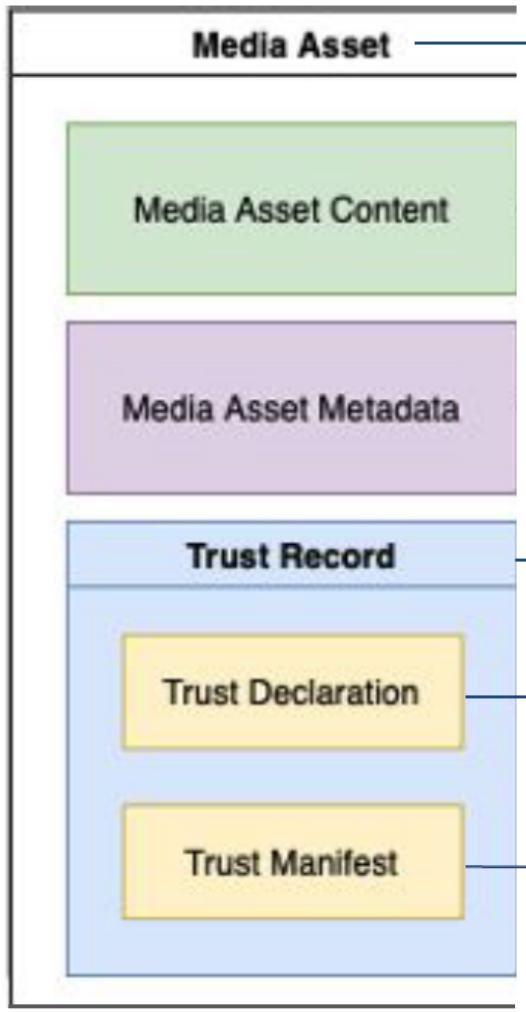
Reference software

MIPAMS JPEG Systems library extension for JPEG Trust leading to a JPEG Trust library to be used by end apps.

1) Support JPEG Trust content types and boxes:
   - JPEG Trust record (C2PA manifest store), declaration/standard/update/compressed manifest, claim, claim signature, assertion store
   - Salt box (c2sh) -> Included in the private field of each assertion JUMBF box for entropy.
2) Provide a ManifestBuilder interface to generate new manifest JUMBF boxes.
3) Provide initial test cases to create JPEG Trust records:
   - as standalone JUMBF boxes (.jumbf)
   - embedded in JPEG-1, JXL, JP2 encoded images.



JPEG Trust implementation as per January 2025



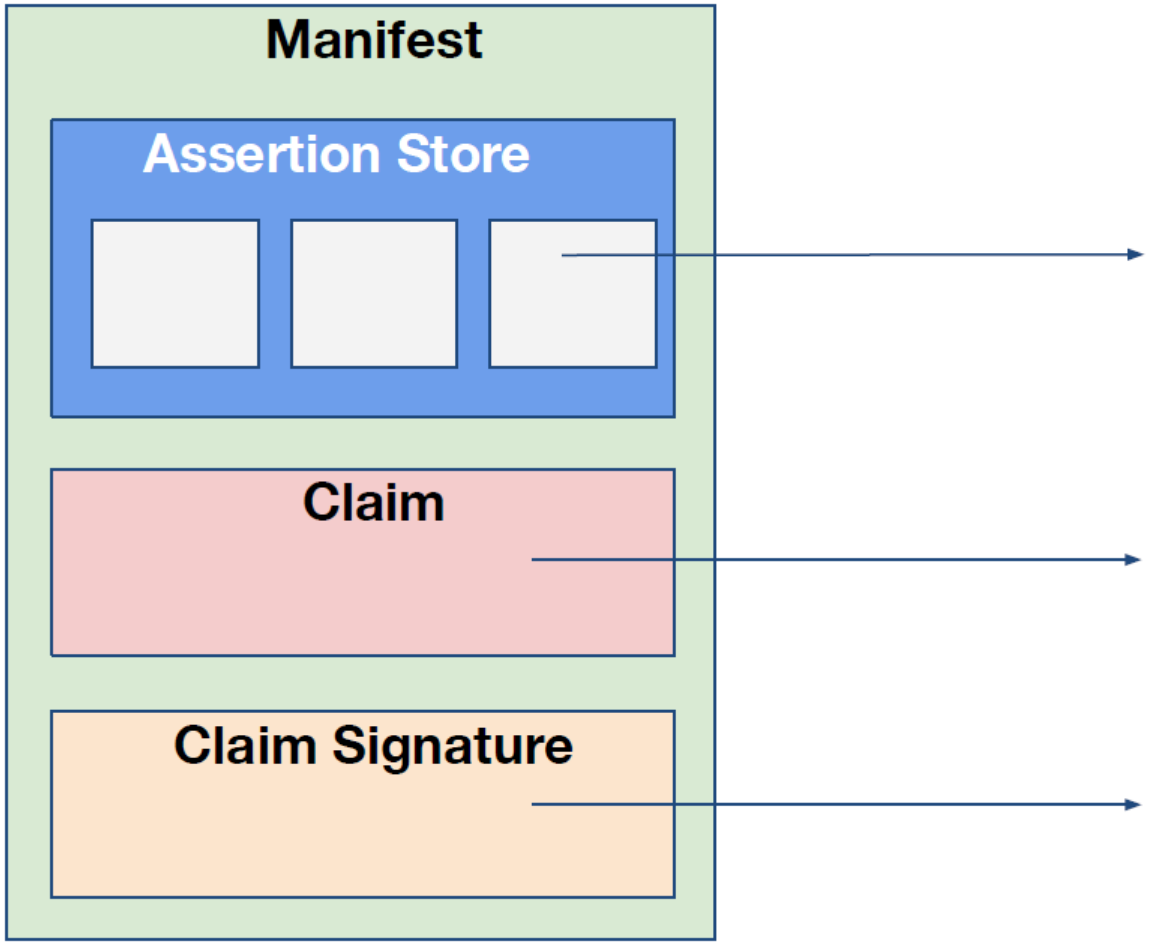
JPEG-1, JXL, JP2

Trust Record Content type

Trust Declaration Content type

Standard, Compressed, Update, Timestamp Content types

JPEG Trust implementation as per January 2025



- c2pa.hash.data,
- c2pa.actions, **c2pa.actions.v2**
- c2pa.thumbnail.claim,
- c2pa.thumbnail.ingredient
- c2pa.ingredient, **c2pa.ingredient.v3**
- c2pa.assertion.metadata
- (~15 assertions unsupported)

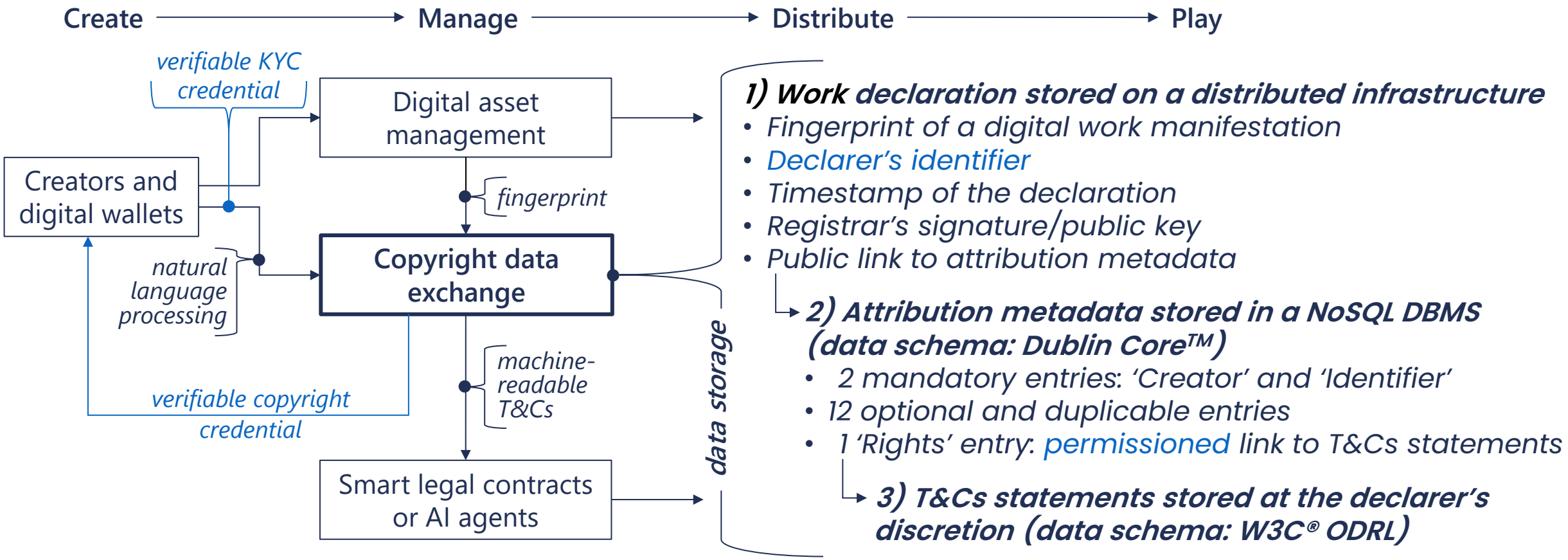
c2pa.claim, c2pa.claim.v2

c2pa.claim.signature

Verifiable credentials and storage of copyright data

valunode

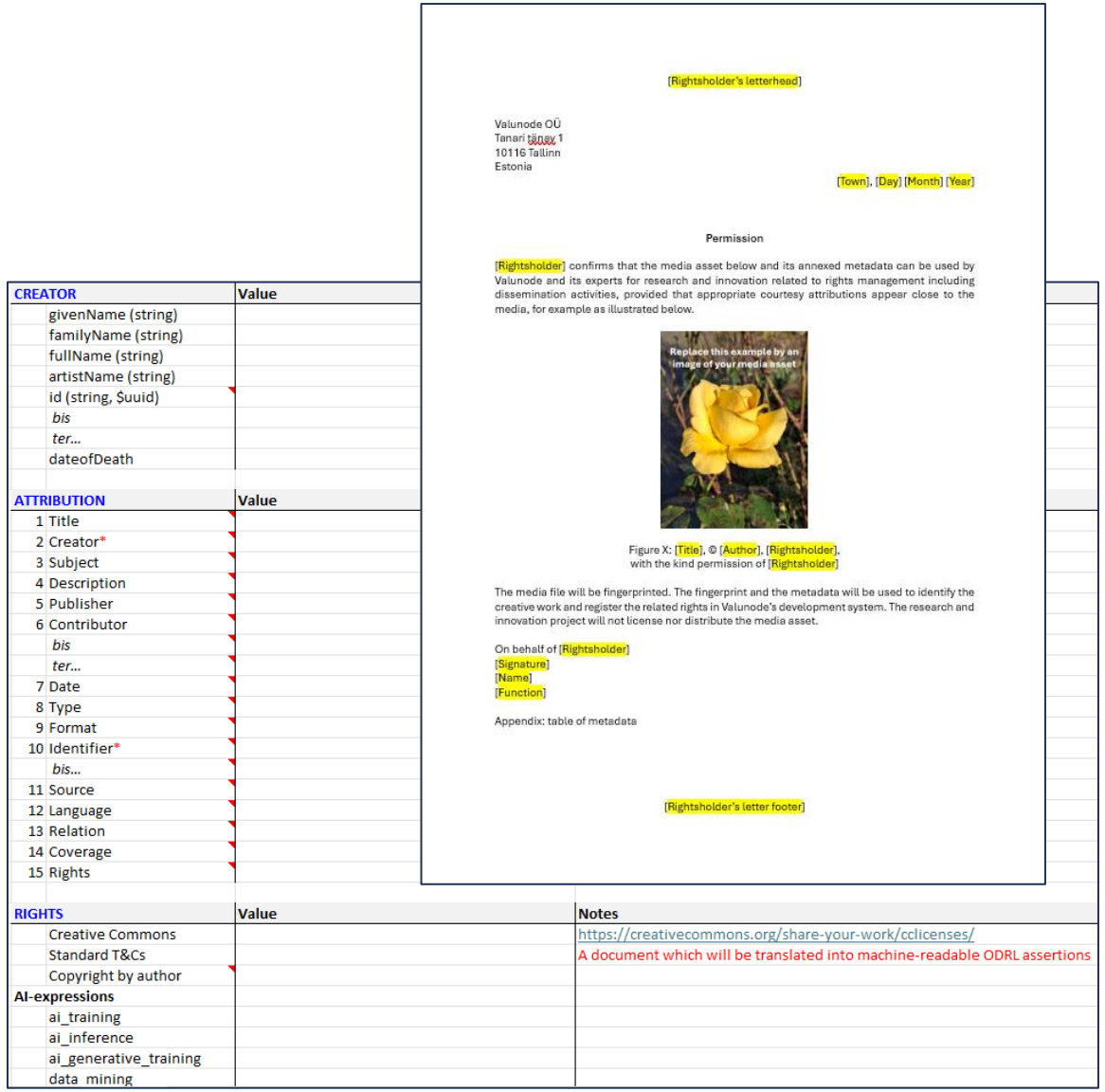
valunode stores data at 3 levels to protect privacy and trade secrets. The 2 first levels are included in the data exchange protocol. The 3rd level is accessed through permissioned APIs. At each level, access is granted on presentation of verifiable KYC credentials.



Real-world piloting in Spring 2025

valunode

1) Authenticate the declarer (verifiable KYC credential)
2) Fingerprint the photograph
3) Declare the creative work
4) Attribute the photograph
5) State Terms & Conditions (including AI reservations)
6) Issue attestation (verifiable copyright credential)



CREATOR	Value
givenName (string)	
familyName (string)	
fullName (string)	
artistName (string)	
id (string, $uuid)	
bis	
ter...	
dateofDeath	

	ATTRIBUTION	Value
1	Title	
2	Creator*	
3	Subject	
4	Description	
5	Publisher	
6	Contributor	
	bis	
	ter...	
7	Date	
8	Type	
9	Format	
10	Identifier*	
	bis...	
11	Source	
12	Language	
13	Relation	
14	Coverage	
15	Rights	

RIGHTS	Value	Notes
Creative Commons		https://creativecommons.org/share-your-work/cclicenses/
Standard T&Cs		A document which will be translated into machine-readable ODRL assertions
Copyright by author		
AI-expressions		
ai_training		
ai_inference		
ai_generative_training		
data_mining		

[Rightsholder's letterhead]

Valunode OÜ
Tanari tänav 1
10116 Tallinn
Estonia

[Town], [Day] [Month] [Year]

Permission

[Rightsholder] confirms that the media asset below and its annexed metadata can be used by Valunode and its experts for research and innovation related to rights management including dissemination activities, provided that appropriate courtesy attributions appear close to the media, for example as illustrated below.

Figure X: [Title], © [Author], [Rightsholder], with the kind permission of [Rightsholder]

The media file will be fingerprinted. The fingerprint and the metadata will be used to identify the creative work and register the related rights in Valunode's development system. The research and innovation project will not license nor distribute the media asset.

On behalf of [Rightsholder]
[Signature]
[Name]
[Function]

Appendix: table of metadata

[Rightsholder's letter footer]