Content Authenticity and PDF

Leonard Rosenthol
Chair, C2PA Technical Working Group

PDF Architect, Adobe
Content Authenticity Architect, Adobe

Zen Statement

- Consumers don’t know what to trust online

- They don’t have access to the provenance of assets they see

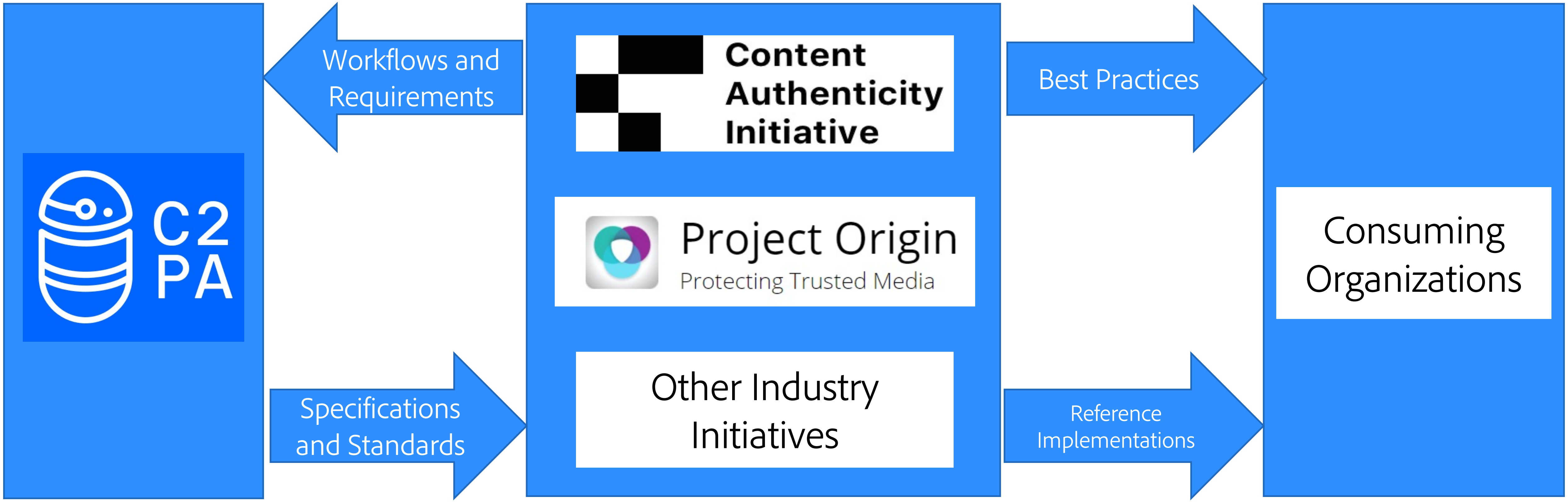
- We’re building trust by attaching attribution and history to assets

Standards Benefit Everyone

Coalition for Content Provenance and Authenticity (C2PA)

- The C2PA is a Joint Development Foundation project whose mission is to develop technical specifications that can establish content provenance and authenticity at scale to give publishers, creators, and consumers the ability to trace the origin of media.

Working Together



C2PA
Workflows and Requirements
Specifications and Standards
Content Authenticity Initiative
Project Origin
Protecting Trusted Media
Other Industry Initiatives
Best Practices
Reference Implementations
Consuming Organizations

Adobe arm BBC intel

Microsoft Truepic

General Members

france•tv numbers RIAA FOR MUSIC S L THE SOCIETY LIBRARY WITNESS SEE IT FILM IT CHANGE IT

Contributor Members

Akamai CBC Radio-Canada CLink dalet DIGIMARC fastly

MELCHER SYSTEM CONSULTING Ravnur SafeCast SERELAY TRUSTED MEDIA CAPTURE SERUM OF TRUTH COUNTER FAKE NEWS steg.ai

Web Commodore

What are we building?

Why attribution?

- ➢It’s not an arms race
- ➢Edits are good!
- ➢It’s another signal for detection

Instead of guessing what is fake, we can provide information about truth.

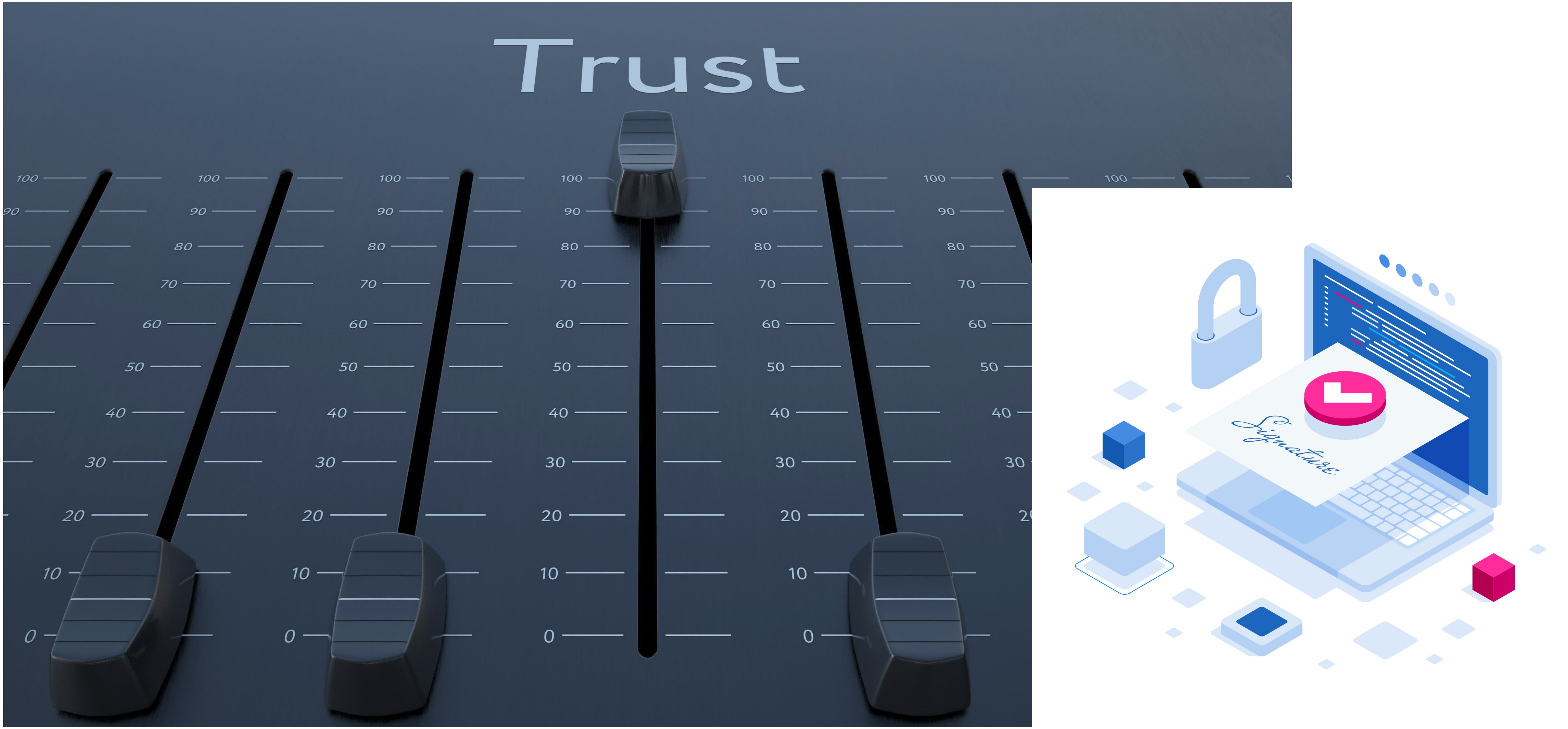
Attribution is….

Who?
What?
When?
Where?
Why?
How?

What is the C2PA Specification?

A model for storing and accessing cryptographically verifiable and tamper-evident information whose trustworthiness can be assessed based on a defined trust model.

Establishing Trust & Trustworthiness



Basics

- A simple structure for storing and accessing cryptographically verifiable metadata combined with both hard and soft bindings to the asset's content
- This metadata comprises statements regarding asset creation, authorship, edit actions, capture device details, software used and many other subjects. This makes up the provenance of a given asset.

(Some of our) Design Goals

- Create only the minimum required novel technology by relying on prior, battle-tested techniques.

- Do not require cloud storage but allow for it.

- Maintain an audit trail of claims across multiple tools, from asset creation through all subsequent modification and publication/distribution.

- Support all standard asset formats supported by common authoring tools, across media types such as images, videos, audio, and documents.

Draft Specification Available - https://c2pa.org/public-draft/

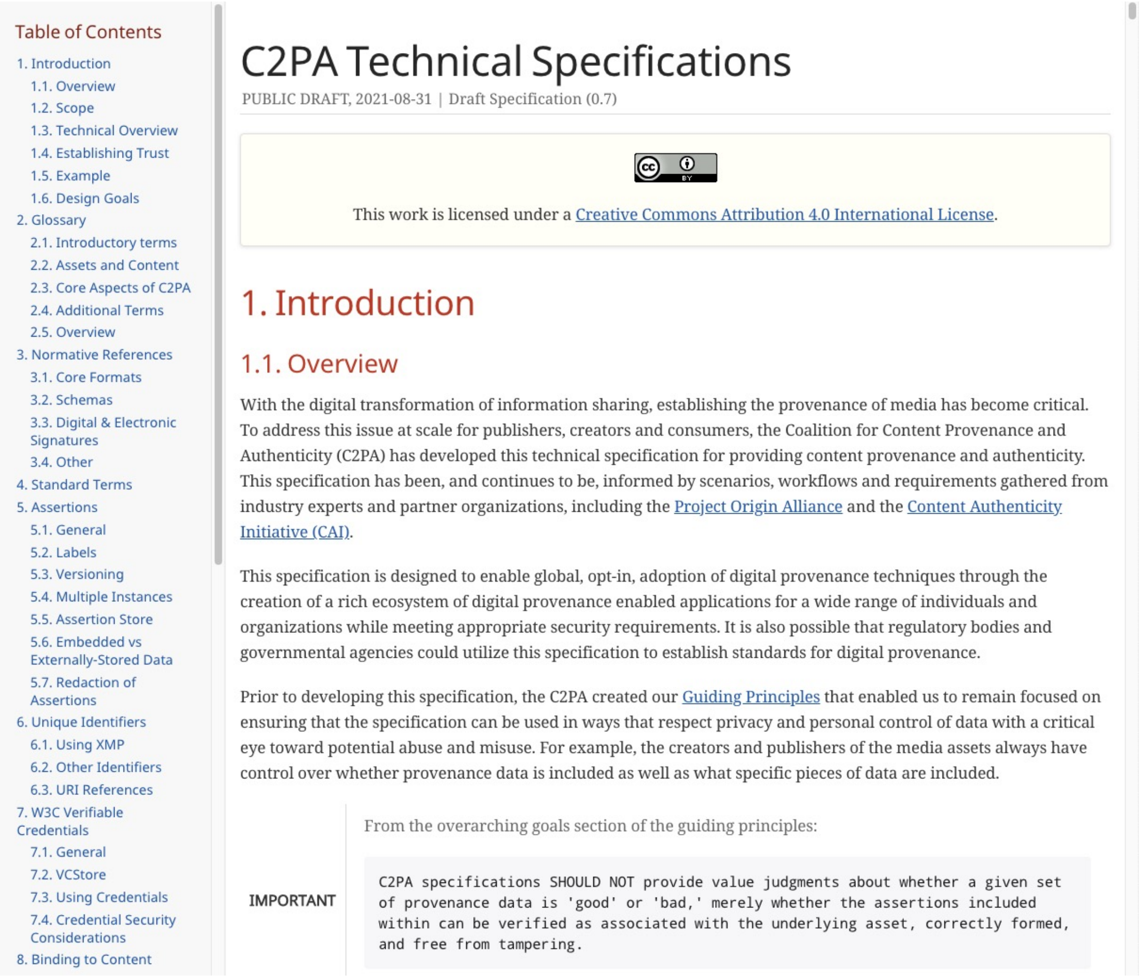


Table of Contents

C2PA Technical Specifications

PUBLIC DRAFT, 2021-08-31 | Draft Specification (0.7)

1. Introduction

1.1. Overview

With the digital transformation of information sharing, establishing the provenance of media has become critical. To address this issue at scale for publishers, creators and consumers, the Coalition for Content Provenance and Authenticity (C2PA) has developed this technical specification for providing content provenance and authenticity. This specification has been, and continues to be, informed by scenarios, workflows and requirements gathered from industry experts and partner organizations, including the Project Origin Alliance and the Content Authenticity Initiative (CAI).

This specification is designed to enable global, opt-in, adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance enabled applications for a wide range of individuals and organizations while meeting appropriate security requirements. It is also possible that regulatory bodies and governmental agencies could utilize this specification to establish standards for digital provenance.

Prior to developing this specification, the C2PA created our Guiding Principles that enabled us to remain focused on ensuring that the specification can be used in ways that respect privacy and personal control of data with a critical eye toward potential abuse and misuse. For example, the creators and publishers of the media assets always have control over whether provenance data is included as well as what specific pieces of data are included.

IMPORTANT

From the overarching goals section of the guiding principles:

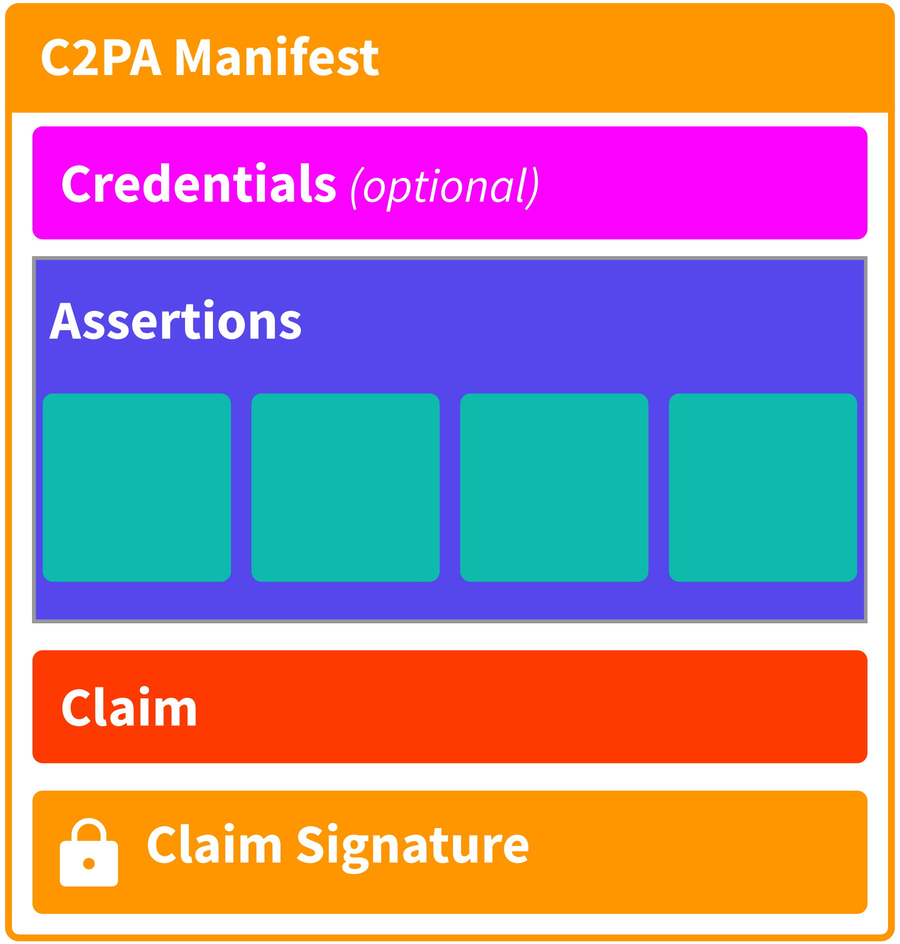
```
C2PA specifications SHOULD NOT provide value judgments about whether a given set
of provenance data is 'good' or 'bad,' merely whether the assertions included
within can be verified as associated with the underlying asset, correctly formed,
and free from tampering.
```

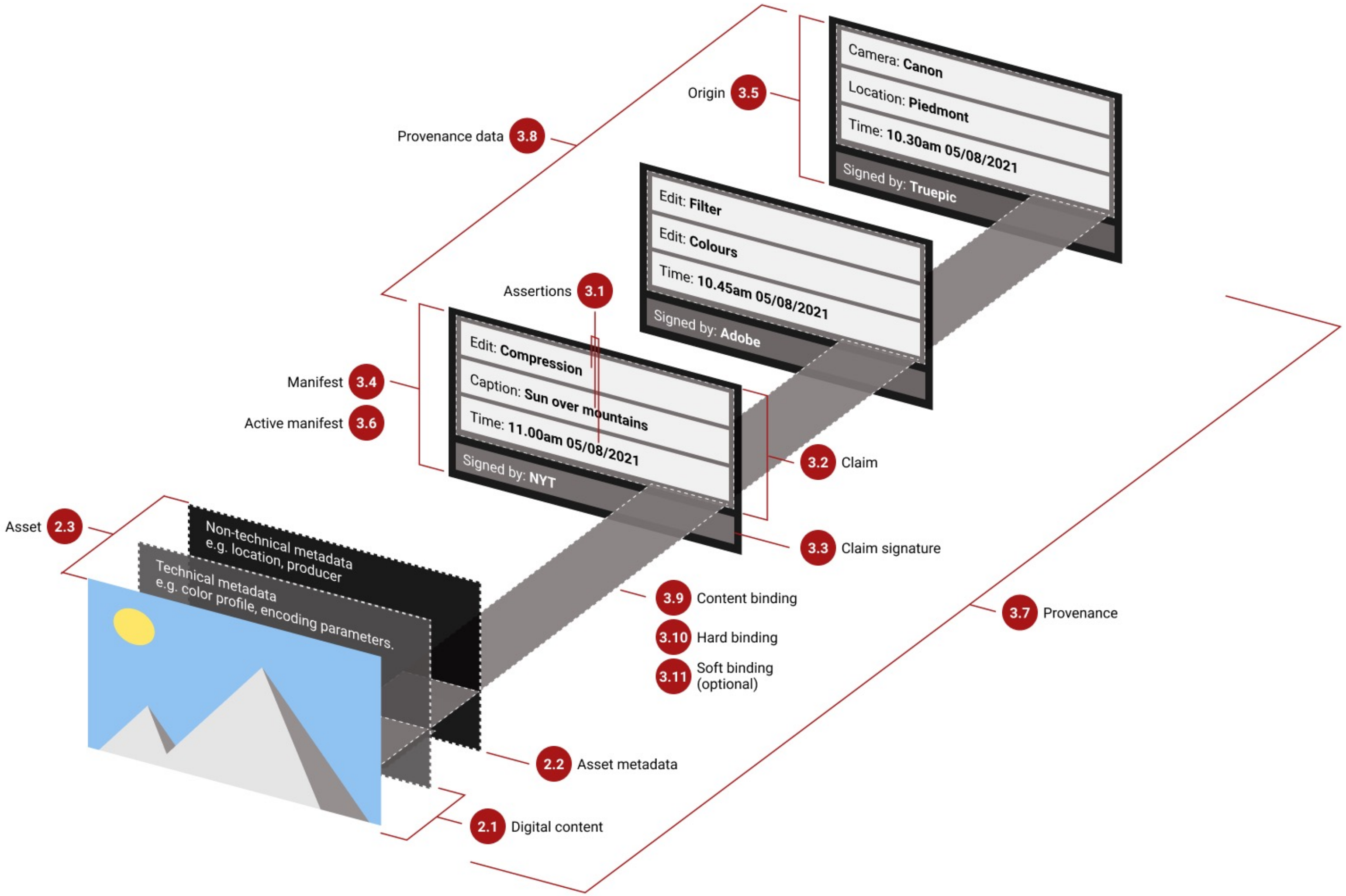
Core Technologies

- JSON
- CBOR
- eXtensible Metadata Platform (XMP)
- JPEG universal metadata box format (JUMBF)
- Cryptographic Message Syntax (CMS)
- CBOR Object Signing and Encryption (COSE)
  - NOTE: working with ETSI on an AdES for COSE (based on JAdES)

Core Components to C2PA

- Assertions
  - A series of statements that cover areas such as asset creation, authorship, edit actions, capture device details, bindings to content and many other subjects.
- Credentials
  - W3C Verifiable Credentials for any actor involved with an assertion.
- Claim
  - A digitally signed entity, created by a Claim Generator, that lists the assertions being made by the Signer.
- Claim signature
  - The digital signature on the claim using the private key of an actor. This data is a part of the manifest.
- Manifest
  - A verifiable unit into which assertions, claims, credentials and signatures are all bound together. The set of manifests, as stored in the asset's Manifest Store, represent its provenance data.




Provenance data 3.8
Origin 3.5
Camera: Canon
Location: Piedmont
Time: 10.30am 05/08/2021
Signed by: Truepic
Edit: Filter
Edit: Colours
Time: 10.45am 05/08/2021
Signed by: Adobe
Assertions 3.1
Edit: Compression
Caption: Sun over mountains
Time: 11.00am 05/08/2021
Signed by: NYT
Manifest 3.4
Active manifest 3.6
3.2 Claim
3.3 Claim signature
Asset 2.3
Non-technical metadata
e.g. location, producer
Technical metadata
e.g. color profile, encoding parameters.
3.9 Content binding
3.10 Hard binding
3.11 Soft binding (optional)
3.7 Provenance
2.2 Asset metadata
2.1 Digital content

Action Assertion

```
{ "actions": [

{ "action": "c2pa.edited", "when": 0("2020-02-11T09:00:00Z"),

"softwareAgent": "Adobe Acrobat DC 2020 for Windows",

"changed": "change1,change2",

"instanceID": 37(h'ed610ae51f604002be3dbf0c589a2f1f'),

"actor": [ {

"credentials": [ {

"url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-
329BF39FA1E4/c2pa.credentials/Joe_Bloggs",

"alg": "sha256",

"hash": b64'hoOspQQ1lFTy/4Tp8Epx670E5QW5NwkNR+2b30KFXug=‘ }]

}]

},
```

```
{

"action": "c2pa.placed",

"when": 0("2020-02-11T09:00:00Z"),

"softwareAgent": "Adobe Acrobat DC 2020 for Windows",

"name": "merged.pdf",

"manifest": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-
329BF39FA1E4"

}]

}
```

Creative Work Assertion

```
{"@type": "CreativeWork",
"datePublished": "2021-05-20T23:02:36+00:00",
"publisher": {"name": "BBC News",
"publishingPrinciples": "https://www.bbc.co.uk/news/help-41670342",
"logo": "https://m.files.bbci.co.uk/modules/bbc-morph-news-waf-page-meta/5.1.0/bbc_news_logo.png",
"parentOrganization": {
          "name": "BBC",
          "legalName": "British Broadcasting Corporation"
}
},
"url": "https://www.bbc.co.uk/news/av/world-europe-57194011",
"identifier": "p09j7vzv",
"producer": {
  "identifier": "https://en.wikipedia.org/wiki/Joe_Bloggs",
  "name": "Joe Bloggs",
  "credential": [ {
    "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2pa.credentials/Joe_Bloggs",
    "alg": "sha256",
    "hash": "Auxjtmax46cC2N3Y9aFmBO9Jfay8LEwJWzBUtZ0sUM8gA"
  }]
},
"copyrightHolder": {
          "name": "BBC",
          "legalName": "British Broadcasting Corporation"
},
"copyrightYear": 2021,
"copyrightNotice": "Copyright © 2021 BBC."
}
```

Data Hash Assertion

```
{
  "exclusions": [
  {
    "start": 9960,
    "length": 4213
  }
  ],
  "name": "JUMBF manifest",
  "alg" : "sha256",
  "hash": "Auxjtmax46cC2N3Y9aFmBO9Jfay8LEwJWzBUtZ0sUM8gA=",
  "pad" : " "
}
```

Example Claim

```
{

  "claim_generator": "Joe's PDF Editor/2.0 (Windows 10)",

  "signature" : "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2pa.signature",

  "alg" : "sha256", "dc:format": "application/pdf",

  "assertions" : [

    { "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-
329BF39FA1E4/c2pa.assertions/c2pa.hash.data",

      "hash": b64'U9Gyz05tmpftkoEYP6XYNsMnUbnS/KcktAg2vv7n1n8=‘ },

    { "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2pa.assertions/c2pa.actions",

      "hash": b64'G5hfJwYeWTlflxOhmfCO9xDAK52aKQ+YbKNhRZeq92c=‘ },

    { "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2pa.assertions/stds.schema-
org.CreativeWork",

      "hash": b64'Yzag4o5jO4xPyfANVtw7ETlbFSWZNfeM78qbSi8Abkk=‘ } ],

}
```

Claim Signature

- X.509-based certificates
  - Though the specification is open to other forms in the future
- Common algorithms
  - ECDSA, RSASSA-PSS, adding Ed25519
- COSE (vs. CMS)
  - Aligns with our use of CBOR for assertions & claims
  - Safer (more secure) than CMS with respect to parsing and implementations
  - *BUT* its newer, so less existing implementations to choose from

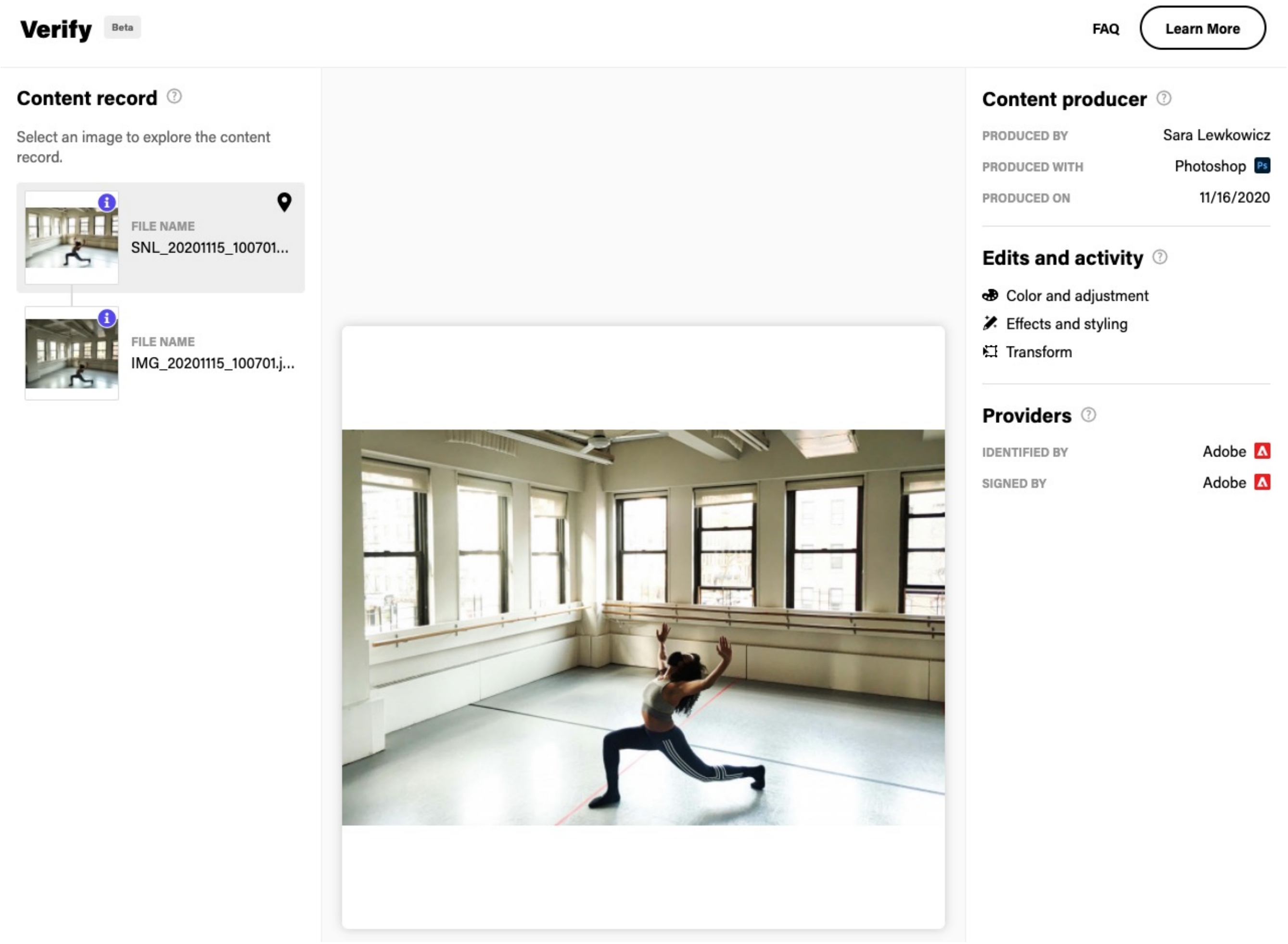
Connecting C2PA with PDF

- C2PA Manifest is embedded into a PDF as an embedded file
  - An embedded file specification (ISO 32000, 7.11.3) which is referenced from the **EmbeddedFiles** NameTree (`/Catalog/Names/EmbeddedFiles`) as well as the value of the **AF** key in the document catalog dictionary. The file specification dictionary shall have an **AFRelationship** key whose value is *C2PA_Manifest*.
- In each update, you need only include the new manifest with references back to the previous manifest (as the *parent* ingredient).

More on C2PA and PDF

- Although the PDF is already ”signed” as part of C2PA, it might be useful to add a PDF signature (certifying or approval). PDF signing **MUST** take place **AFTER** the application of the C2PA manifest, though some “trickery” is involved. (but that also means better compatibility with PDF)
    - Size and location of the PDF signature ”hole” must be known prior to completion of the C2PA manifest
        - The ”hole” is the added to the list of exclusions in the data.hash assertion.
- Encrypted PDFs are supported, but the embedded file needs to have the *Identity* crypt filter

verify.contentauthenticity.org



Verify Beta

FAQ

Learn More

Content record

Select an image to explore the content record.

FILE NAME
SNL_20201115_100701...

FILE NAME
IMG_20201115_100701.j...

Content producer

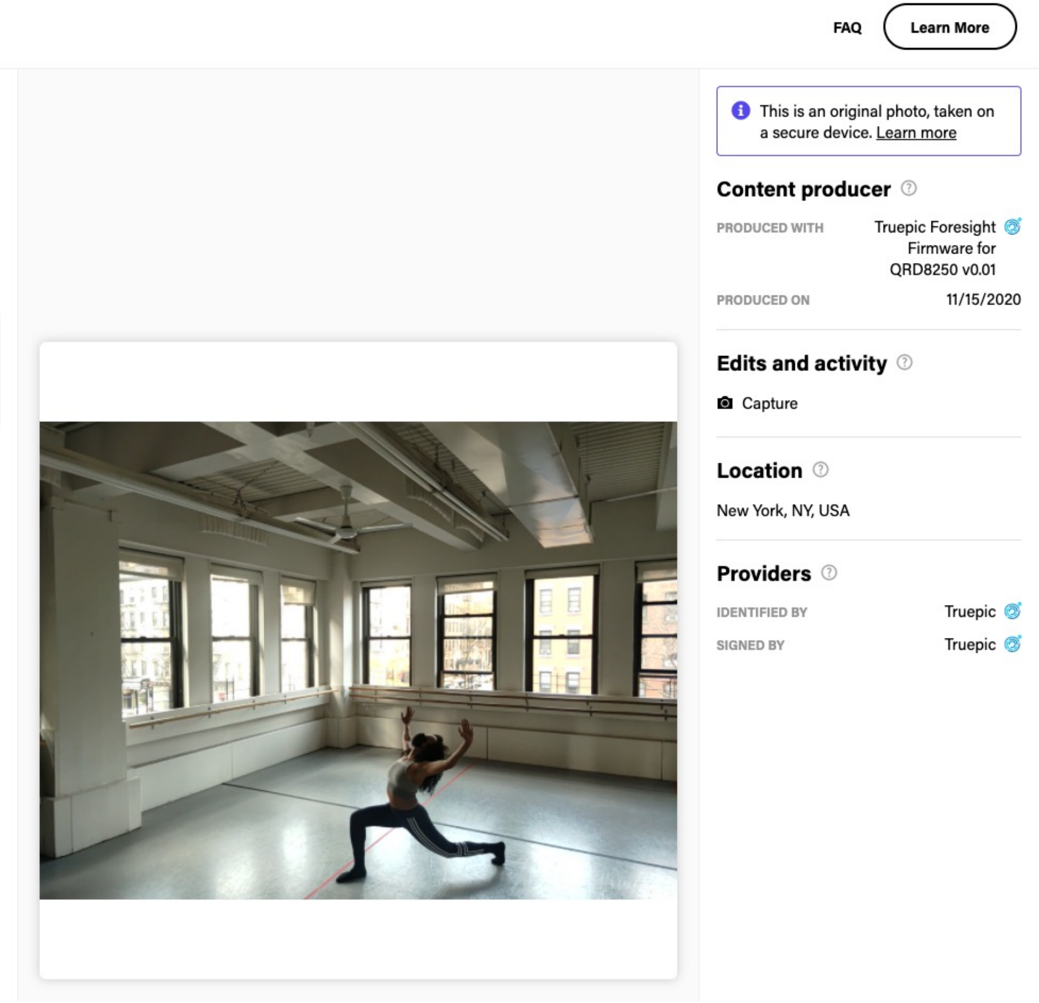
PRODUCED BY	Sara Lewkowicz
PRODUCED WITH	Photoshop
PRODUCED ON	11/16/2020

Edits and activity

- Color and adjustment
- Effects and styling
- Transform

Providers

IDENTIFIED BY	Adobe
SIGNED BY	Adobe



FAQ

Learn More

This is an original photo, taken on a secure device. Learn more

Content producer

PRODUCED WITH	Truepic Foresight Firmware for QRD8250 v0.01
PRODUCED ON	11/15/2020

Edits and activity

- Capture

Location

New York, NY, USA

Providers

IDENTIFIED BY	Truepic
SIGNED BY	Truepic

https://verify.contentauthenticity.org/inspect?tour=1&source=https%3A%2F%2Fverify.contentauthenticity.org%2Fsdk%2Fstatic%2Fsample-images%2FSNL_20201115_100701_M.jpg

In Closing

- Increasing trust in media requires the ongoing engagement of diverse communities.
  - Which is why we are engaging with the PDF Association!
- The C2PA does not prescribe a unified single platform for authenticity, but instead presents a set of standards that can be used to create and reveal attribution and history for images, documents, time-based media (video, audio) and streaming content.
- PDF is one of the key formats that C2PA has defined support for since its original specification and one we look forward to seeing implementations of in conjunction with the release of the specification.

Questions

Adobe

Establishing Trust & Trustworthiness

- C2PA Trust Model
  - The basis of making trust decisions in C2PA is the identity of the actor associated with the cryptographic signing key used to sign the claim in the active manifest.
  - The identity of a signatory is not necessarily a human actor, and the identity presented may be a pseudonym, completely anonymous, or pertain to a service or trusted hardware device with its own identity, including an application running inside such a service or trusted hardware.
- Trust Signals
  - Assertions make up the provenance of a given asset and represent a series of trust signals that can be used by a human to improve their view of trustworthiness concerning the asset.