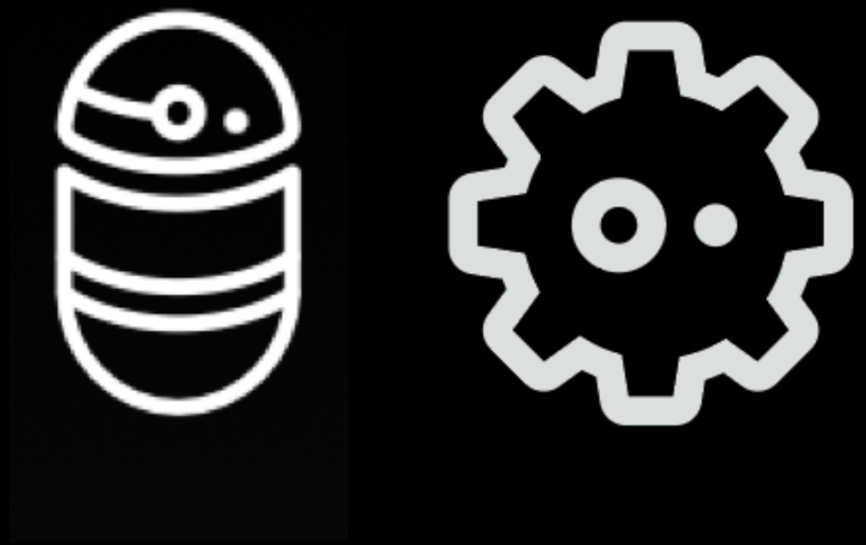
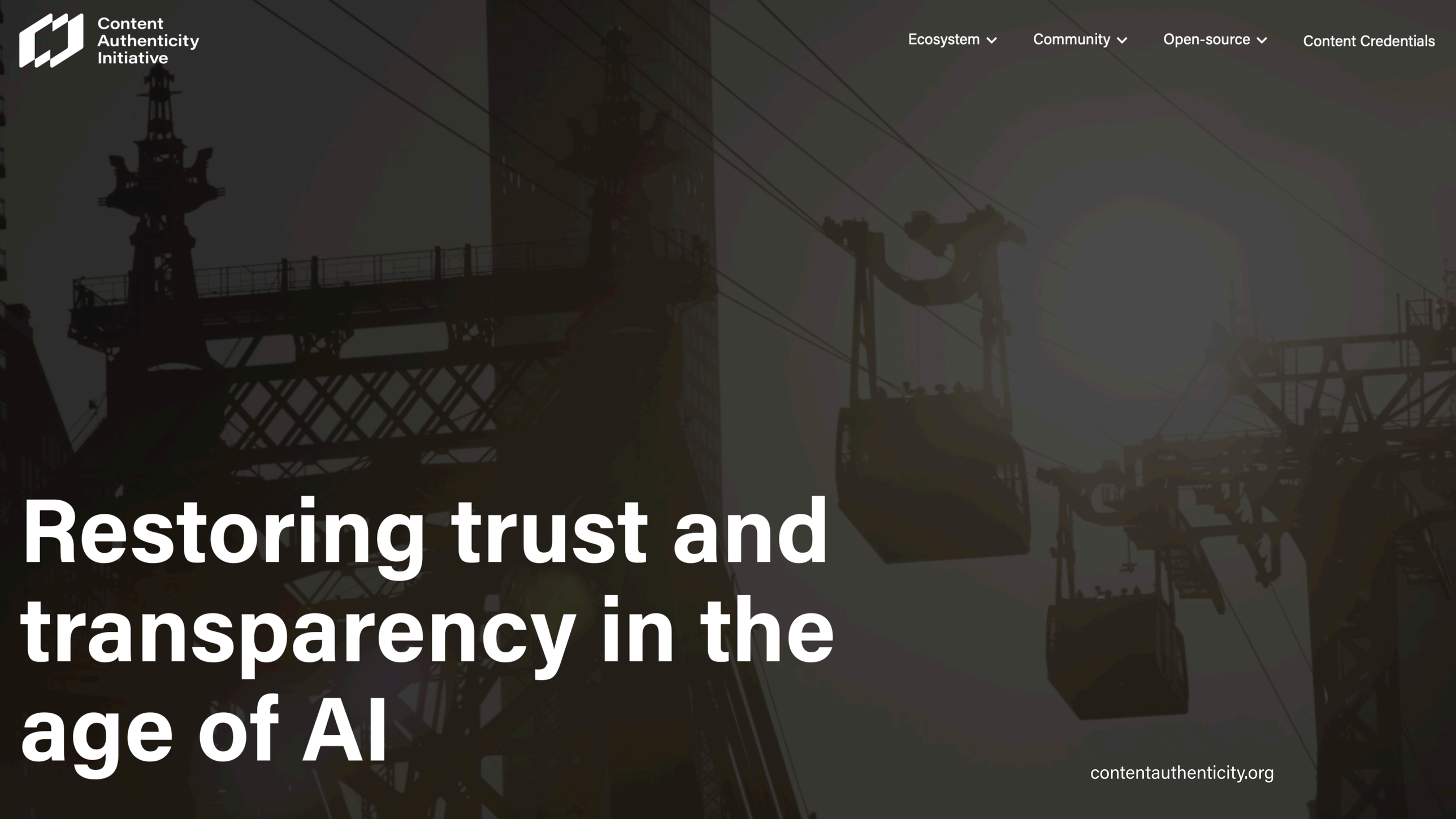


C2PA + CAWG

Building identity into the content provenance ecosystem

Eric Scouten · Principal Scientist and Identity Architect, CAI · Adobe
Scott Perry · Digital Governance Institute

IIW 42 · 28 April 2026


Content
Authenticity
Initiative
Ecosystem
Community
Open-source
Content Credentials
Restoring trust and transparency in the age of AI
contentauthenticity.org

The problem, in a nutshell

On the Internet …

digital media content

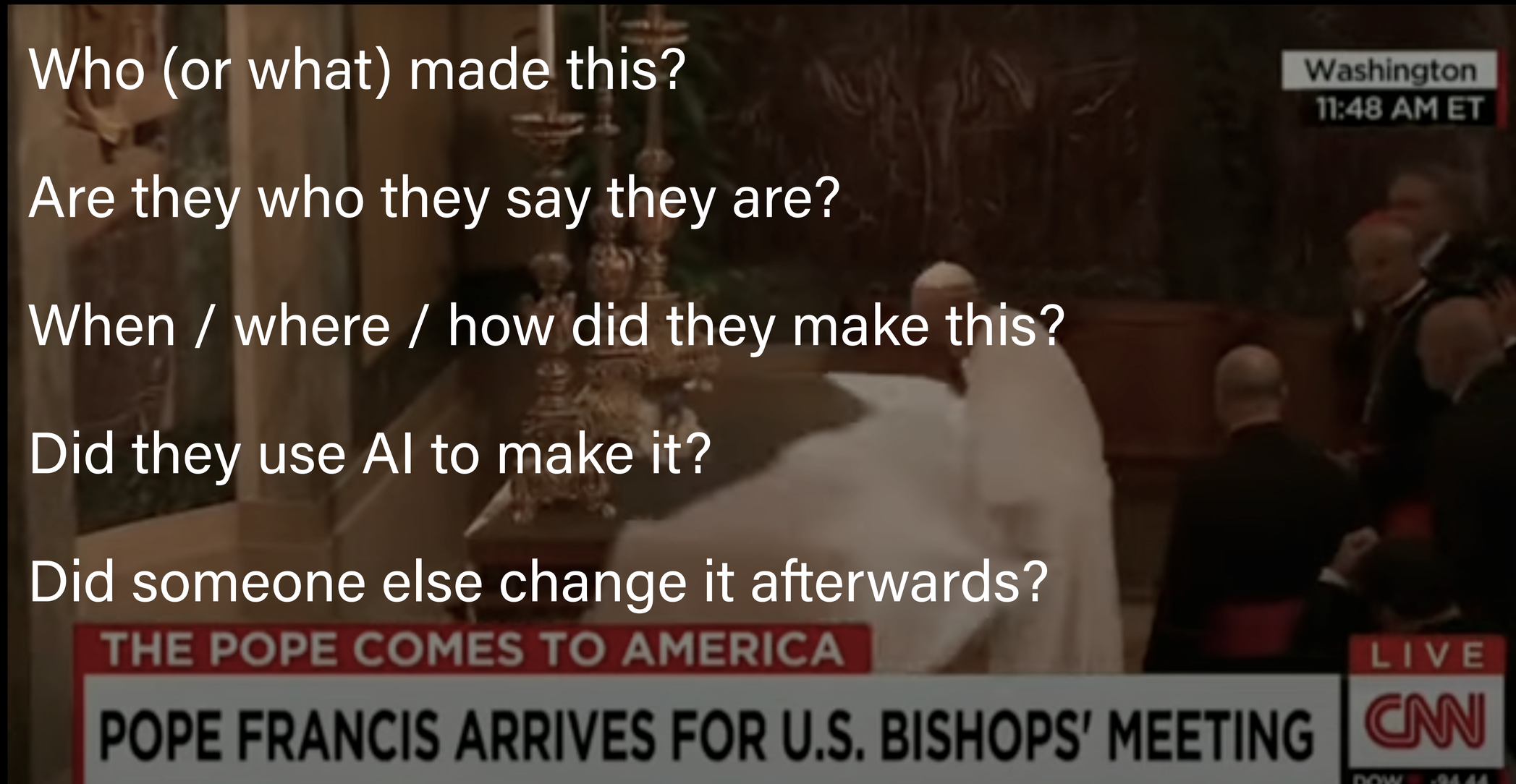
can travel from a **content creator**

to **unforeseen recipients**

via **unknown channels**.

You might ask yourself …

- Who (or what) made this?
- Are they who they say they are?
- When / where / how did they make this?
- Did they use AI to make it?
- Did someone else change it afterwards?



A tamper-evident digital “nutrition label”

We provide tools for digital **content creators** …

- Hardware and software **tool vendors** – and
- Individual and organizational **content creators**

… to describe and sign their work.

The three Cs … who does what here?

What and how
C2PA

Coalition for Content Provenance and Authenticity

c2pa.org

Who
CAWG

Creator Assertions Working Group *(part of DIF)*

cawg.io

Advocacy and education
contentauthenticity.org

Who is taking accountability?

C2PA claim generator

Hardware or software tool involved in creating the content.

CAWG named actor

Individual or organization involved in creating the content.

What are they taking responsibility for?

C2PA claim generator
can describe ...

- GPS data / time of capture (if known to hardware)
- Edit actions taken / AI used
- Ingredients incorporated into content

CAWG named actor
can describe ...

- Individuals or organizations involved in *creating* content
- Events or locations *depicted* in content
- Metadata / context for content

Two responsible parties, two signatures

C2PA claim generator

- X.509 certificate / COSE signature
- **NEW** (July 2025): Certificates have C2PA-specific key usage, not interoperable with other purposes
- Issued to hardware or software that demonstrates compliance with C2PA rules

CAWG named actor

- **Flexible** *framework* for using multiple kinds of digital credentials
- Intended to bind credential to content
- Optional – for those that wish to identify themselves as content creator

C2PA data model

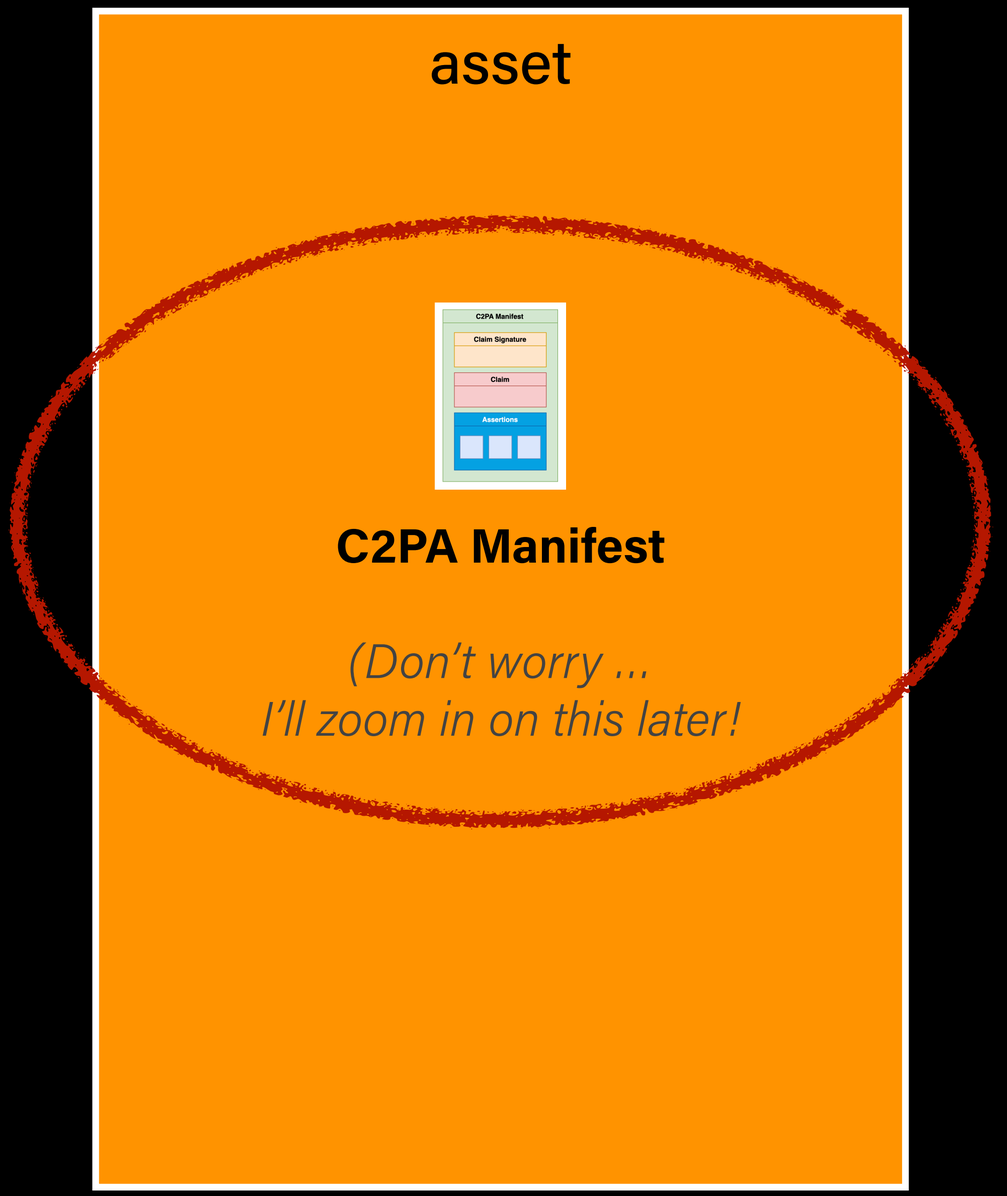
C2PA data model

Overview

An **asset** is any piece of digital media that we wish to describe.

Currently, we support still images, motion pictures, recorded audio, documents (PDF), fonts, and more.

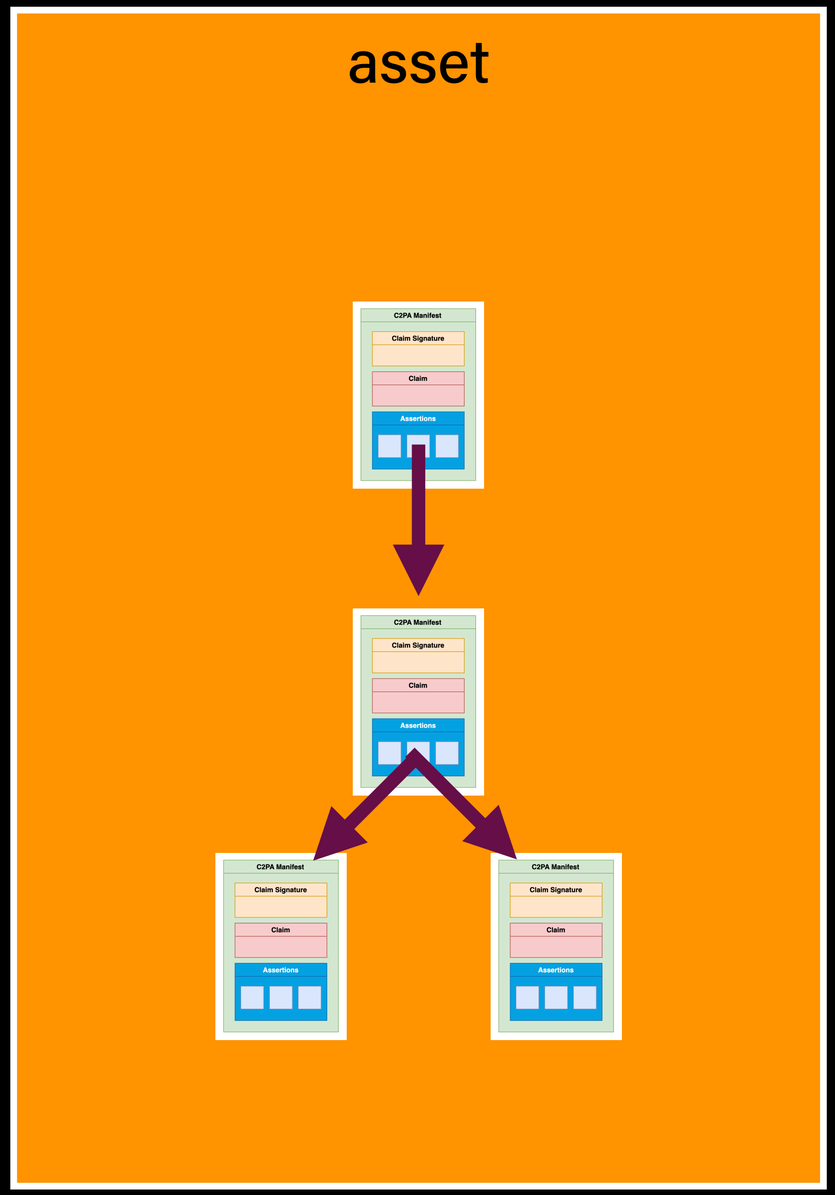
An asset is described by a **C2PA Manifest**.



C2PA data model

Overview

A C2PA Manifest can refer to any number of *ingredient manifests* when earlier content is incorporated and composed into a new asset.



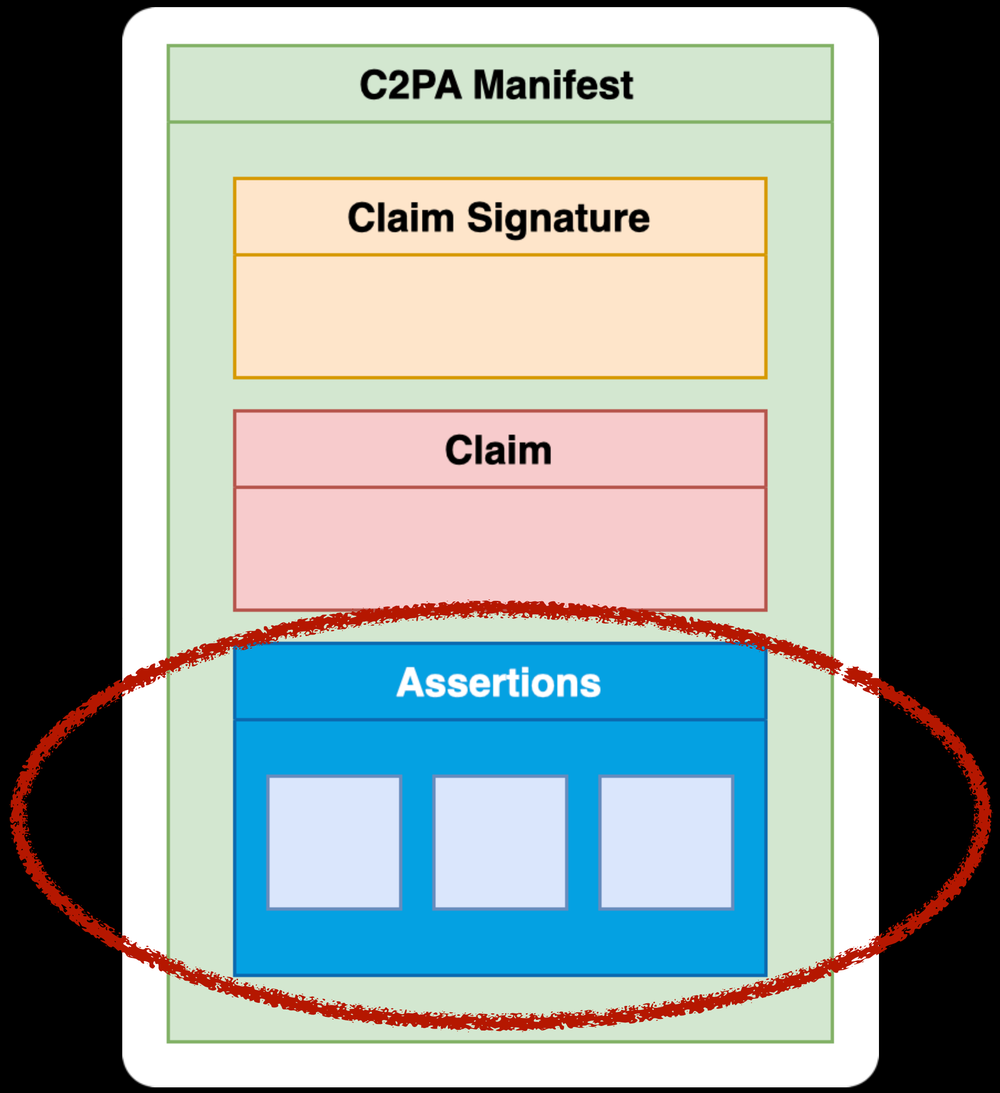
C2PA data model

Assertions

Assertions are opt-in statements that cover areas such as:

- hard binding to asset's binary content
- capture device details
- edit actions
- thumbnail of the content
- other content (ingredients) that were incorporated into this content

This mechanism is **extensible.**

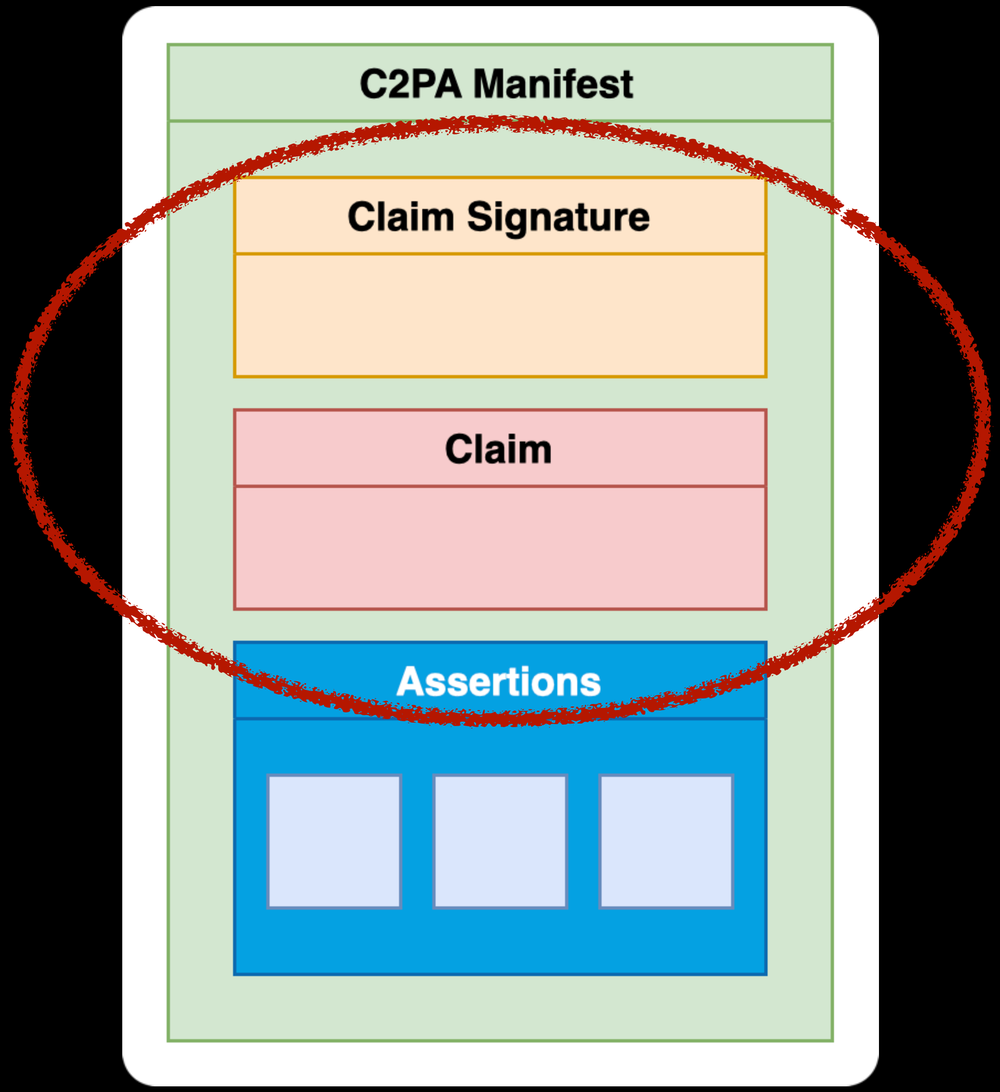


C2PA data model

Claim

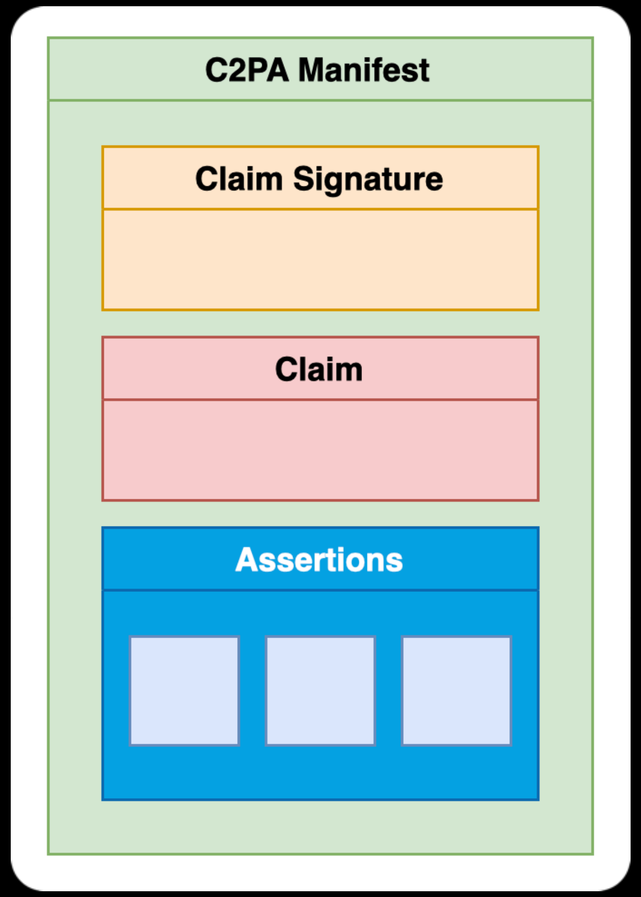
Every C2PA Manifest has exactly one **claim,** which lists the assertions and describes the claim generator (tool that built the Manifest).

This claim is signed using an X.509 certificate, which provides evidence of the tool used and provides tamper evidence if a third party attempts to change the claim after the fact.

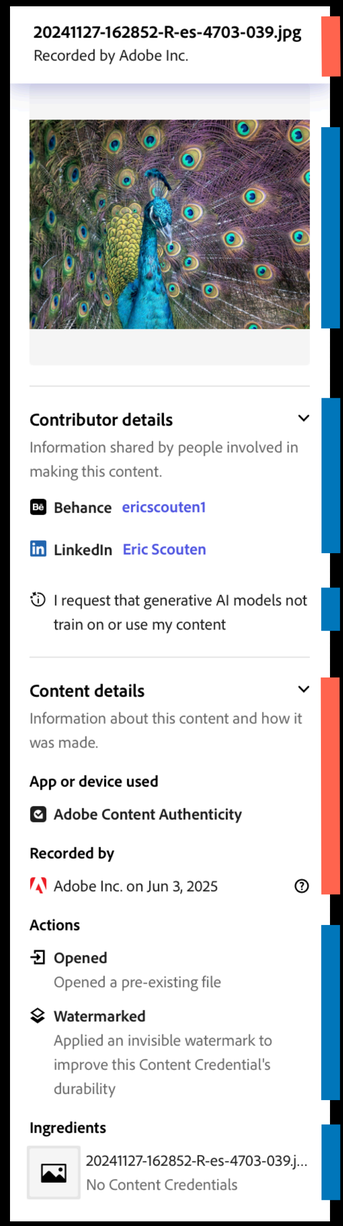


C2PA data model

How we display it



contentauthenticity.adobe.com/inspect



claim generator (C2PA)

thumbnail assertion (C2PA)

identity assertion (CAWG)

training + data mining assertion (CAWG)

claim generator (C2PA)

actions assertion (C2PA)

ingredients assertion (C2PA)

Introducing CAWG

CAWG (Creator Assertions Working Group)

was created in early 2024 to create technical standards to house metadata sourced from individual and organizational content creators.

CAWG became a working group within DIF in March 2025.

What does CAWG do?

Four assertion standards, building on C2PA technical spec:

- **Endorsement** ► Forward permission for CDN-style renditions on C2PA assets
- **Identity** ► Binding digital identity credentials to C2PA assets
- **Metadata** ► Associate user-generated metadata with C2PA assets
- **Training and Data Mining** ► Express permissions regarding AI training and data mining usage

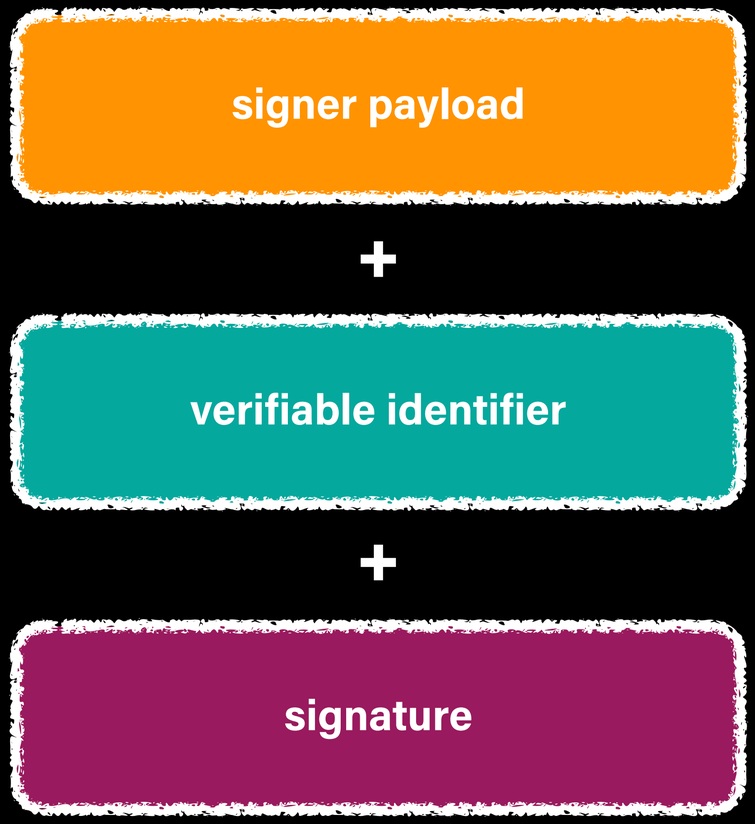
What does CAWG do?

Four assertion standards, building on C2PA technical spec:

- **Endorsement** ► Forward permission for CDN-style renditions on C2PA assets
- **Identity** ► Binding digital identity credentials to C2PA assets
- **Metadata** ► Associate user-generated metadata with C2PA assets
- **Training and Data Mining** ► Express permissions regarding AI training and data mining usage

Identity assertion

is a framework



A **signed assertion** that
this credential subject created*
this – and *only* this –
content.

* or edited / published / translated / re-rendered / etc. ...

Identity assertion

Data model

signer payload

verifiable identifier

signature

Identity assertion (CBOR)

```
{
  "signer_payload": {
    "sig_type": "cawg.x509.cose",
    "referenced_assertions": [
      {
        "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
        "hash": b64'U9Gyz05tmpftkoEYP6XYNsMnUbnS/KcktAg2vv7n1n8='
      },
      {
        "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
        "hash": b64'G5hfJwYeWTlflxOhmfCO9xDAK52aKQ+YbKNhRZeq92c='
      },
      {
        "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
        "hash": b64'Yzag4o5jO4xPyfANVtw7ETlbFSWZNfeM78qbSi8Abkk='
      }
    ],
    "role": ["cawg.creator"],
  },
  "signature": b64'....', // COSE signature
  "pad1": b64'....', // zero-filled pad buffer
  "pad2": b64'....'  // zero-filled pad buffer
}
```

Identity assertion

What is a signer payload?

signer payload

(cryptographic description of digital media asset)

Identity assertion (CBOR)

`sig_type`

What type of credential was used?

```
{
"signer_payload": {
  "sig_type": "cawg.x509.cose",
  "referenced_assertions": [
    {
      "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
      "hash": b64'U9Gyz05tmpftkoEYP6XYNsMnUbnS/KcktAg2vv7n1n8='
    },
    {
      "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
      "hash": b64'G5hfJwYeWTlflxOhmfCO9xDAK52aKQ+YbKNhRZeq92c='
    },
    {
      "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
      "hash": b64'Yzag4o5jO4xPyfANVtw7ETlbFSWZNfeM78qbSi8Abkk='
    }
  ],
  "role": ["cawg.creator"],
},
 "signature": b64'....', // COSE signature
 "pad1": b64'....', // zero-filled pad buffer
 "pad2": b64'....'  // zero-filled pad buffer
}
```

Identity assertion

What is a signer payload?

signer payload

(cryptographic description of digital media asset)

Identity assertion (CBOR)

```
{
 "signer_payload": {
  "sig_type": "cawg.x509.cose",
  "referenced_assertions": [
   {
    "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
    "hash": b64'U9Gyz05tmpftkoEYP6XYNsMnUbnS/KcktAg2vv7n1n8='
   },
   {
    "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
    "hash": b64'G5hfJwYeWTlflxOhmfCO9xDAK52aKQ+YbKNhRZeq92c='
   },
   {
    "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
    "hash": b64'Yzag4o5jO4xPyfANVtw7ETlbFSWZNfeM78qbSi8Abkk='
   }
  ],
  "role": ["cawg.creator"],
 },
 "signature": b64'....', // COSE signature
 "pad1": b64'....', // zero-filled pad buffer
 "pad2": b64'....'  // zero-filled pad buffer
}
```

`referenced_assertions`

What part of the asset is the credential subject taking responsibility for?

IMPORTANT: Must include hard binding.

Identity assertion

What is a signer payload?

signer payload

(cryptographic description of digital media asset)

Identity assertion (CBOR)

Identity assertion

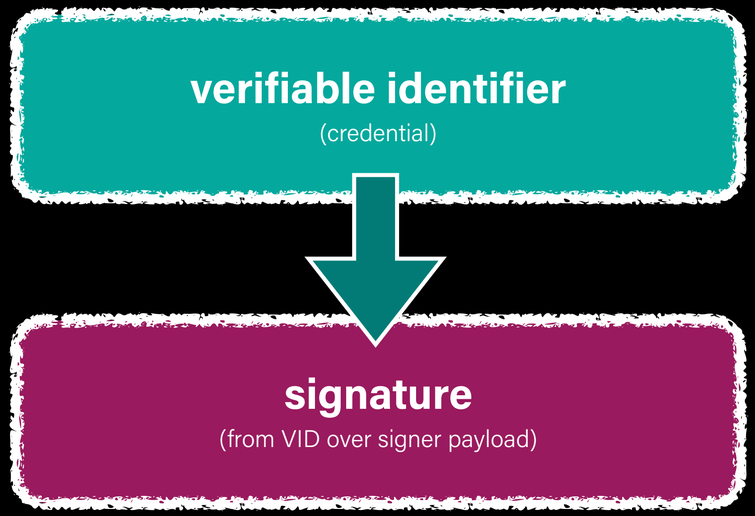
What is a verifiable identifier?

verifiable identifier
(credential)

Any credential for which an **independent system** is able to associate, discover, and verify the **cryptographic keys** associated with that credential.

Identity assertion

Signing workflow



Identity assertion (CBOR)

```
{
  "signer_payload": {
    "sig_type": "cawg.x509.cose",
    "referenced_assertions": [
      {
        "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
        "hash": b64'U9Gyz05tmpftkoEYP6XYNsMnUbnS/KcktAg2vv7n1n8='
      },
      {
        "url": "self#jumbf=c2pa/urn:uuid:F9168C5E-CEB2-4faa-B6BF-329BF39FA1E4/c2p
        "hash": b64'G5hfJwYeWTlflxObmf
      },
      {
        "url": "self#jumb
        "hash": b64'Yzag4
      }
    ],
    "role": ["cawg.creator"]
  },
  "signature": b64'....',
  "pad1": b64'....', // zero-filled pad buffer
  "pad2": b64'....'  // zero-filled pad buffer
}
```

signature

Proves association of credential subject to content.

Identity assertion

What kinds of credentials can be used?

verifiable identifier
(credential)

In principle, **any credential** that meets the ToIP definition of **verifiable identifier** *could* be used ...

provided ... someone describes how to do so.

Identity assertion

What we've done do far (1 of 2 – for institutional content creators)

verifiable identifier
(credential)

→ **X.509 certificate** (S/MIME and IPTC)

signature
(from VID over signer payload)

→ **COSE signature**

Identity assertion

What we've done do far (2 of 2 – for individual content creators)

verifiable identifier
(credential)

Ummm ...

signature
(from VID over signer payload)

???

Identity assertion

What we've done do far (2 of 2 – for individual content creators)

verifiable identifier
(credential)

signature
(from VID over signer payload)

Problem: Individual content creators don't think of their identities in the way that we in the identity world do.

- Instagram
- Twitter
- Other social media
- Web site
- Identity document
  (mDL or physical drivers license, etc.)

Identity assertion

What we've done do far (2 of 2 – for individual content creators)

Solution: Describe how a platform vendor can *aggregate* these identity signals and attest to them on behalf of their customer.

verifiable identifier
(credential)

Collection of gathered federated IDs

signature
(from VID over signer payload)

W3C verifiable credential*
signed by identity claims aggregator

Identity assertion

Work in progress for 2026 (1 of 2)

verifiable identifier
(credential)

→ **W3C Verifiable Credential (e.g. First Person Project)**

signature
(from VID over signer payload)

→ **COSE signature**

Identity assertion

Work in progress for 2026 (2 of 2)

verifiable identifier
(credential)

→ **KERI ACDC (GLEIF vLEI)**

signature
(from VID over signer payload)

→ **ACDC proof** *–or–*
self-addressing data wrapper

New work in CAWG

Sessions tomorrow and Thursday

- Governed metadata assertion
- Archival-quality identifiers
- Collaboration with First Person Project and similar projects (Keyring, etc.)
- Consent assertion (consent of subjects portrayed in content)

Come help us bind content provenance with identity!

CAWG is part of DIF

Meetings are every other Monday at 0800 US Pacific / 1500 UTC.

Next meeting: **6 May**