



# C2PA & CAWG

**Leading Efforts for Content Provenance, Authenticity and Attribution**

**ToIP Symposium November 19, 2025**

**Scott Perry, Digital Governance Institute**  
**Eric Scouten, Adobe**

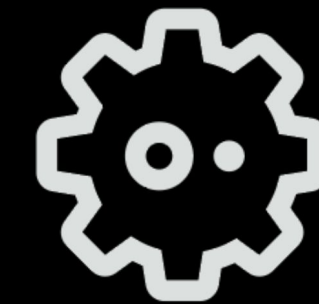
# The three Cs ... who does what here?



**What and how**  
C2PA

Coalition for Content  
Provenance and Authenticity

[c2pa.org](https://c2pa.org)



**Who**  
CAWG

Creator Assertions Working  
Group (*part of DIF*)

[cawg.io](https://cawg.io)



**Advocacy and education**  
[contentauthenticity.org](https://contentauthenticity.org)



# **The problem, in a nutshell**

On the Internet ...

**digital media content**

**can travel from a content creator**

**to unforeseen recipients**

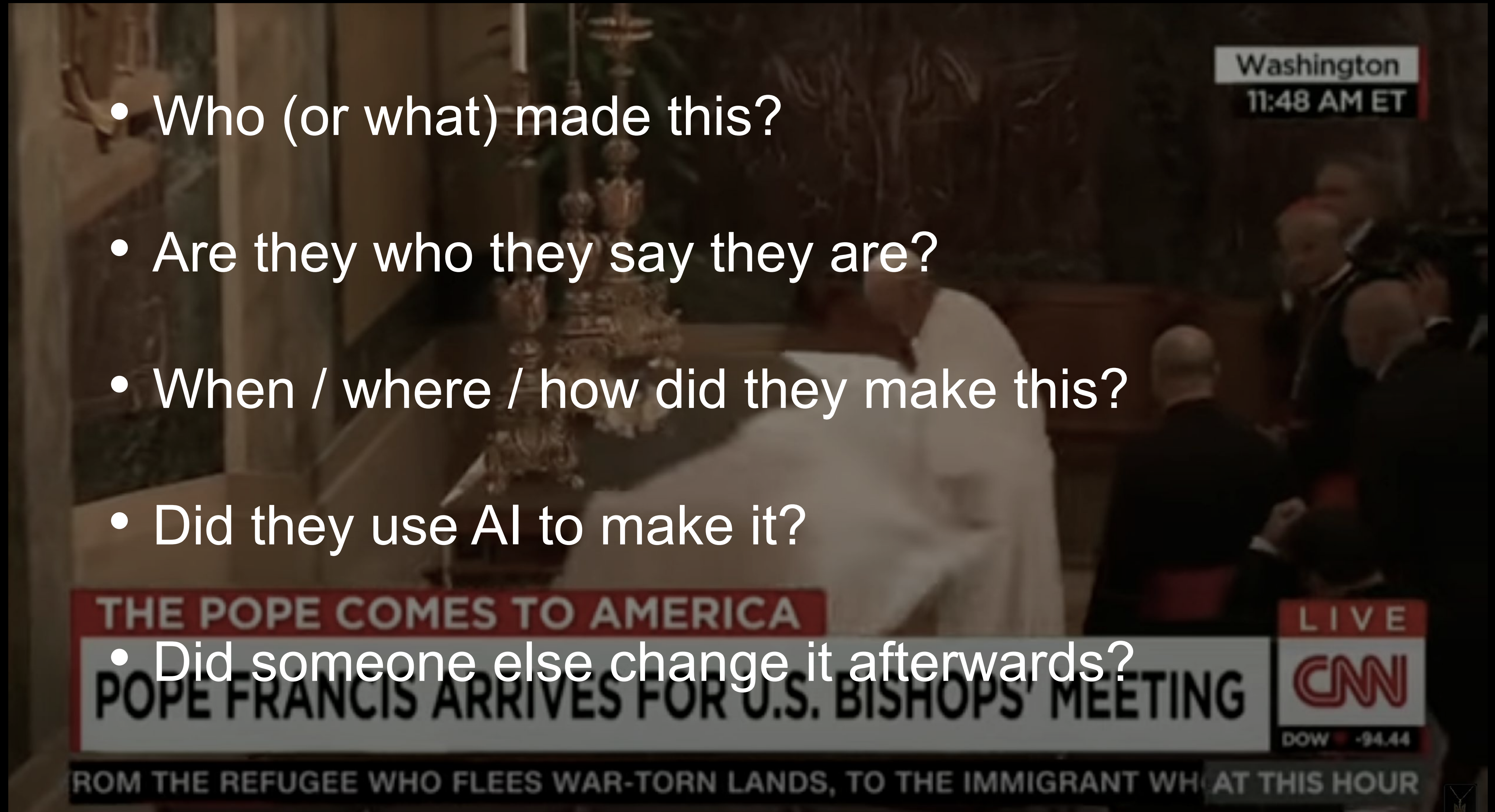
**via unknown channels.**





## 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**

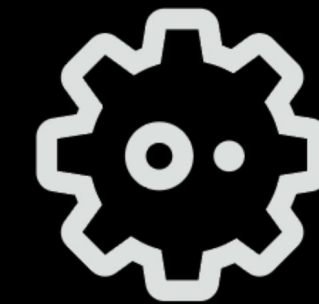
**... to describe and sign their work.**

# 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.**

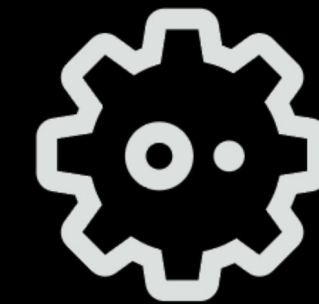


# What are they taking responsibility for?



**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 ...

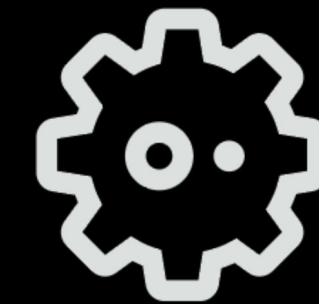
- Individuals or organizations involved in *creating* content
- Individuals or organizations *depicted* in content
- Metadata / context for content

# 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



## 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



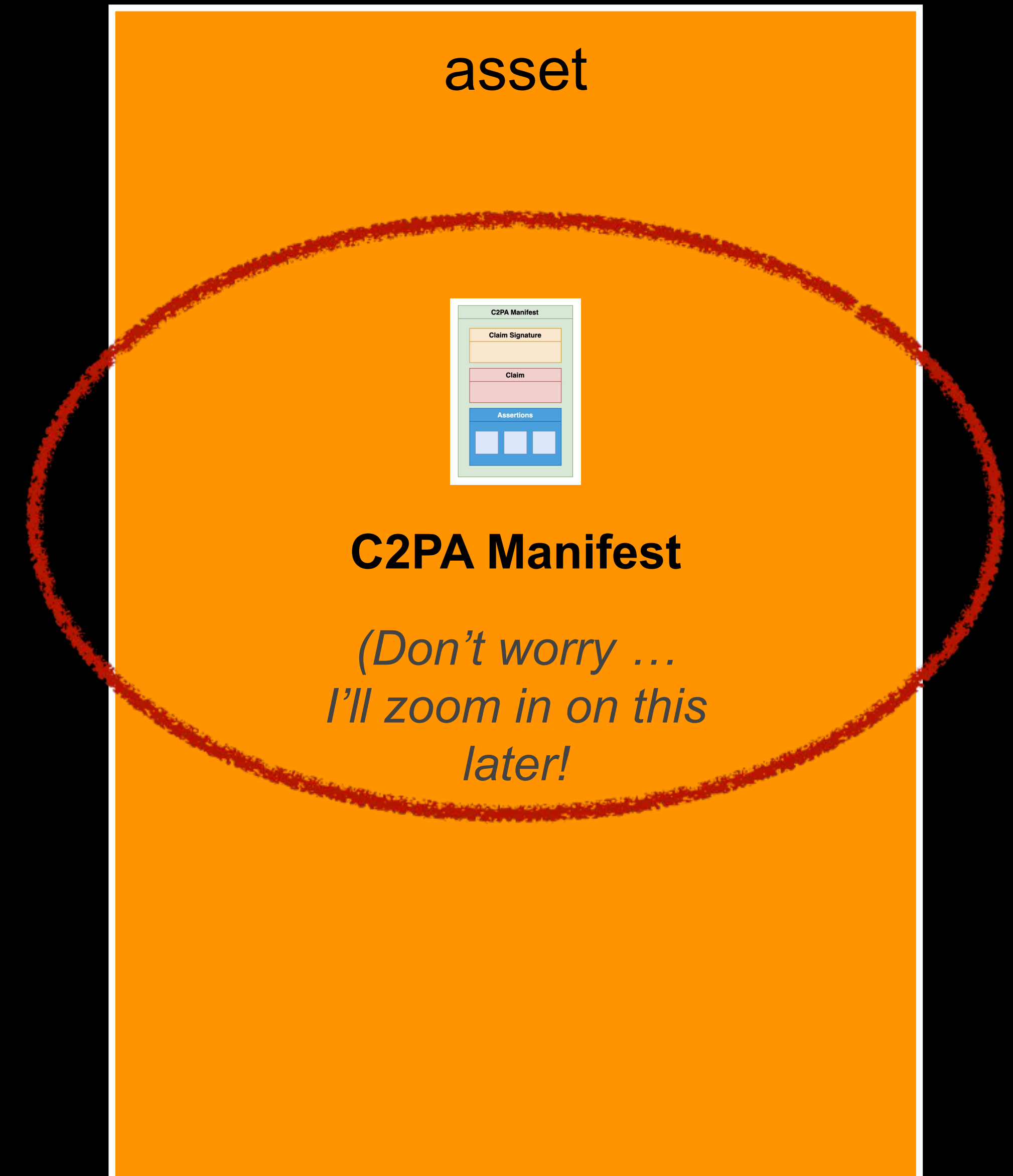
# C2PA data model

## 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**.

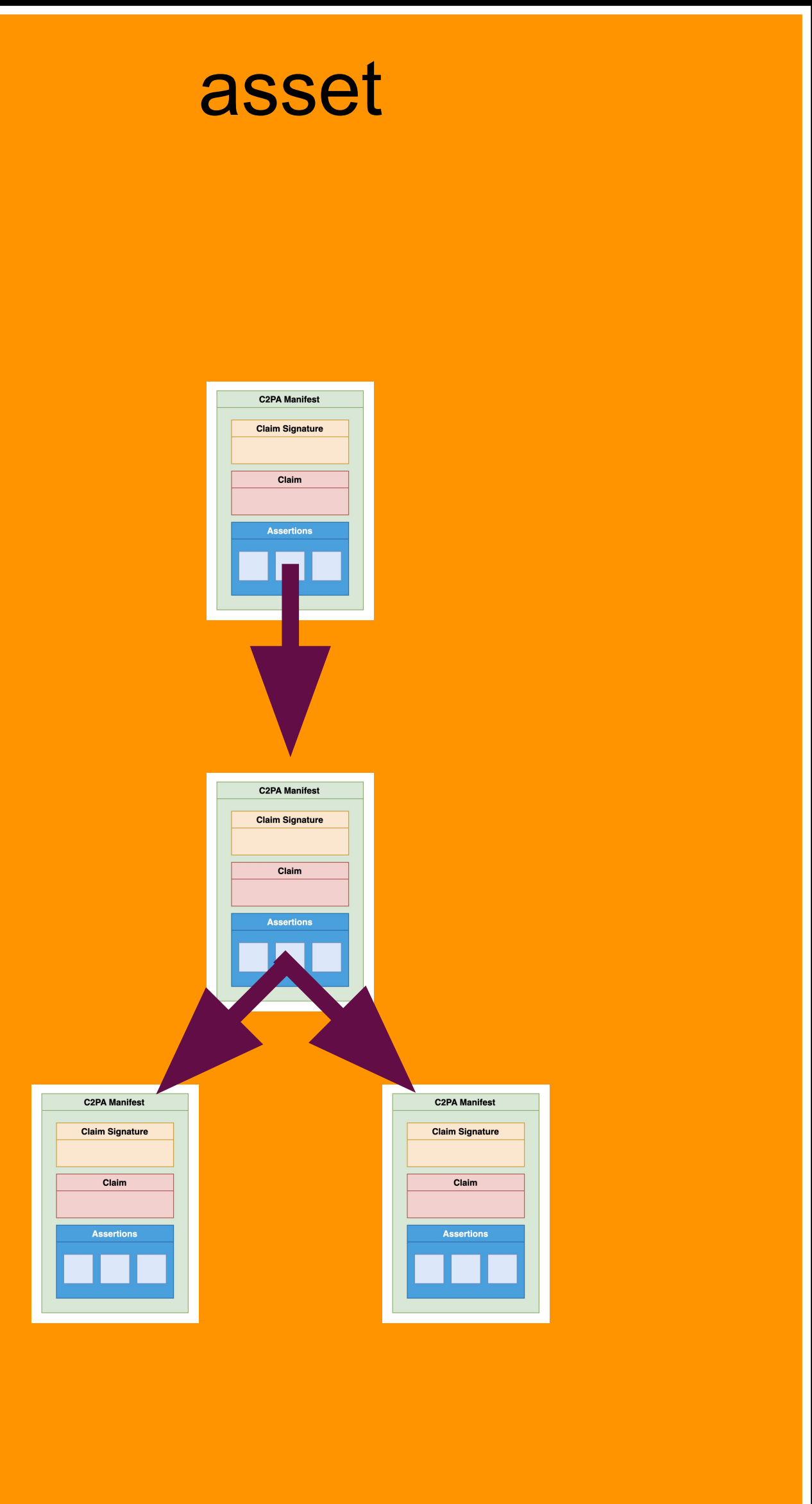




# C2PA data model

## Overview

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





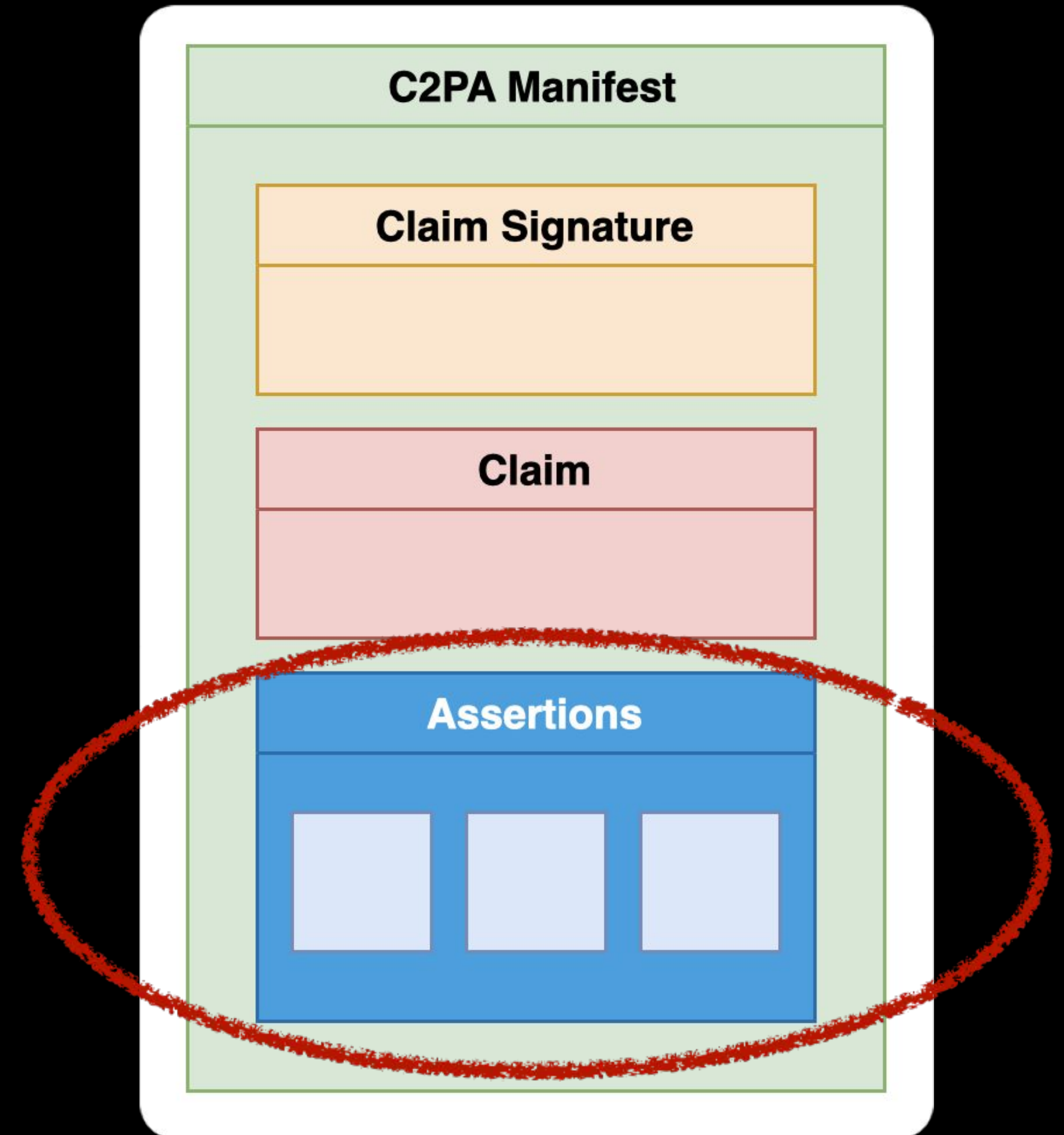
# C2PA data model

## 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**.





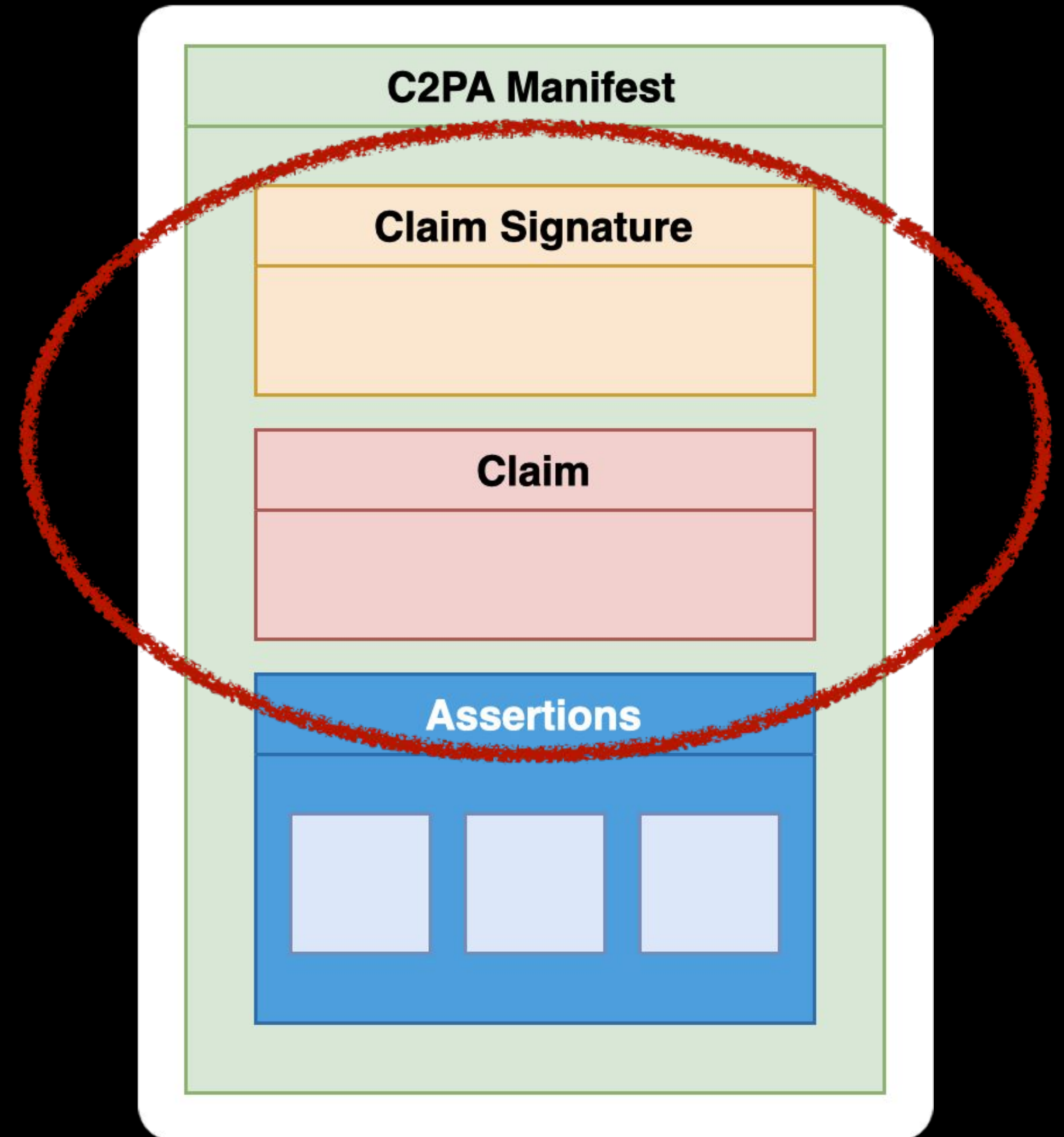


# C2PA data model

## Claim

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

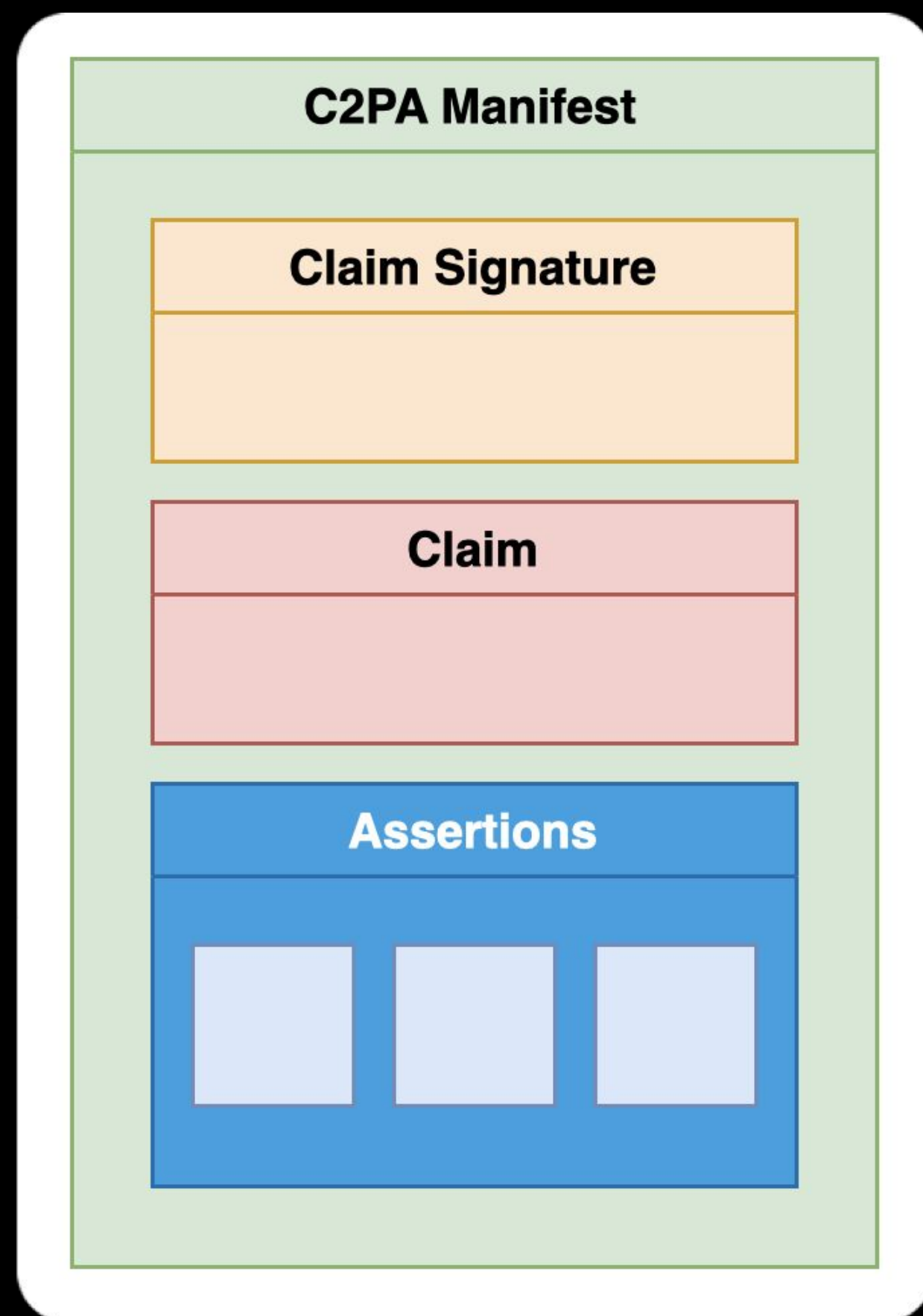
This claim is signed using an X.509 certificate, which provides evidence of the tool used and provides tamper evidence if a third party attempts to change the claim after the fact.






# C2PA data model

How we display it



[contentauthenticity.adobe.com/inspect](https://contentauthenticity.adobe.com/inspect)

20241127-162852-R-es-4703-039.jpg  
Recorded by Adobe Inc.



**Contributor details** ▾  
Information shared by people involved in making this content.  
Behance [ericscouten1](#)  
LinkedIn [Eric Scouten](#)  
I request that generative AI models not train on or use my content

**Content details** ▾  
Information about this content and how it was made.

**App or device used**  
Adobe Content Authenticity

**Recorded by**  
Adobe Inc. on Jun 3, 2025 ⓘ

**Actions**  
Opened  
Opened a pre-existing file  
Watermarked  
Applied an invisible watermark to improve this Content Credential's durability

**Ingredients**  
20241127-162852-R-es-4703-039.j...  
No Content Credentials

**claim generator**  
(C2PA)

**thumbnail assertion**  
(C2PA)

**identity assertion**  
(CAWG)

**training + data mining assertion**  
(CAWG)

**claim generator**  
(C2PA)

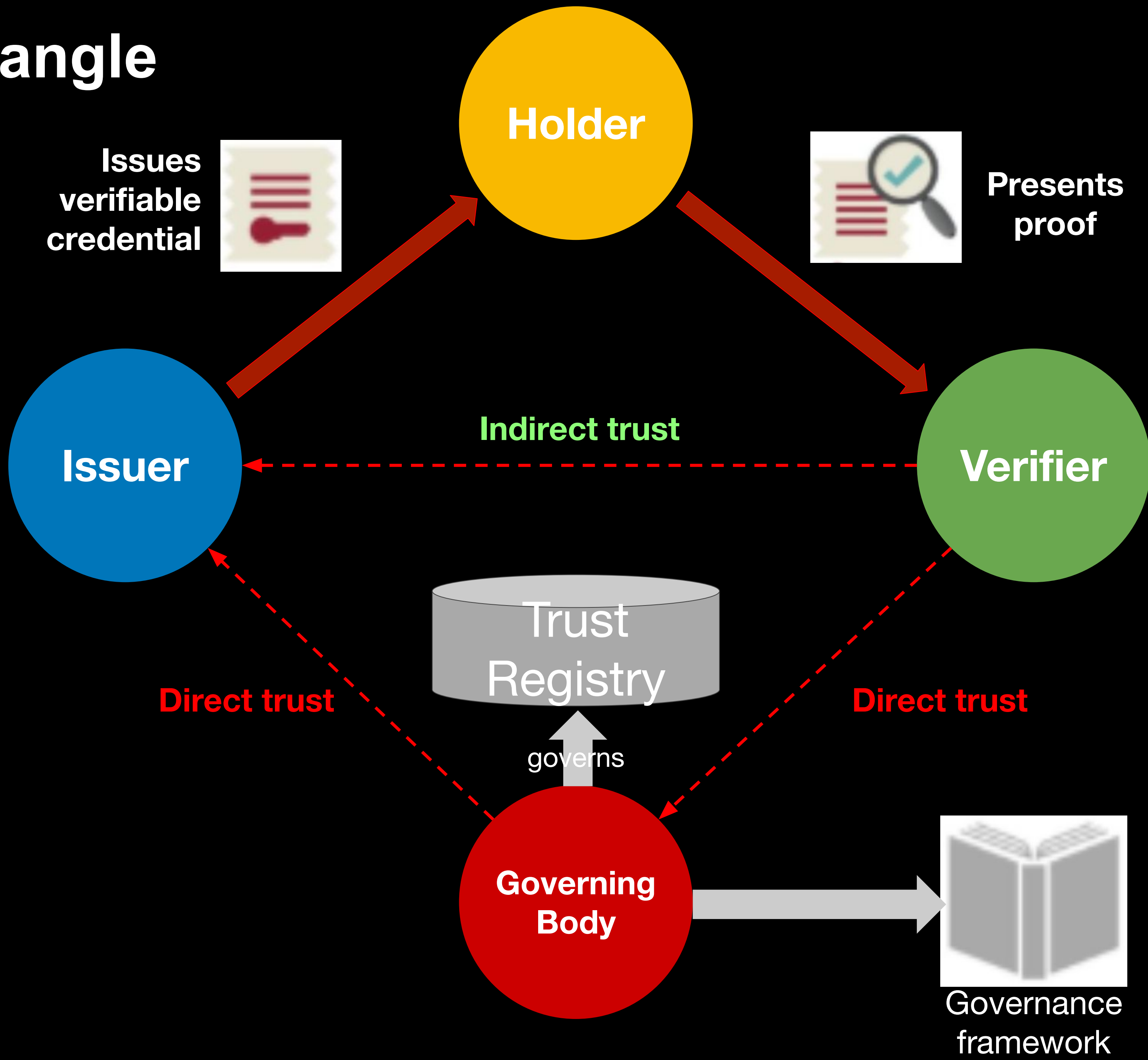
**actions assertion**  
(C2PA)

**ingredients assertion**  
(C2PA)



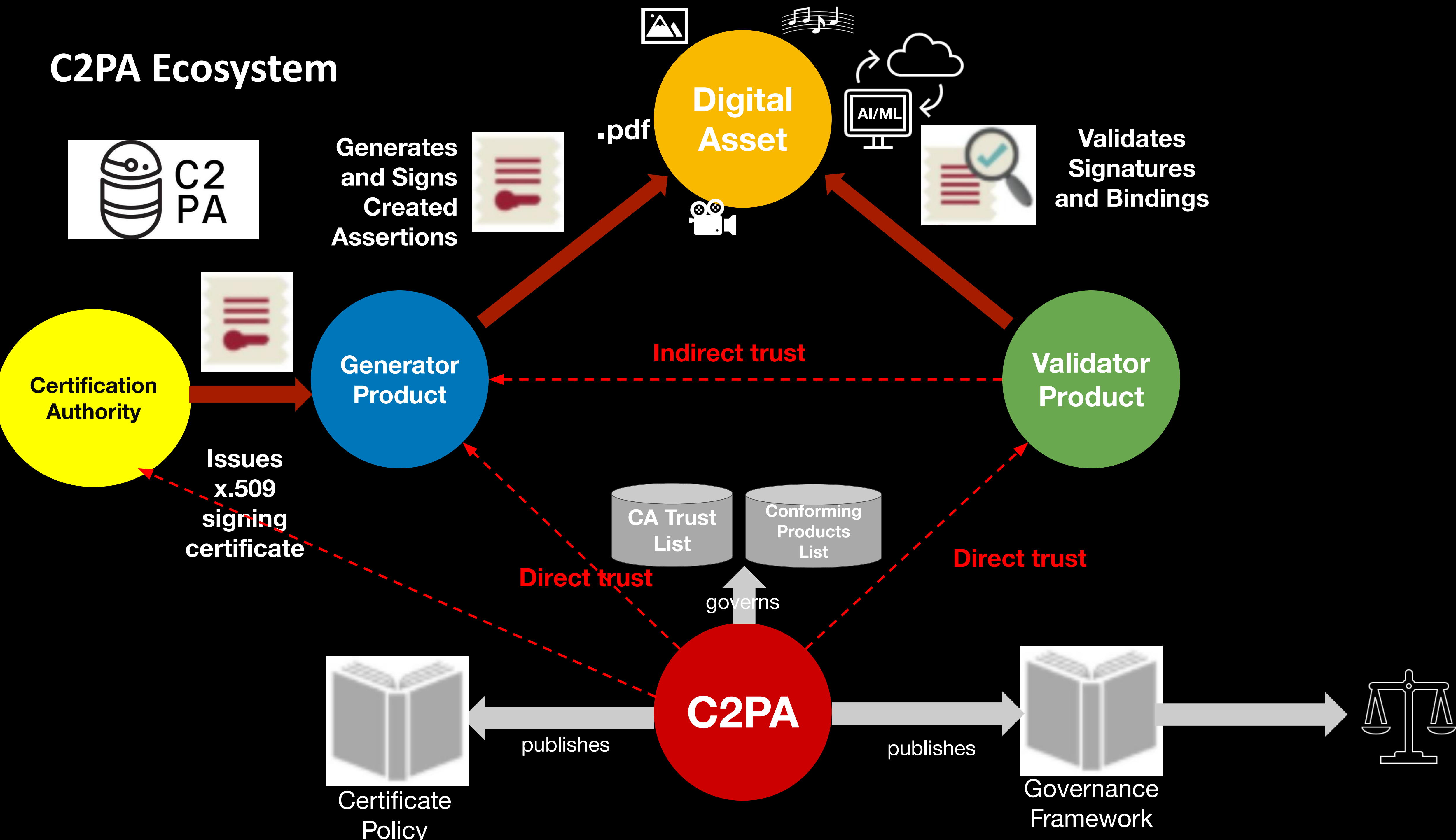
# C2PA Conformance Program

# Trust Triangle





# C2PA Ecosystem



# C2PA Conformance Program

- ❖ Holds Claim Generator and Validator Companies Accountable for C2PA Specification
- ❖ Holds Certification Authorities Accountable for C2PA Certificate Policy
- ❖ Establishes Four Levels of Implementation Assurance
- ❖ Manages Certification Authority and Conforming Products Trust Lists (Registries)
- ❖ Enacts Legal Agreements between Applicants and the C2PA

## PLANNED PROGRAM RELEASES

### INTERIM (v.01) 2Q2025

- ❖ Legal Agreements
- ❖ Trust Lists
- ❖ Two Levels of Implementation Assurance
- ❖ Self-Assertion

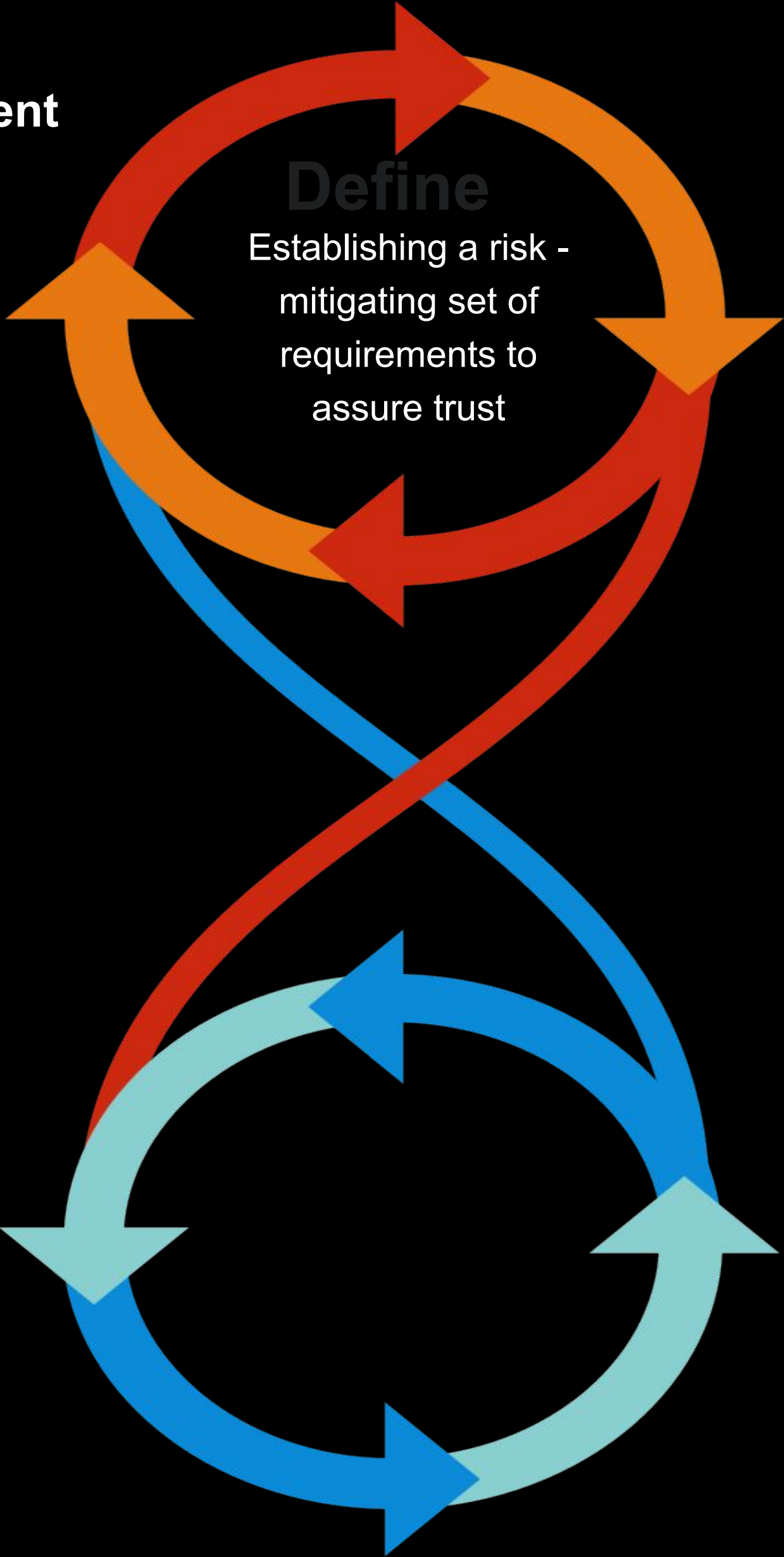
### INITIAL (v.1.0) 2Q2026?

- ❖ Legal Agreements
- ❖ Trust Lists
- ❖ Four Levels of Implementation Assurance
- ❖ Independent Attested Conformance

# Governance

Controllable risks  
are evaluated  
for likelihood and  
impact

## Risk Assessment



# Risk Assessment

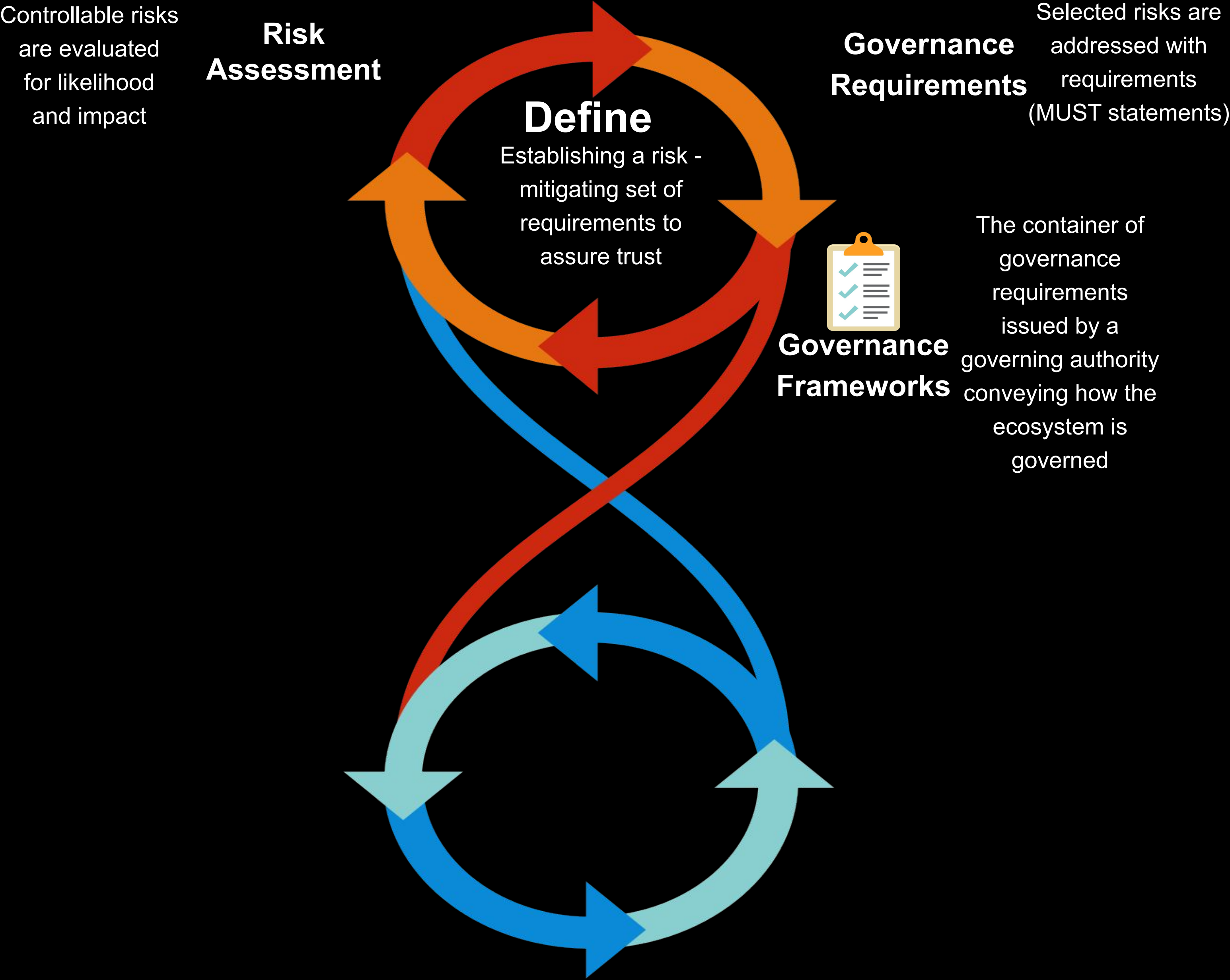
LEGEND			
COLUMN HEADER	EXPLANATION	Potential Values	
Risk #	A unique identifier of a risk for reference purposes	#	
Risk Description	Description of a unique risk	Text	
ToIP Layer	The Governance Stack Layer the risk operates based on the ToIP Governance Stack	Ecosystem	
		Credential	
		Provider	
		Utility	
Trust Area Affected	Information trust component affected by the risk	Governance	
		Availability	
		Security	
		Availability	
		Privacy	
		Processing Integrity	
Severity	Judgemental evaluation of impact the risk would have on the entity if realized	Negligible	1
		Minor	2
		Moderate	3
		Major	4
		Critical	5
Likelihood	Judgemental evaluation of the potential that the risk will occur risk without controls or other circumstances to prevent it.	Highly Unlikely	1
		Unlikely	2
		Possible	3
		Likely	4
		Highly Likely	5
Impact	Judgemental scoring of risk's effect based on severity and and likelihood.	Low	1-3
		Low-Medium	4-7
		Medium	8-12
		Medium-High	13-18
		High	19-25
Risk Consideration Actions	Factors to consider regarding risk treatment	Text	
Risk Treatment	Recommended action category to take to handle the risk	Mitigation	
		Avoidance	
		Transference	
		Acceptance	
		Other	
Risk Treatment Action	High level action identified to treat risk	Text	
Residual Risk	Judgemental level or state of risk after applying risk treatment	Text or Impact Level	

## Identified threats for Implementors

- ❖ Spoofing signed C2PA metadata via stolen key.
- ❖ Spoofing signed C2PA metadata via misuse of claim generator.
- ❖ Exploitation of the hosting environment.
- ❖ Interception and/or modification of traffic between two trusted sources.
- ❖ Impersonating conforming CGI during automated certificate enrollment.
- ❖ Tampering with asset and/or assertions at generation.



# Governance



# Governance Requirements / Governance Frameworks

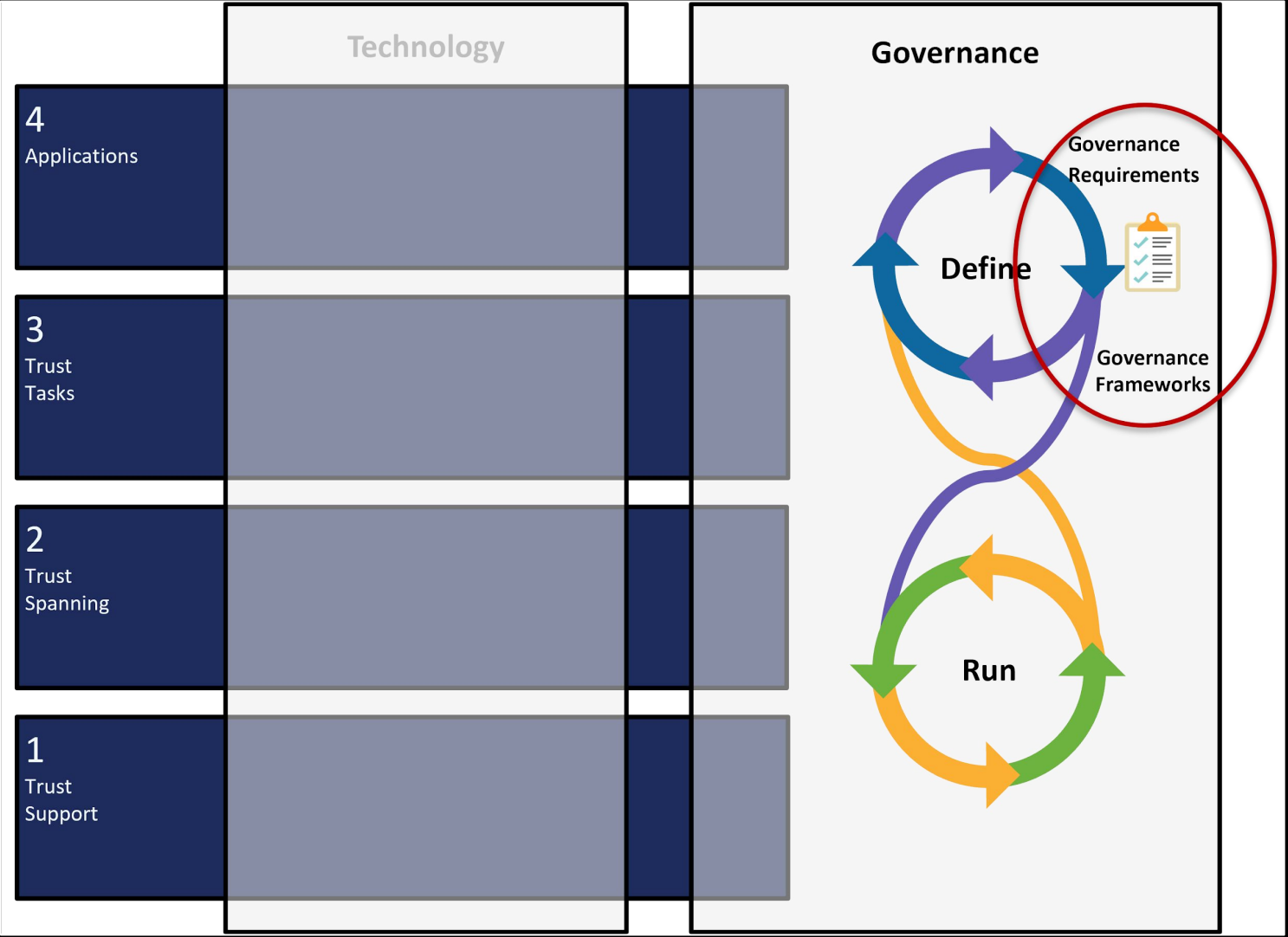
## Primary Document

- Introduction
- Terminology
- Governing Authority
- Administering Authority
- Purpose
- Scope
- Objectives
- Principles
- General Requirements
- Revisions
- Extensions
- Schedule of Controlled Documents

## Controlled Documents

Glossary	Risk Assessment	Trust Assurance & Certification
Governance Requirements	Business Requirements	Technical Requirements
Information Trust Requirements	Inclusion, Equitability, & Accessibility	Legal Agreements

Selected risks are addressed with requirements (MUST statements)



# C2PA Governance Framework

## Primary Sections

- ❖ Introduction
- ❖ Terminology
- ❖ Governing Authority
- ❖ Administering Authority
- ❖ Purpose
- ❖ Scope
- ❖ Program Participants
- ❖ Key Processes
- ❖ Objectives
- ❖ Principles
- ❖ Revisions
- ❖ Extensions

Risk  
Assessment

C2PA  
Conformance  
Program

Business  
Requirements

Information  
Trust  
Requirements

C2PA  
Specification  
Requirements

Governance  
Requirements

Privacy  
Inclusion  
Equitability  
Accessibility  
Requirements

Legal  
Agreements

C2PA  
Certificate  
Policy



# Governance





# Trust Assurance (Conformance)



Certification scheme is developed from requirements with independent evaluations from qualified auditors

## Trust Assurance and Certification Template:

<https://trustoverip.org/permalink/ToIP-Trust-Assurance-and-Certification-Controlled-Document-Template-V1.0-2021-10-19.pdf>

## Companion Guide:

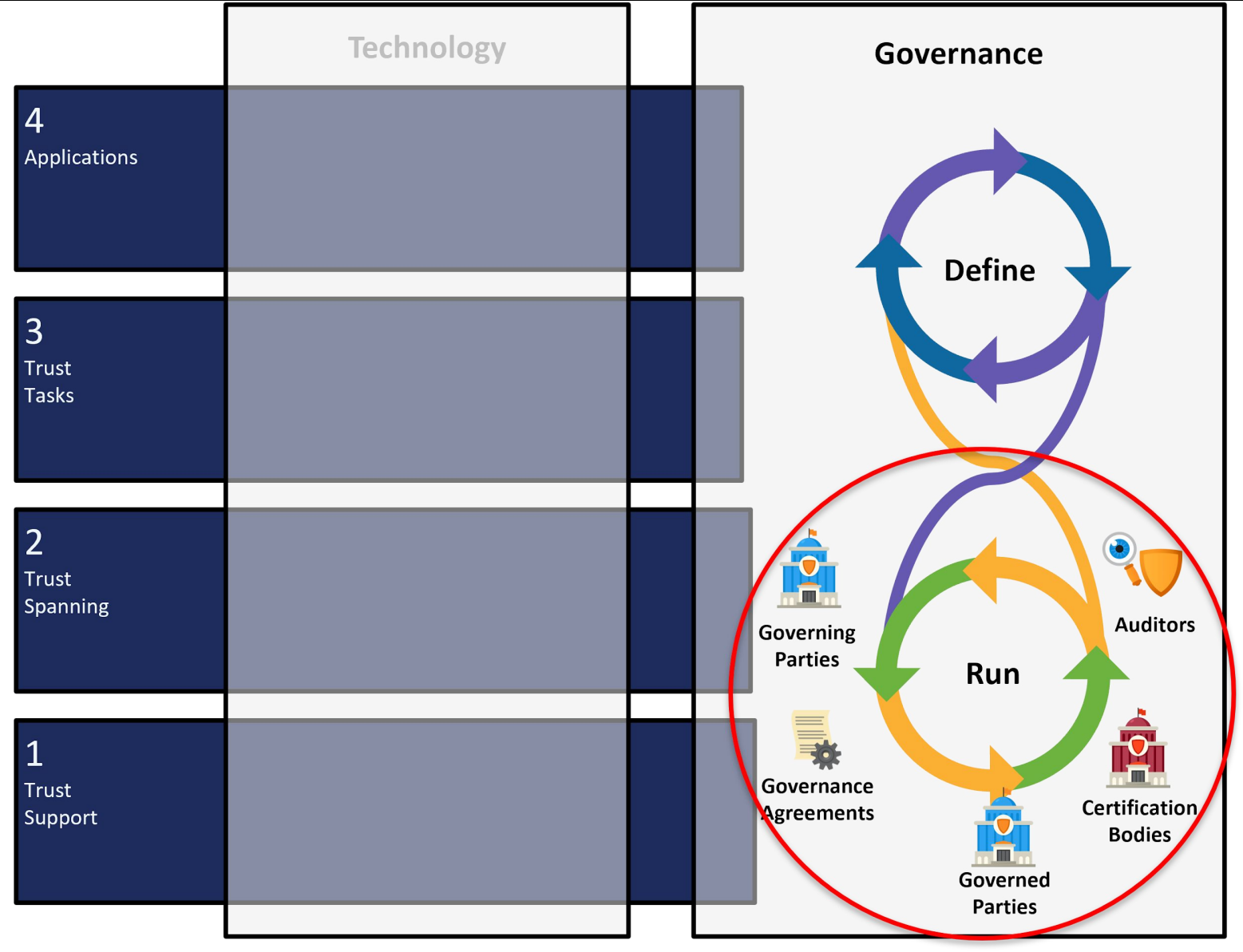
<https://trustoverip.org/permalink/ToIP-Trust-Assurance-Companion-Guide-V1.0-2021-10-19.pdf>

## Trust Assurance Criteria Template:

<https://trustoverip.org/permalink/ToIP-Trust-Assurance-Criteria-Matrix-Template-ToIP-Approved-V1.0-2021-10-10.>

## Companion Guide:

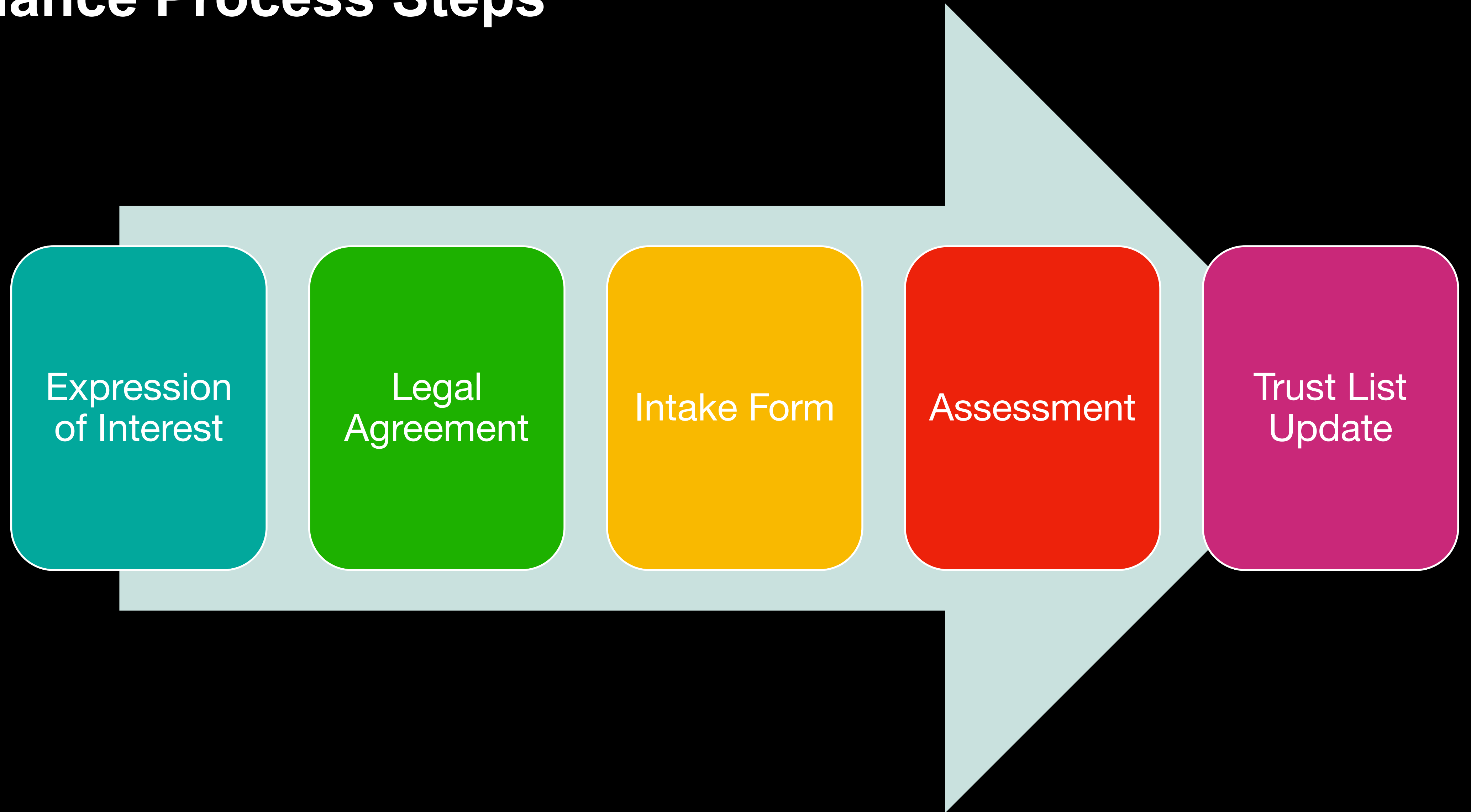
<https://trustoverip.org/permalink/ToIP-Trust-Criteria-Matrix-Companion-Guide-V1.0-2021-10-19.pdf>



# C2PA Trust Lists

TRUST LIST ATTRIBUTE	CA Trust List	Conforming Products List
Company Represented	Certification Authority	Claim Generator Claim Validator
Record	Issuing CA	Claim Generator Product Claim Validator Product Library Component
Key Record Attributes	Serial # Thumbprint Not Before/After	File Types (e.g audio, video) Max Assurance Level (1-4) SBOM
Revocation Available	Yes	Yes

# Conformance Process Steps



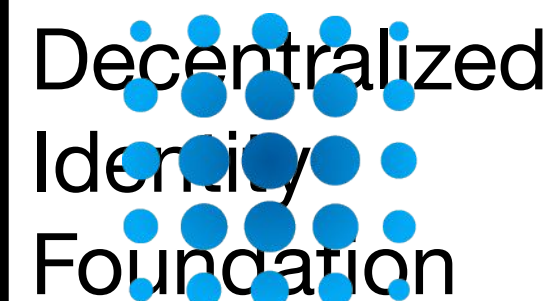


# Introducing CAWG

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.

The logo for the Decentralized Identity Foundation, featuring a cluster of blue dots of varying sizes arranged in a roughly circular pattern to the left of the text.

Decentralized  
Identity  
Foundation



## 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

The actor\* described by ...  *$\{credential\}$*

using a credential issued by ...  *$\{issuer\}$*

produced the content described by ...  *$\{signer\_payload\}$*

---

Signed by ...  *$\{credential\_holder\}$*

\*actor can be human, non-human, or organization of humans



# Identity assertion

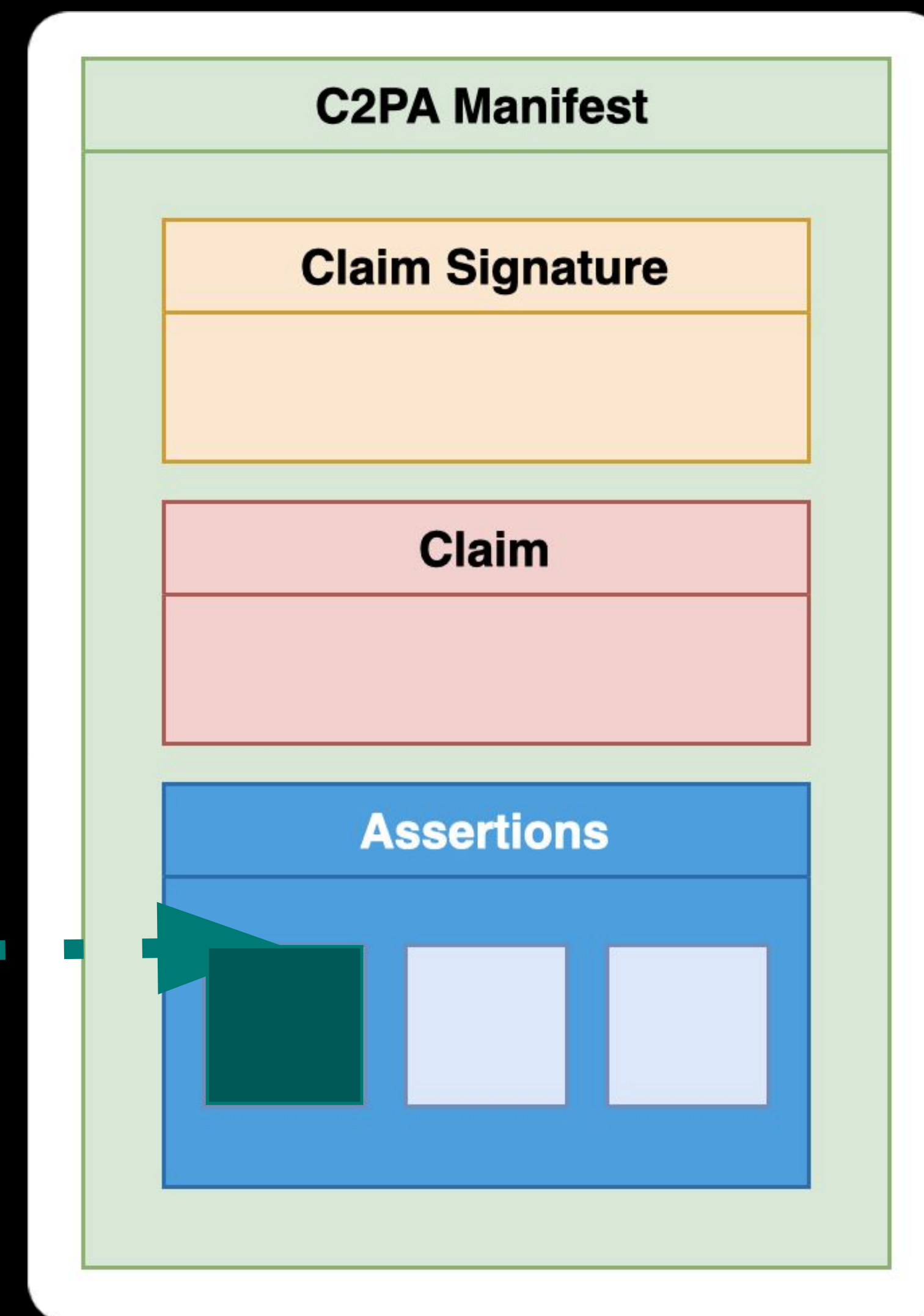
in the C2PA data model

A **CAWG identity assertion** is typically meant to indicate subject's **authorization of** or **active participation in** production of the asset.

It provides a **tamper-evident binding** between a digital credential and the asset described by the

C2PA Manifest *and* potentially other assertions in the same C2PA Manifest.

The action described by ...	<i><code>\${credential}</code></i>
using a credential issued by ...	<i><code>\${issuer}</code></i>
produced the content described by ...	<i><code>\${signer_payload}</code></i>
Signed by ...	<i><code>\${credential holder}</code></i>



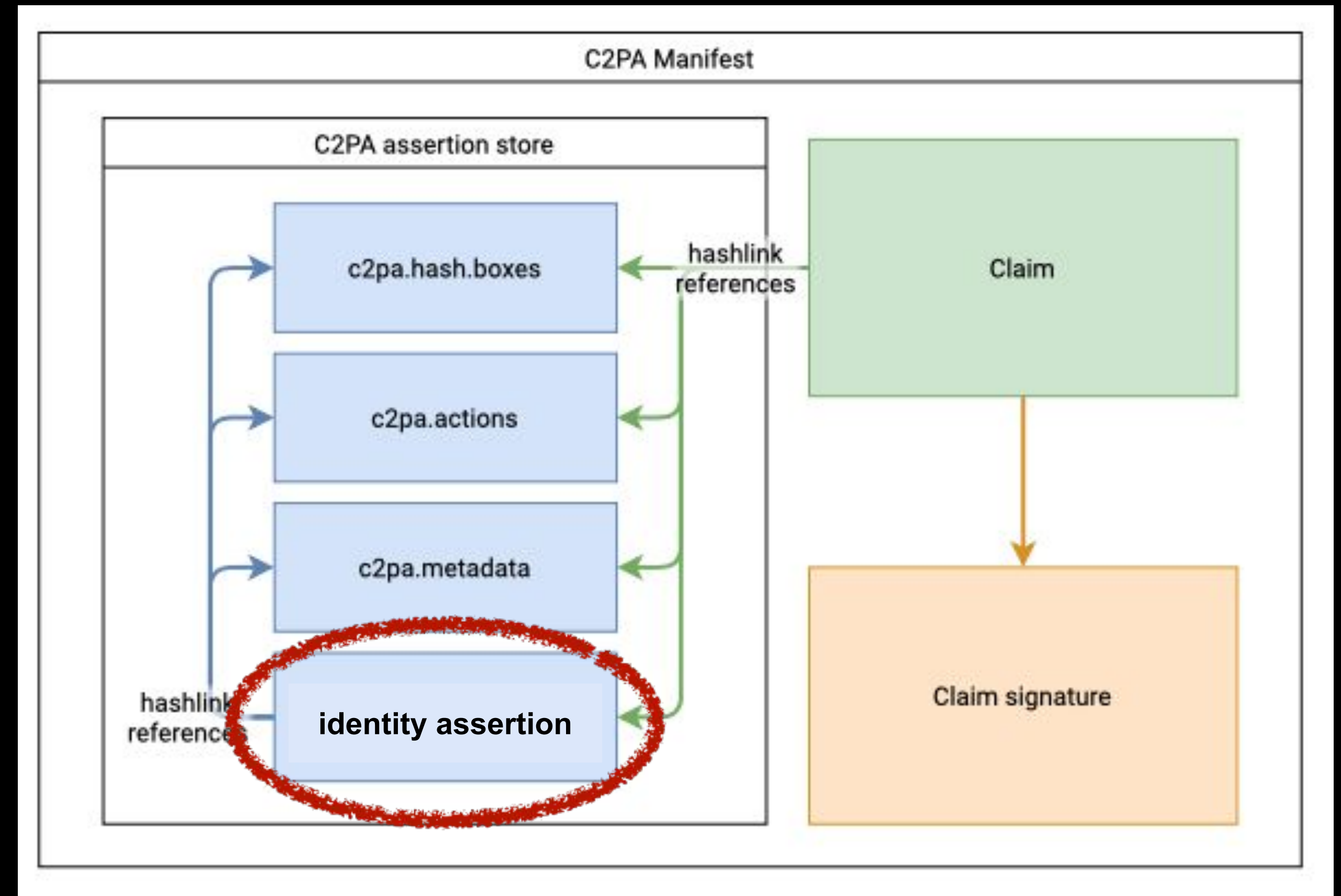


# Identity assertion

## Overview

Identity assertion allows a credential holder to sign a **signer payload** data structure which contains tamper-evident references to one or more other assertions in the same C2PA Manifest (including hard-binding assertion).

New trust signal separate from C2PA claim generator.





# Identity assertion

Two flavors (so far)

- **X.509 certificate**

*Typically used for institutional content creators such as news media. (More discussion in breakout part 2.)*

- **Identity claims aggregation**

*Targeted for individual content creators; contains links to social media, web site, etc.*

- **Extensible**

*More flavors coming in 2026*





# Identity assertion

Individual content creators

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

**Problem:** These credentials can generally be *observed* or *gathered* temporarily, but they generally don't have autonomous signing capability.



# Identity assertion

Individual content creators

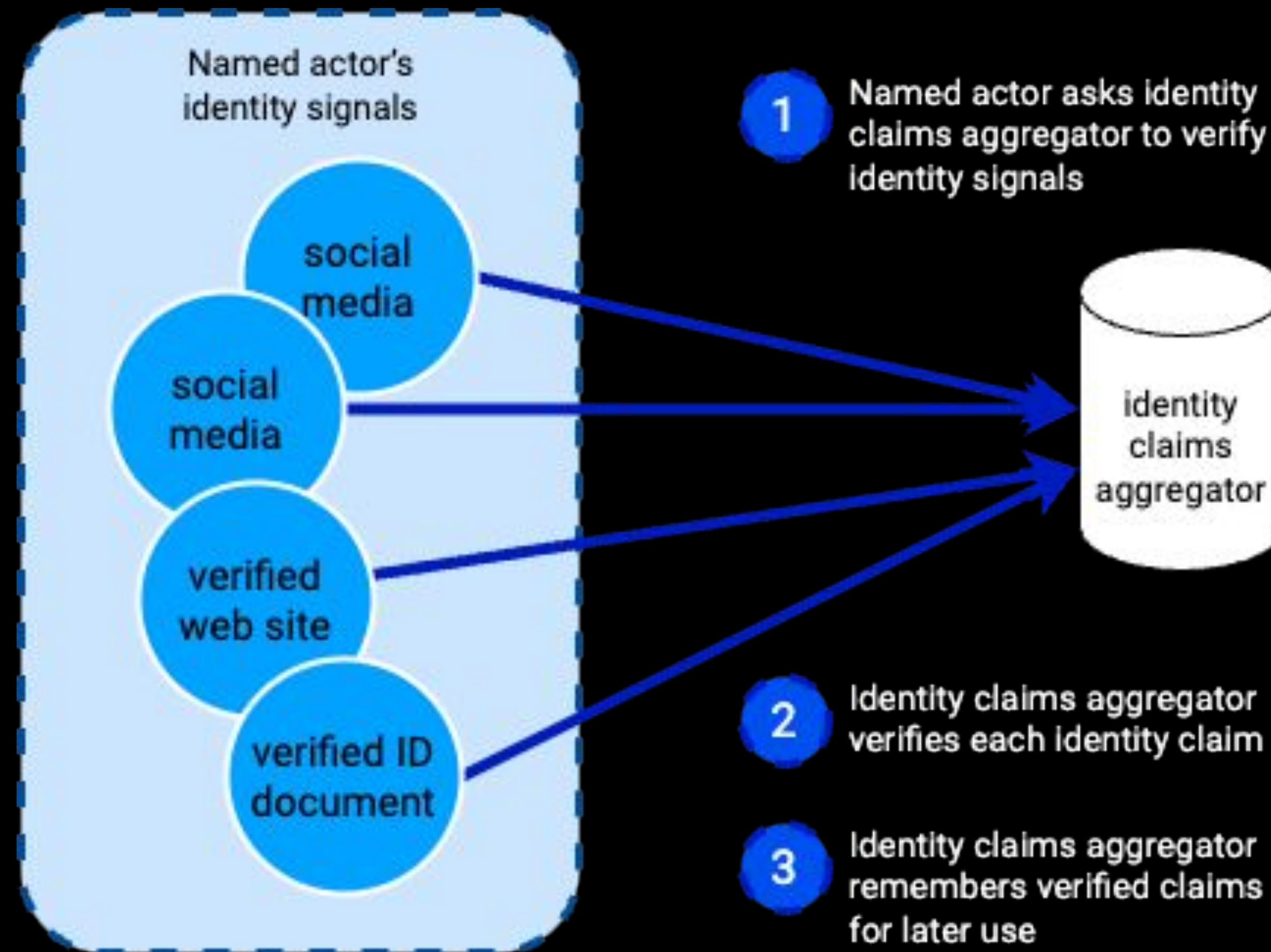
- Instagram
- Twitter
- Other social media
- Web site
- Identity document (mDL or physical drivers license, etc.)

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



# Identity assertion

Individual content creators: Verifying identity attestations

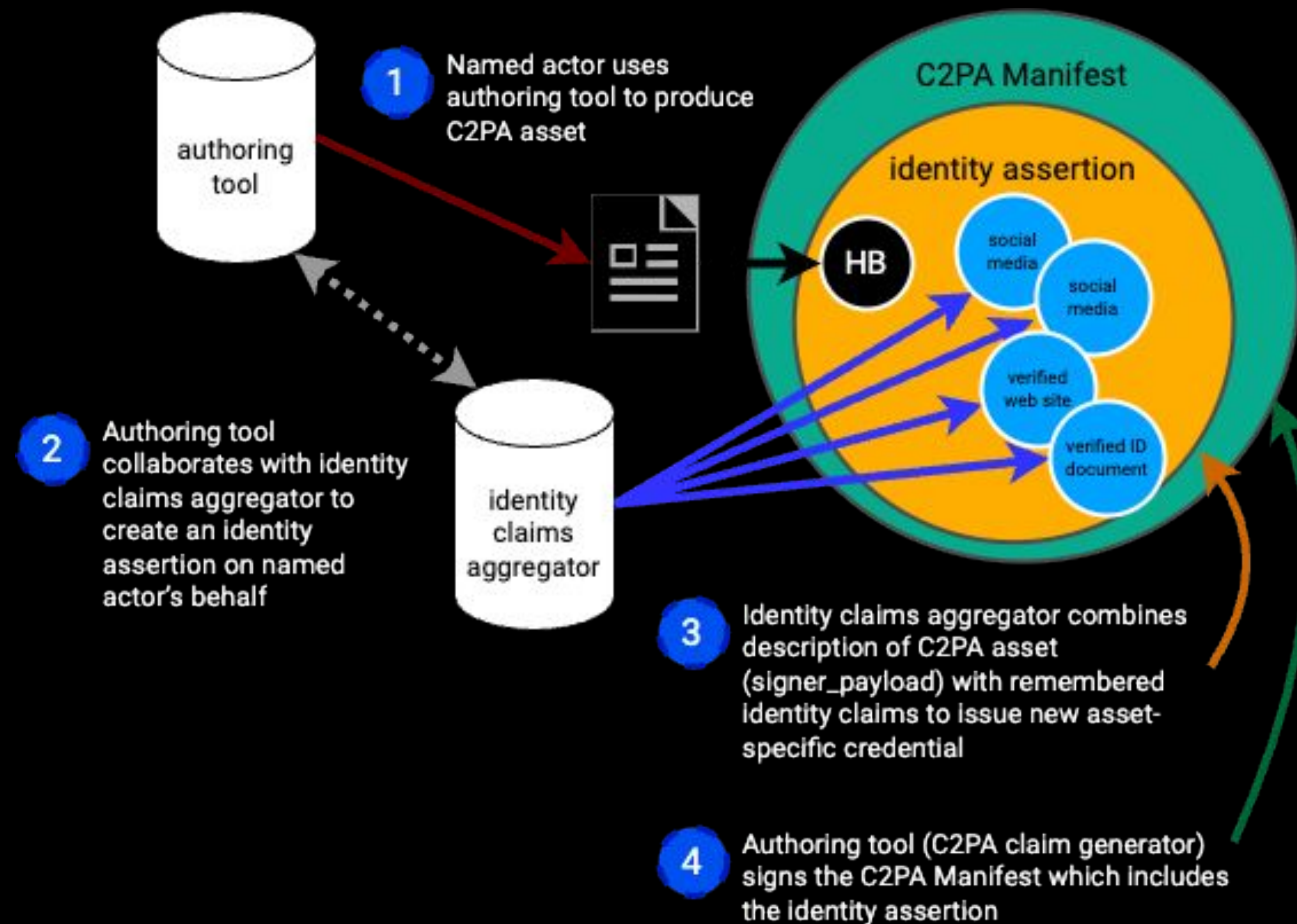






# Identity assertion

Individual content creators: Creating content





# Adobe Content Authenticity

## UX for CAWG identity claims aggregation

[contentauthenticity.adobe.com/preferences](https://contentauthenticity.adobe.com/preferences)

### Preferences

Manage information to include in Content Credentials from Adobe Content Authenticity (Beta).

#### Social media accounts

Behance

[ericscouten1](#)

...

Instagram

Connect

...

LinkedIn

[Eric Scouten](#)

...

X (Twitter)

Connect

...

Add social media accounts to your Content Credentials by logging in to prove that they're yours.

[contentauthenticity.adobe.com/inspect](https://contentauthenticity.adobe.com/inspect)

Contributor details

Name

[Jane Smith](#)

Verified by LinkedIn

Behance

[Julie Smith](#)

Instagram

[juliesmith](#)

I request that generative AI models not train on or use my content.

Content details

Data sourced from  
CAWG identity  
assertion





# Identity assertion

Individual content creators

The actor described by ... VC with aggregated ID signals

using a credential issued by ... identity claims aggregator

produced the content described by ... `${signer_payload}`

---

Signed by ... identity claims aggregator



## Caution

Identity claims aggregation is *one way* to provide information about a content creator.

It's useful as a bridge between the identity signals mentioned before and current credential technology, but it is *not* fundamental to the identity assertion.



# Identity assertion

Organizational identity via CAWG X.509

The actor described by ... X.509 certificate

using a credential issued by ... certificate authority

produced the content described by ...  $\{signer\_payload\}$

---

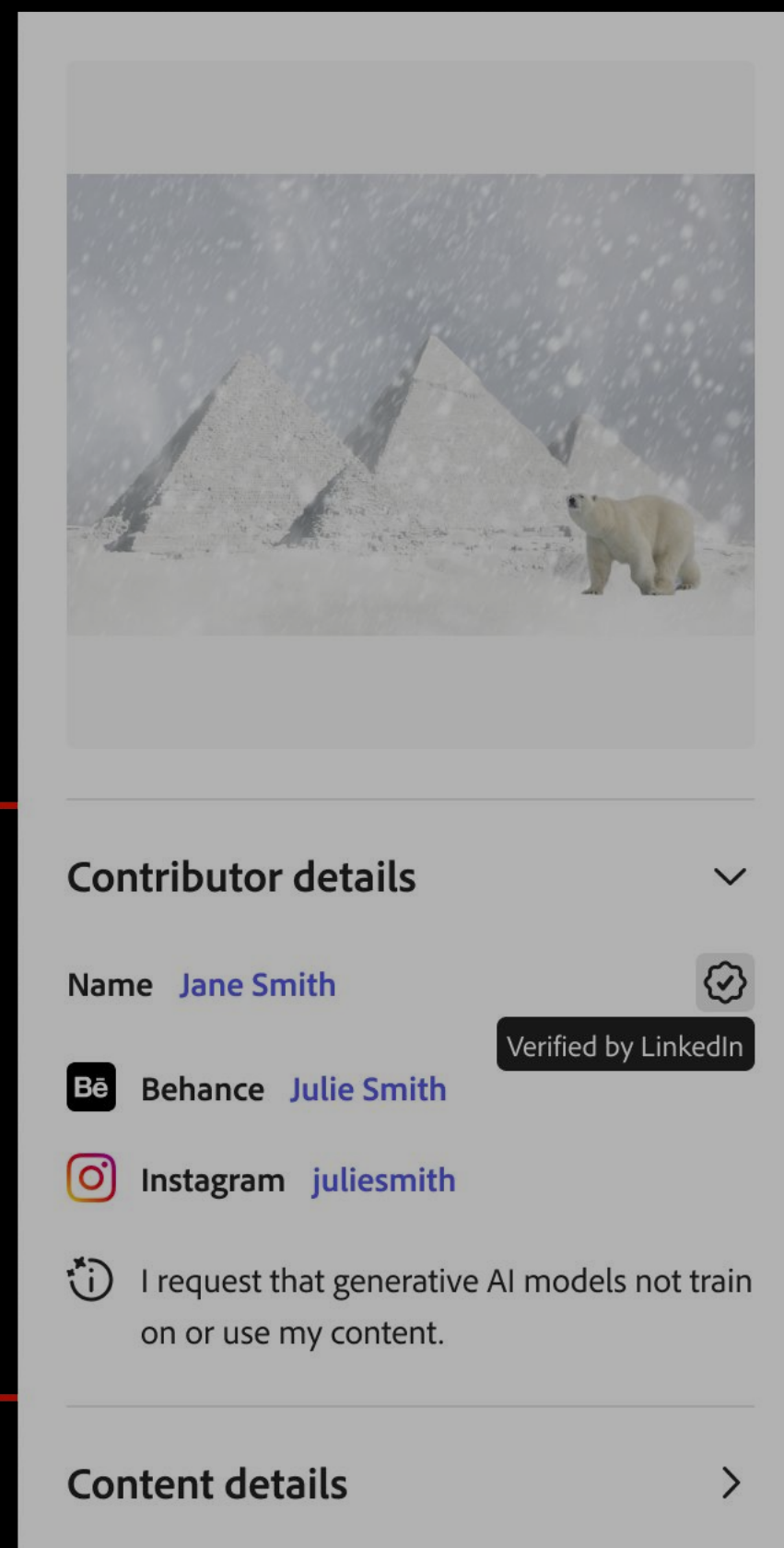
Signed by ... X.509 credential holder



# Adobe Content Authenticity

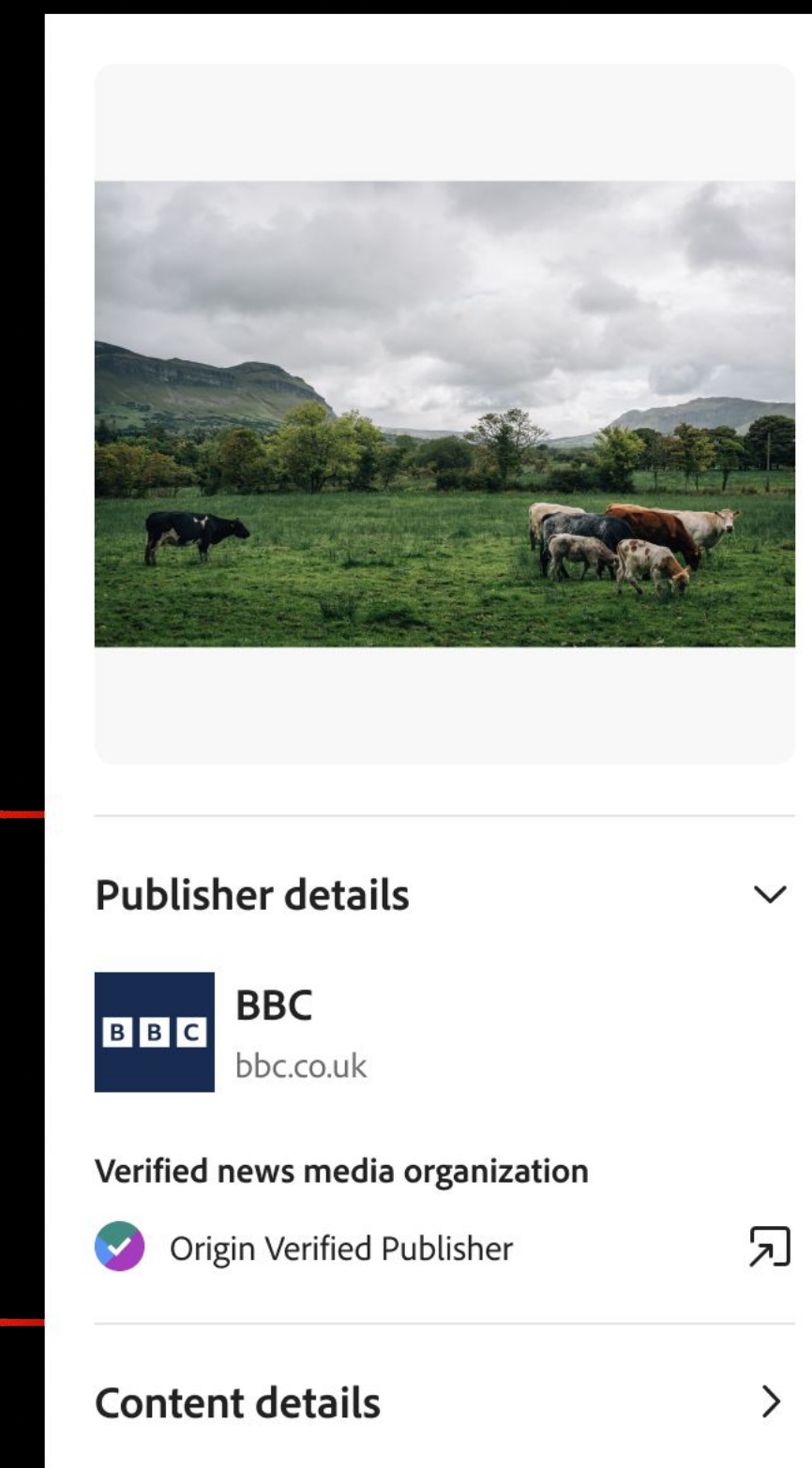
## Proposed UX for Origin verified publisher content

contentauthenticity.adobe.com/inspect  
(for individual-created content)



Data sourced from  
**CAWG identity**  
assertion

contentauthenticity.adobe.com/inspect  
(for news media content)




Data sourced from  
**CAWG identity**  
assertion






# Adobe Content Authenticity



Publisher provides additional metadata



**Publisher details** ▾


 **BBC**  
bbc.co.uk

Verified news media organization


 Origin Verified Publisher 

**Content details** >

Data sourced from  
**CAWG metadata**  
assertion



**Publisher details** ▾

 **BBC**  
bbc.co.uk



**Title**  
Cattle Grazing Beneath Stormy Skies in County Sligo

**Description**  
A group of cows graze in a green pasture surrounded by rolling hills and cloudy skies in a rural landscape, likely in a temperate region.

**Credit**  
Photo by Jane McConnell / Reuters

**Published on** September 15, 2012

**Verified news media organization**

 Origin Verified Publisher 

**Content details** >



# Current work

Identity and metadata 1.2



## Identity assertion 1.2 – likely very soon

Driven by interest from news media, entertainment, and organizational brands:

- Establish an **interim** trust model for CAWG X.509, largely based on S/MIME certificate infrastructure
- Add guidance for using logos and icons contained in X.509 certificates
- Fix a C2PA compatibility issue, allowing identity assertions to appear in update manifests



## Metadata assertion 1.2 – likely very soon

- New guidance for how to use metadata assertion to document involvement of many contributors with particular emphasis on motion picture and recorded music.
- Recommend use of identity assertion to attest to metadata authorship.





# Upcoming work

Identity 1.3



## **Identity assertion 1.3**

Proposed goals – still under discussion

- Identity evolution
- Self-control of identity signals
- Privacy preservation
- Broader integration with W3C VCs and VPs



## Identity assertion 1.3

Proposed goals – **identity evolution**

- Name changes
- New social media / web site / contact

Allow content creators to provide new information – or remove existing information – about their identity for existing C2PA assets, *even if no information was provided at time of asset creation.*



## Identity assertion 1.3

Proposed goals – **self-control**

- Allow content creators to control their own identity signals.
- Allow content creators to use the same identity signals across authoring tools.
- Allow content creators the ability to choose when/if to disclose aspects of their identity.





## Identity assertion 1.3

Proposed goals – **privacy preservation**

- Allow content creators to control whether identity signals among C2PA assets are correlatable.
- Avoid unintended identity signals through unintended correlation between identity assertions.
- Allow content creators the ability to choose when/if to disclose aspects of their identity. *(repeat)*



## **Identity assertion 1.3**

Proposed technical approaches – still under discussion

- Identity hooks
- First-person credentials



## Identity assertion 1.3

Proposed technical approaches – identity hooks  
Core idea: **Automatically create an “identity hook” (a public-private key pair or DID) for every C2PA asset created and privately remember the association between private key and asset.**

This allows the content creator to subsequently release information that is associated with that specific asset of the form: “I can prove that I created the specific asset in question and I would now like you to know \_\_\_\_.”

... without inadvertently proving that you created any *other* C2PA asset.

**More info:** [github.com/decentralized-identity/cawg-identity-assertion/issues/216](https://github.com/decentralized-identity/cawg-identity-assertion/issues/216)



## Identity assertion 1.3

Proposed technical approaches – **first-person credentials**

Core idea: **Establish a self-controlled credential that is based on verifiable relationships.**

Allow content creators to associate reputation-based credentials with the content they create.

Intending to collaborate closely with First Person Project.





**Come help us bind content provenance with identity!**

CAWG is part of  **DIF**

Meetings are every other Monday at 0800 Pacific /  
1100 Eastern / 1500 UTC.

Next meeting: 2 December