Dude (Person), Where’s Your DID?

Eric Scouten · Identity Standards Architect · Adobe

30 October 2024

Content Authenticity 101: Lightning Round

Content
Authenticity
Initiative

Coalition for
Content
Provenance
and Authenticity

Creator
Assertions
Working Group

ericscouten.dev/2024/
content-authenticity-101/

Who’s who?

Content Authenticity Initiative	Outreach · Advocacy · Open Source ** also name of Adobe’s team*
C2PA Coalition for Content Provenance and Authenticity	Technical Standards: **What / How**
Creator Assertions Working Group	Technical Standards: **Who**

C2
PA

Our goals

Allow **content creators** to make tamper-evident, digitally-signed statements about what they’ve created.

Allow **content consumers** to evaluate those statements and use them to make trust decisions.

Our non-goals

Content Authenticity is **not:**

- fact-checking
- fake image detection
- politically opinionated

C2PA data model

C2PA data model

Overview

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

asset

Currently supported asset types include:

photo

video

audio

documents

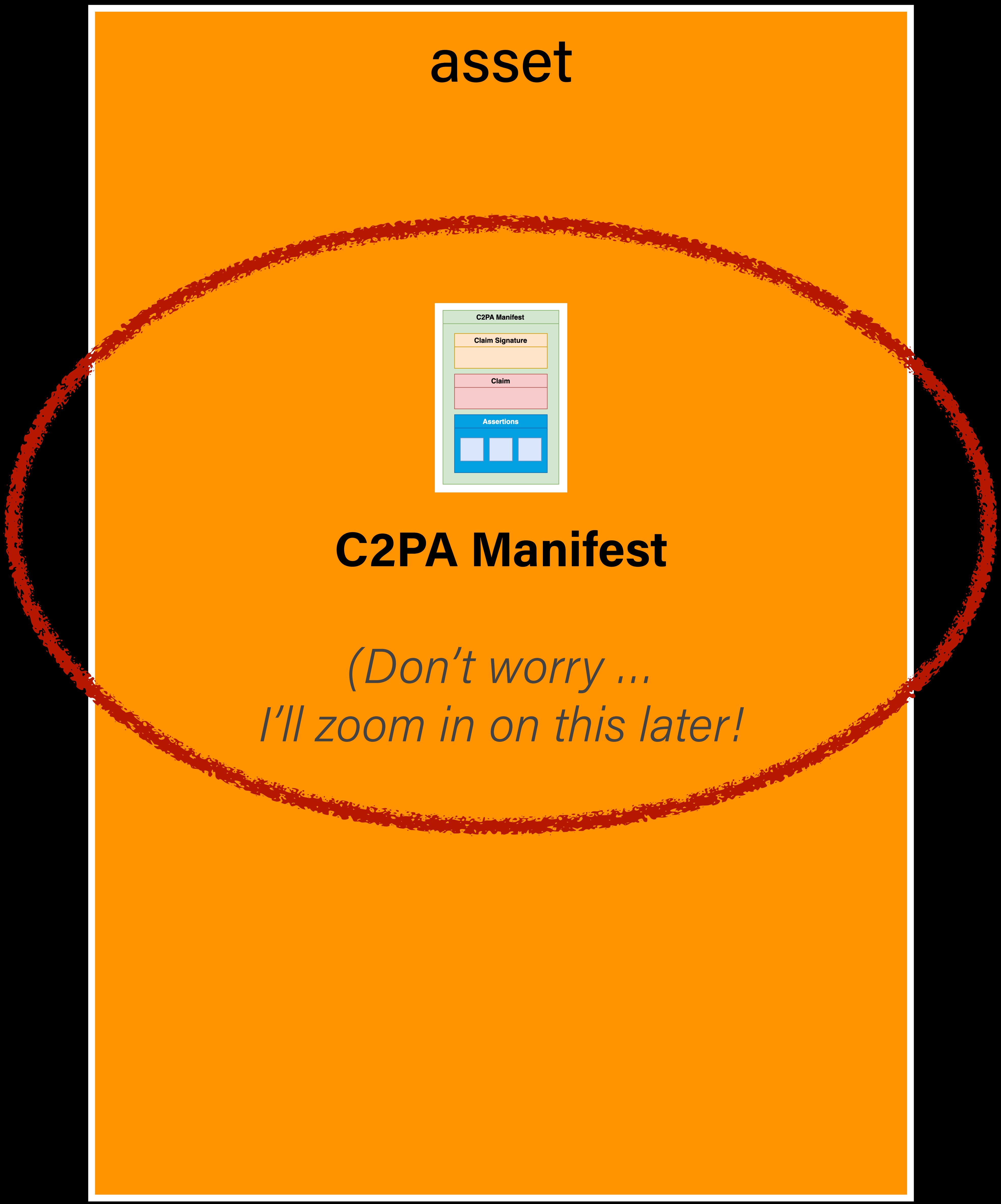
fonts

C2PA data model

Overview

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

It is described by a **C2PA Manifest**.



*(Don’t worry …
I’ll zoom in on this later!*

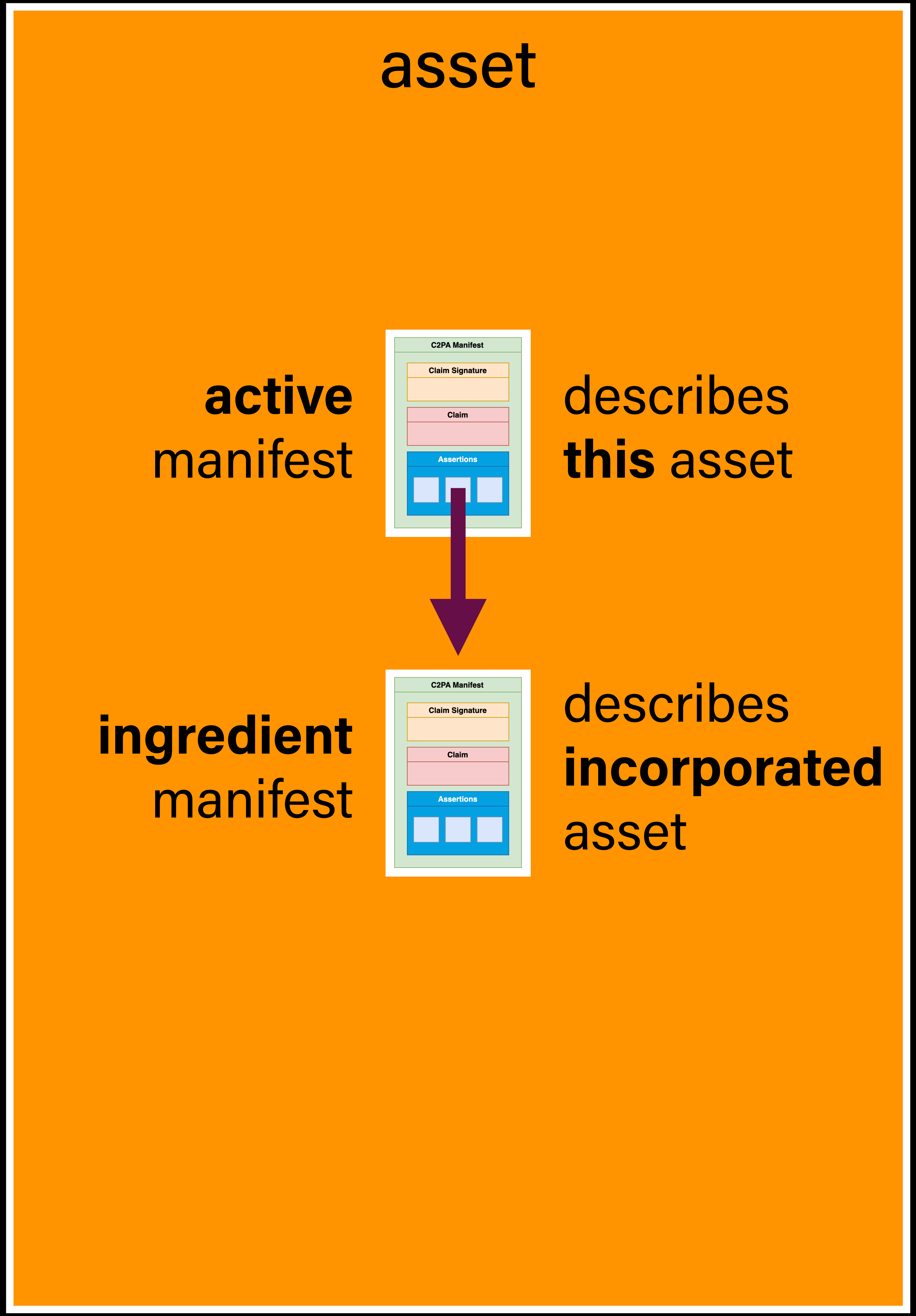
C2PA data model

Overview

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

It is described by a **C2PA Manifest**. Each asset in C2PA has an *active manifest* which describes the current asset.

That C2PA Manifest may refer to *ingredient manifests* when earlier content is incorporated.



asset

active manifest

describes **this** asset

ingredient manifest

describes **incorporated** asset

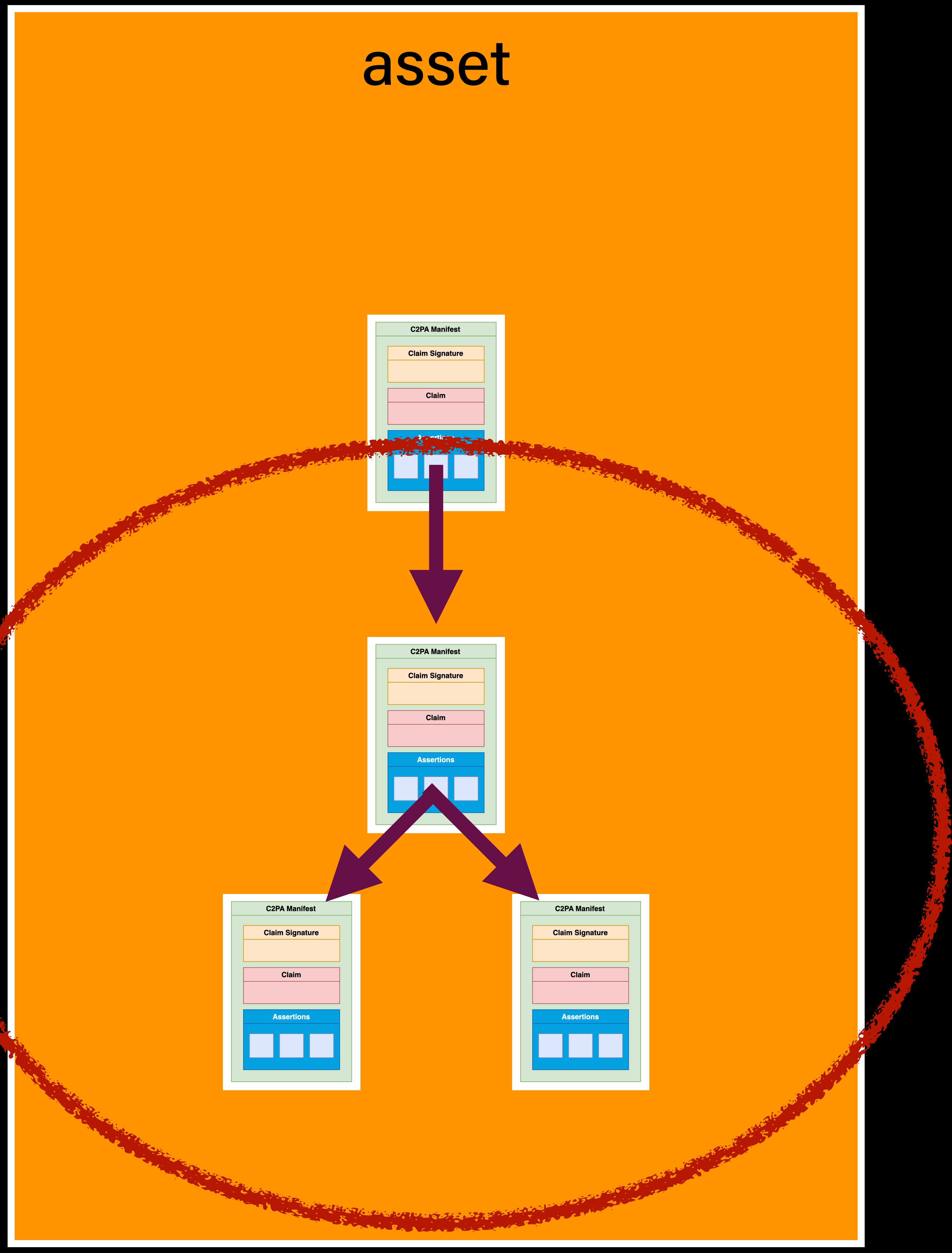
C2PA data model

Overview

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

It is described by a **C2PA Manifest**. Each asset in C2PA has an *active manifest* which describes the current asset.

That C2PA Manifest may refer to *ingredient manifests* when earlier content is incorporated.



C2PA data model

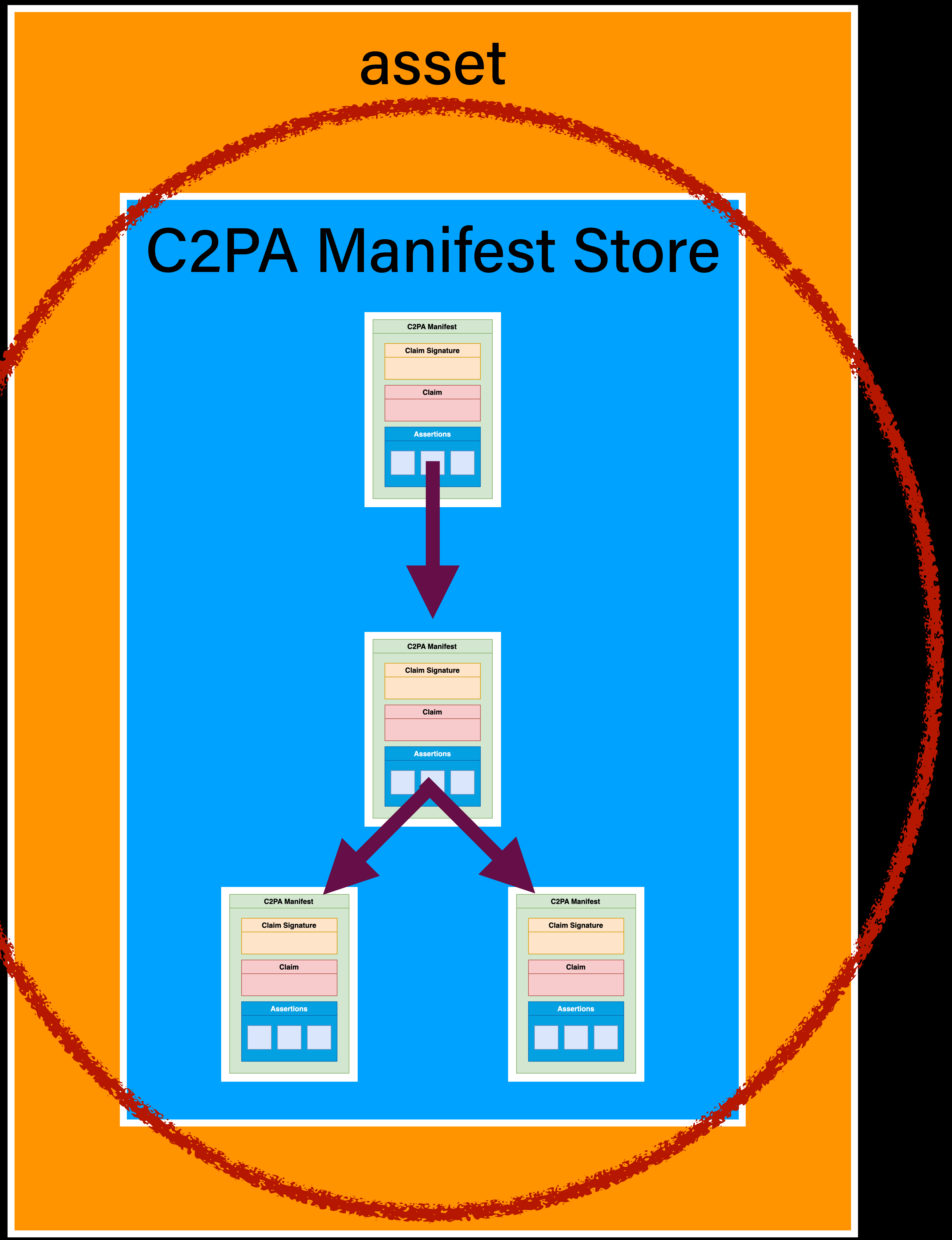
Overview

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

It is described by a **C2PA Manifest**. Each asset in C2PA has an *active manifest* which describes the current asset.

That C2PA Manifest may refer to *ingredient manifests* when earlier content is incorporated.

The collection of C2PA Manifests is referred to as a **C2PA Manifest Store.**

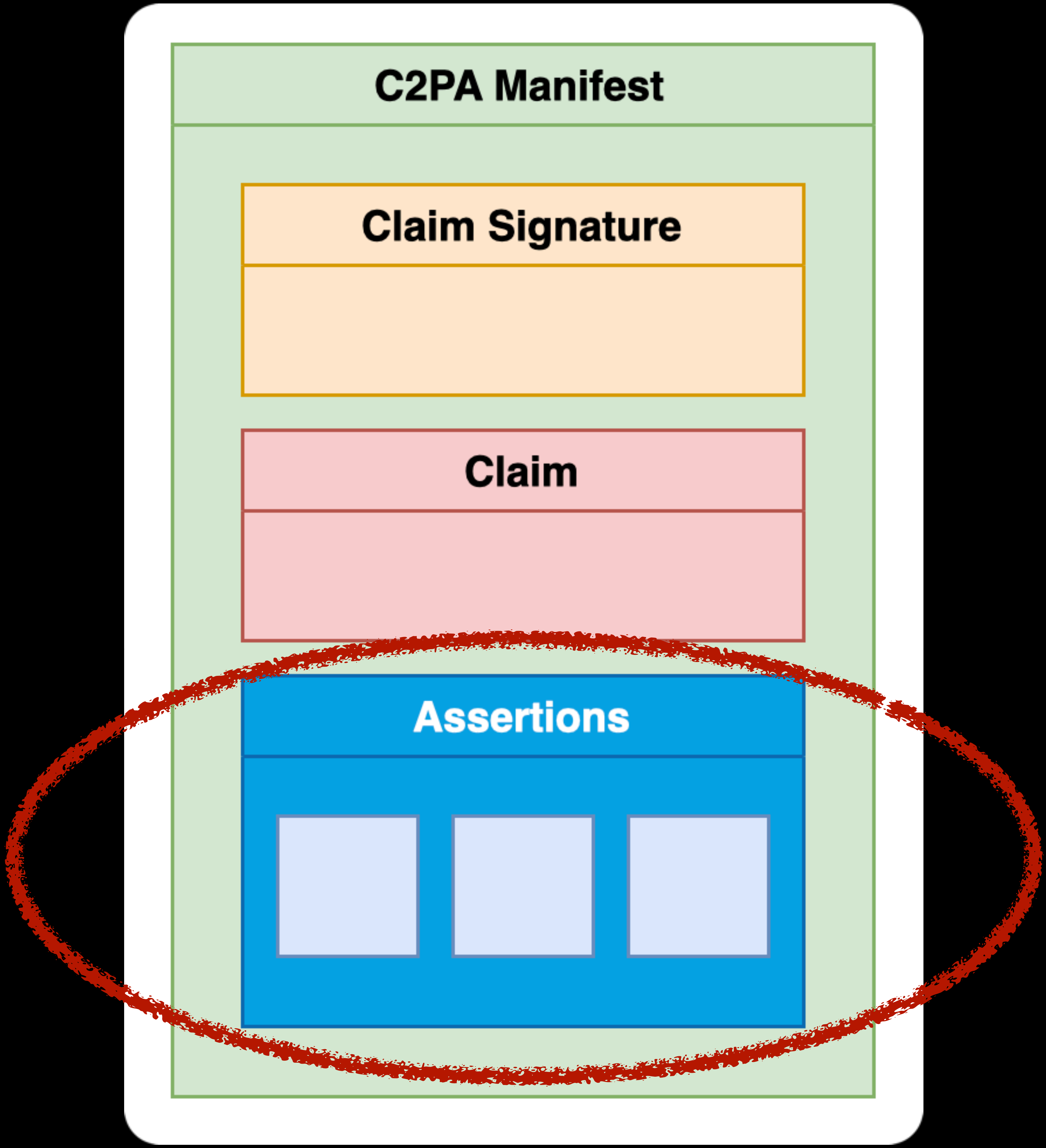


C2PA data model

Assertions

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

- hard binding to asset’s binary content *(required – provides tamper evidence)*
- capture device details
- edit actions
- thumbnail of the content
- other content (ingredients) that were incorporated into this content

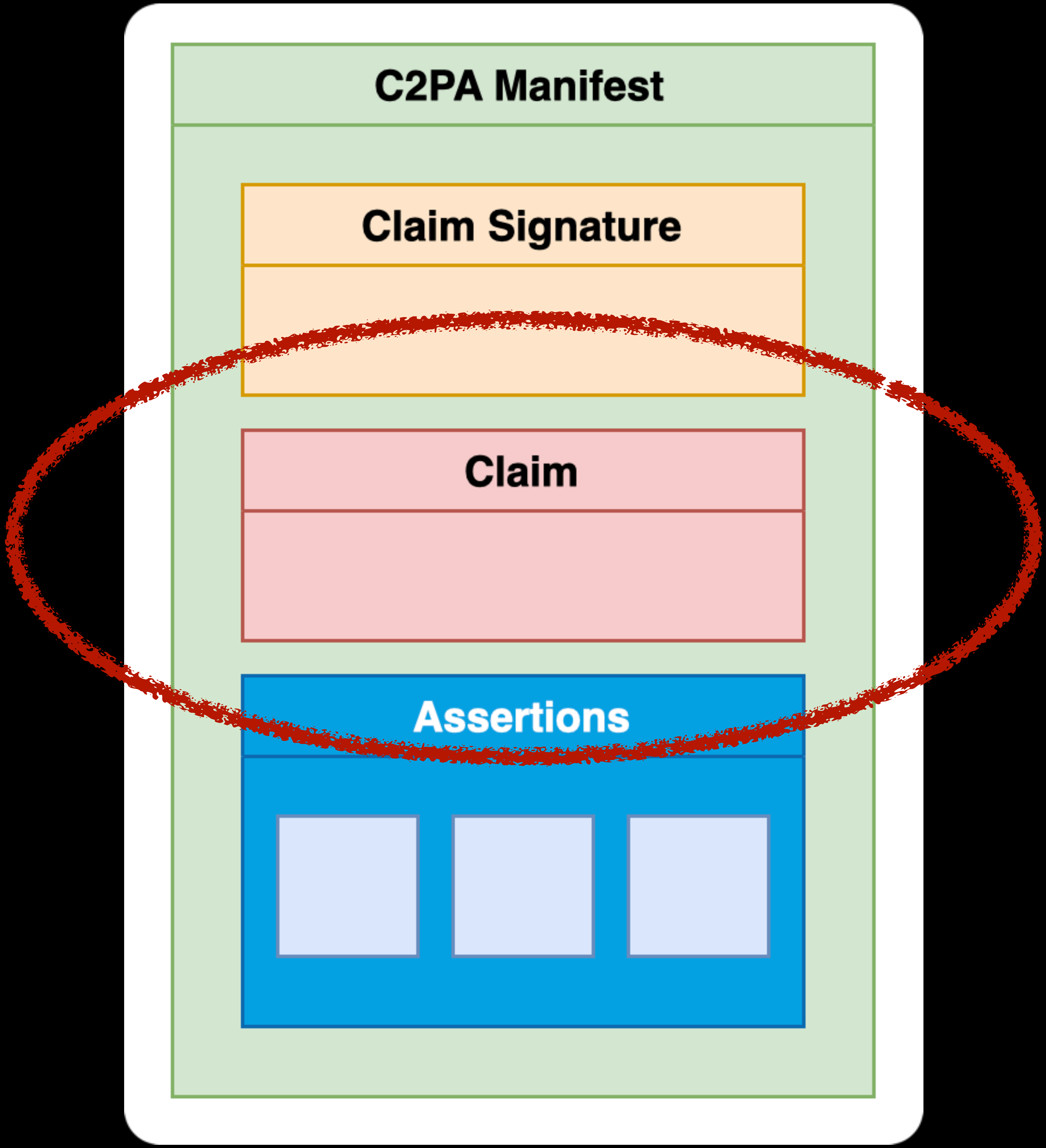


C2PA data model

Claim

Every C2PA Manifest has exactly one **claim,** which contains:

- a list of its assertions (via hashed JUMBF URI)
- information about who created the claim (typically tool vendor)
- assertions from ingredients that were redacted

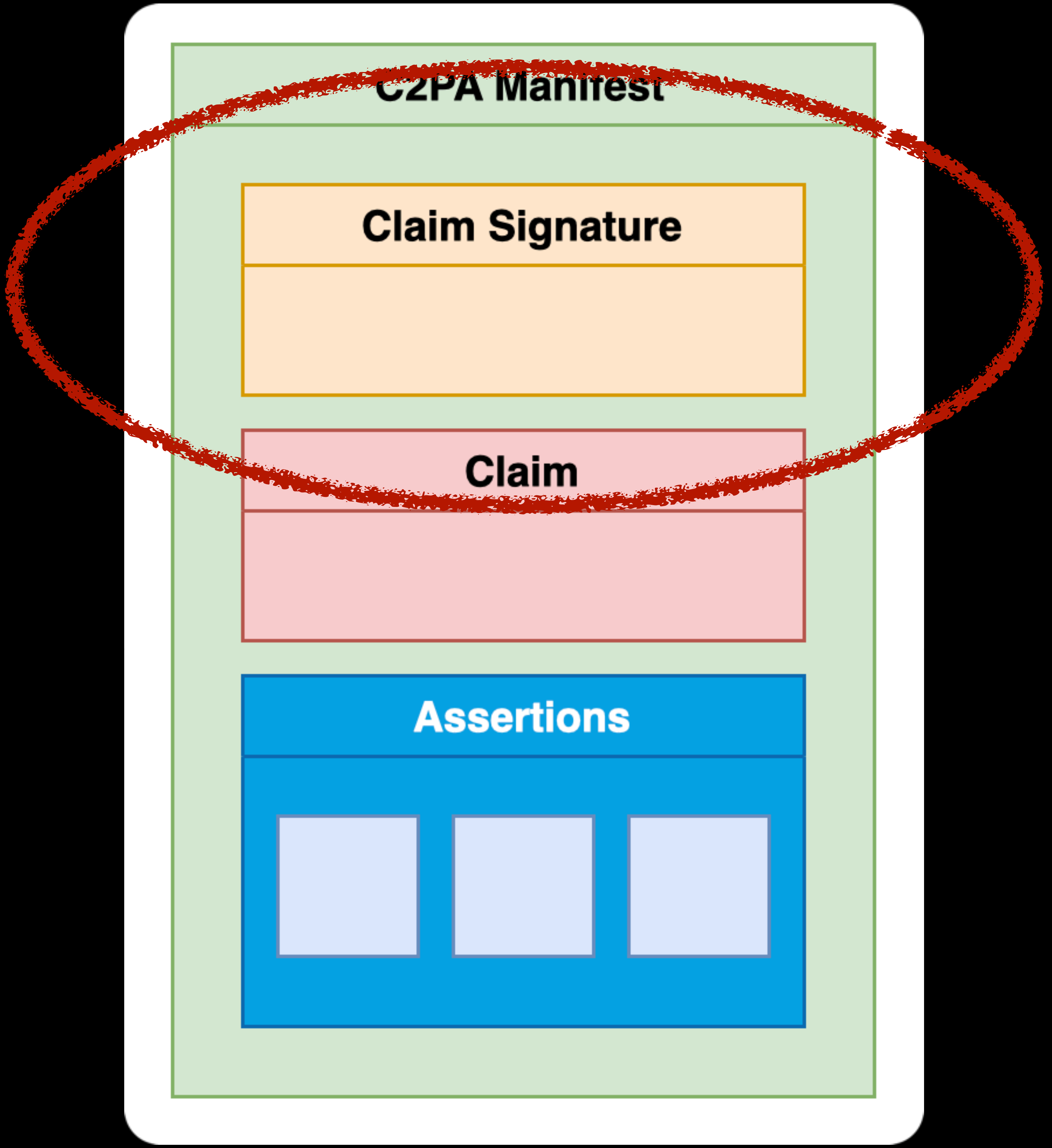


C2PA data model

Claim signature

A **claim signature** is a COSE signature that binds the claim data structure to an X.509 certificate holder.

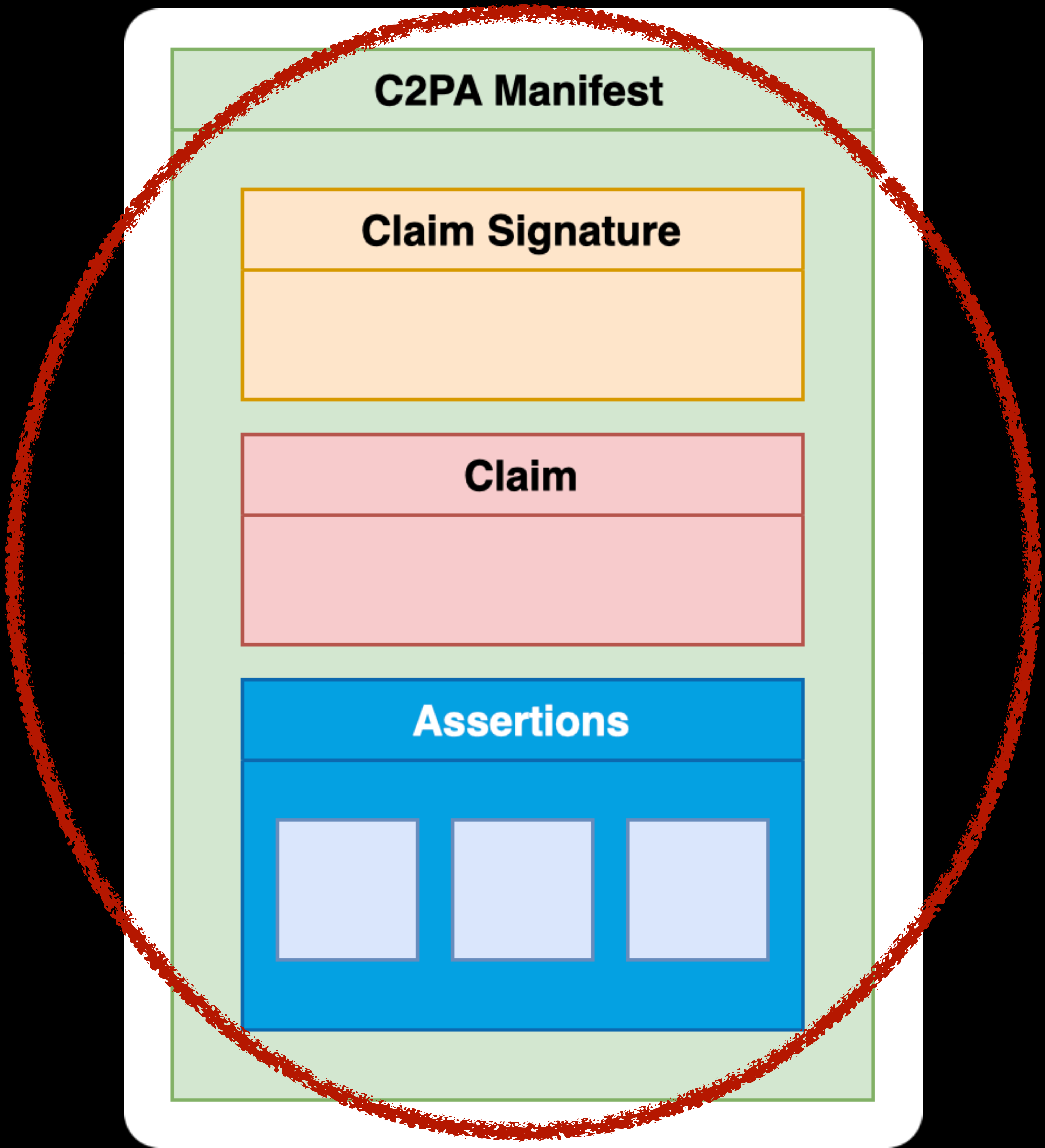
The X.509 certificate typically identifies the *implementation* of C2PA (hardware or software), **not** the content author.



C2PA data model

C2PA Manifest

A **C2PA Manifest** is a JUMBF data structure which contains the claim signature, claim, and assertions.



Creator Assertions Working Group

How identity fits into the C2PA ecosystem

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}*

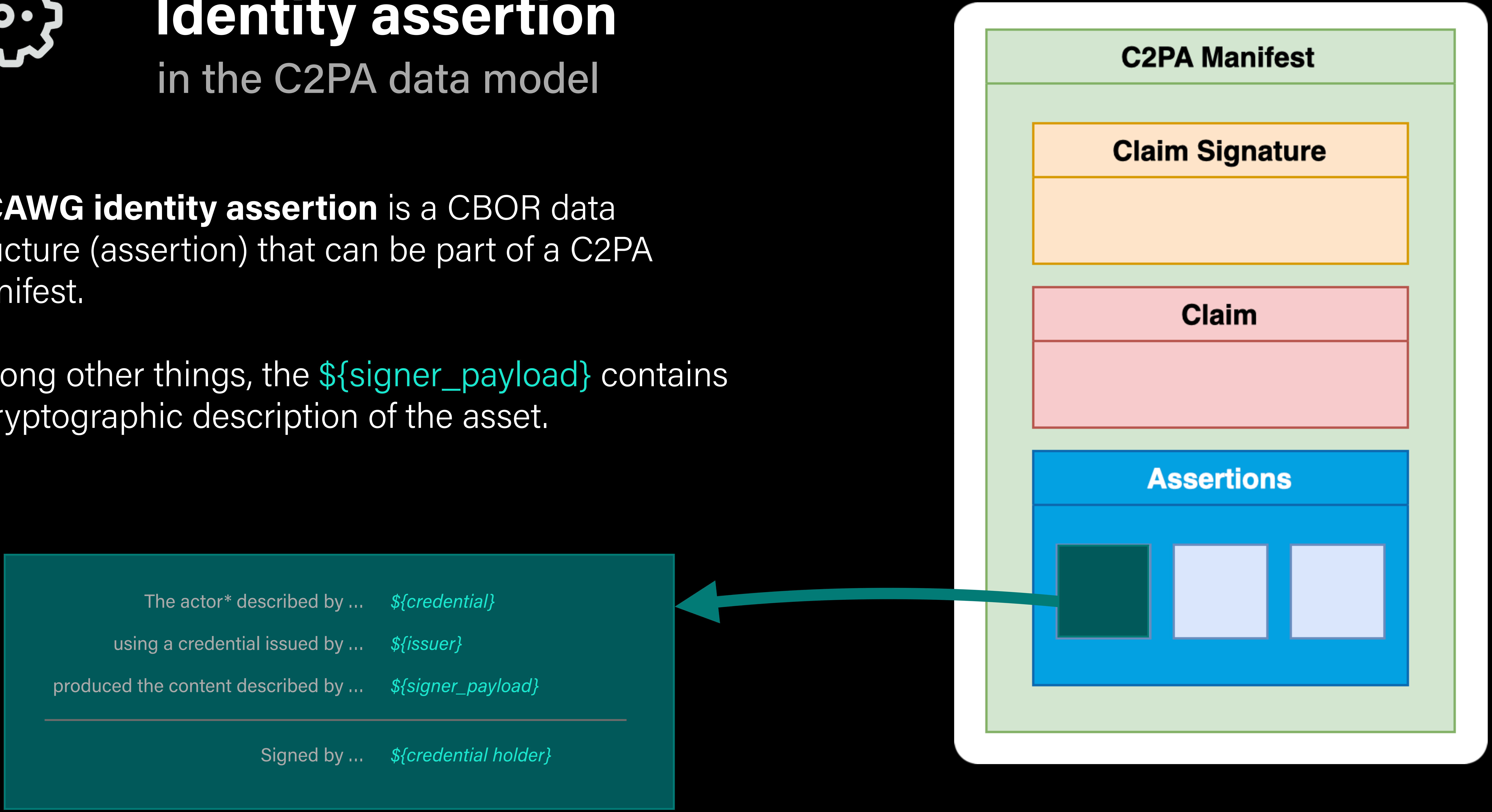
*actor can be human, non-human, or organization of humans

Identity assertion

in the C2PA data model

A **CAWG identity assertion** is a CBOR data structure (assertion) that can be part of a C2PA Manifest.

Among other things, the ${signer_payload} contains a cryptographic description of the asset.



The actor* described by … ${credential}

using a credential issued by … ${issuer}

produced the content described by … ${signer_payload}

Signed by … ${credential holder}

C2PA Manifest

Claim Signature

Claim

Assertions

Identity assertion

in the C2PA data model

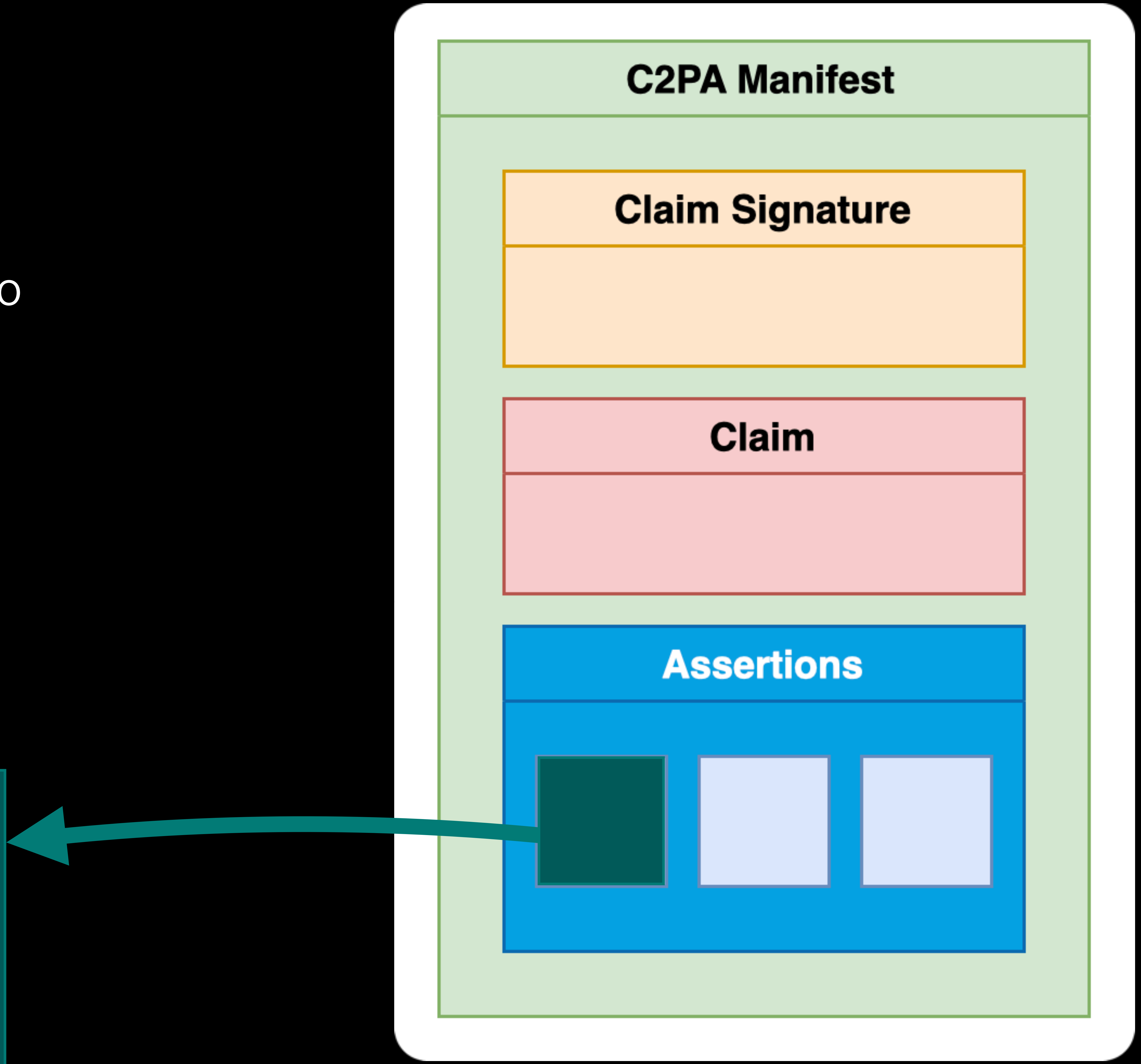
A **CAWG identity assertion** is typically meant to indicate subject's **authorization or active participation** in production of the asset.

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

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

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

Signed by ... *${credential holder}*



Identity assertion

How do content creators want to be identified in 2024?

Identity assertion

GOOB

(Get Out of the Building)

Identity assertion

Who we’ve talked to (so far)

Institutional news media

Individual creative professionals

Institutional brands

Identity assertion

Institutional news media

The actor described by … X.509 certificate

using a credential issued by … certificate authority

produced the content described by … ${signer_payload}

Signed by … certificate holder

(CAWG identity assertion 1.0)

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

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

(CAWG identity assertion 1.1 draft – in progress now)

Dude (Person), where’s your DID?

My challenge to the SSI community ...

Connect the dots.

Introduce me to content creators who have access to autonomous signing credentials and know how to use them.

Identity assertion

Who’s next?

The actor described by …	???
using a credential issued by …	???
produced the content described by …	${signer_payload}
Signed by …	content creator for themselves, ideally

Identity assertion

Help us build it!

- **https://creator-assertions.github.io**
- Weekly meetings:
  - Typically on Mondays
    0800 US Pacific / 1100 US Eastern / ~~1500~~ 1600 UTC
  - Contact me (scouten@adobe.com) for invitation