# CAWG's identity assertion: A framework for asserting provenance

*Eric Scouten, CAWG co-chair*

## Introduction

I am often asked to explain how the CAWG identity assertion works and how it fits into the overall content authenticity ecosystem. This page is intended to provide a useful overview for understanding the identity assertion.

## What organizations are involved?

There are three independent organizations that collaborate to define and support the content authenticity ecosystem:

- The **Coalition for Content Provenance and Authenticity (C2PA)** defines *technical standards* that provide a framework for securely attaching metadata to digital media files ("assets") and defining specific metadata that can be asserted by the hardware or software implementing C2PA. Think of this as the **"What and how"** for digital media.
- The **Creator Assertions Working Group (CAWG)** defines *technical standards* for human-generated metadata about digital media that fits into the C2PA ecosystem. This work is primarily encapsulated in CAWG's identity assertion and metadata assertion specifications. Think of this as the **"Who"** for digital media.
- The **Content Authenticity Initiative (CAI)** is a business alliance that promotes the cause of digital provenance through education and public policy advocacy. It is also the name of the business unit at Adobe which supports all three of these organizations through open source, open standards development, and support of Adobe product teams implementing CAI.

For the remainder of this page, I will speak of C2PA, CAWG, and other standards that build upon the C2PA core specification as the **C2PA ecosystem.**

IMPORTANT

*CAWG is not part of C2PA*

A common misconception is that CAWG is a working group *within* C2PA. It is not.

C2PA has since 2024 chosen to focus exclusively on metadata that can be directly attested to by a hardware device or software tool *without* human input.

CAWG was created at that time to provide a home for metadata that is attested to by individual or organizational content creators. It is a working group within the Decentralized Identity Foundation (DIF). A membership in DIF is required to participate in CAWG.

## Who signs what?

When an individual or organization wants to claim attribution for a specific content, they sign with their own credentials, *separately* from the hardware or software tool that generated the binary representatio of that content. This separate provides a clear indication of who is taking responsibility for what parts of the content, as shown in the table below:

| | **C2PA claim generator** | **CAWG named actor** |
|---|---|---|
| Specification | C2PA Content Credentials | CAWG identity assertion |
| Who is signing? | Hardware or software product | Individual or organizational content creator |
| How many signatures? | Exactly one, required | Any number, optional<br><br>Available for those content creators who wish to identify themselves as content creators. |
| What are they taking responsibility for? | Information available without human input, e.g.<br>• GPS data<br>• Time of capture<br>• Edit actions taken<br>• Was AI used?<br>• Ingredients incorporated | Information provided by humans, e.g.<br>• Who created the content?<br>• Events or locations depicted in content<br>• Other metadata for context |
| What credential are they using? | X.509 certificate issued to “conforming products” (i.e. hardware or software that demonstrates compliance with C2PA rules) | Multiple credential types (see CAWG credential types below) |

## CAWG credential types

(TO DO: Describe the currently-supported credential types and plans to extend.)

## How is this different from XMP, IPTC, and Exif?

Let's start with how the C2PA ecosystem is *similar* to the existing metadata formats: Many of the same kinds of information that can be conveyed using XMP, IPTC, and Exif standards (e.g., capture device information, location, description, and authorship claims) can also be conveyed through the C2PA ecosystem.

What sets the C2PA ecosystem apart is:

- **C2PA metadata is *securely* attached to content.** C2PA uses cryptographic hashes and signatures to ensure that metadata is not changed since it was changed. These techniques also ensure that a valid C2PA manifest can not be transplanted and used to describe content other than the specific file that it was *intended* to describe. We think of this as a **tamper-evident "nutrition label"** for content.
- **C2PA metadata contains an audit trail.** Unlike XMP, IPTC, and Exif, C2PA metadata *retains* prior attestations when existing content is incorporated into new content. This means that a content consumer can trace back through potentially many sources and read the attestations from each source's creator.
- **CAWG identity assertions require secure digital credentials.** A claim of authorship, as described by the CAWG identity assertion, can only be signed using a digital credential using a private/public key pair. This serves to prevent false claims of authorship.

The specifications on this site are provided under the terms of the W3C Patent Policy, except where otherwise noted.

The UI for this site is derived from the Antora default UI and is licensed under the MPL-2.0 license. Several icons are imported from Octicons and are licensed under the MIT license.

Authored in AsciiDoc. Produced by Antora and Asciidoctor.