Coalition for Content Provenance and Authenticity

Content Credentials

Deployment Guidance

1.0, 2026-07-08: Release

Table of Contents

About This Document

This document was prepared by the Coalition for Content Provenance and Authenticity (C2PA) as a brief explainer for any entity (business, government, organization etc..) interested in implementing the C2PA specification.

The C2PA is the open standards organization responsible for developing and maintaining the Content Credentials specification (the standard). Content Credentials help people understand where a digital file came from (for example, whether it was made by a person or generated/edited by AI) and whether key information about that file has been altered. This guide gives a practical, non-technical overview of what Content Credentials are, what to ask vendors for, and how to choose products that support Content Credentials in a reliable way.

Chapter 1. Introduction

C2PA is a non-profit, multi-stakeholder standards body hosted by the Linux Foundation. It created Content Credentials so that publishers, agencies, and the public can quickly answer practical questions about a file such as: Who created it? Was AI used? Was it edited after it was created? Content Credentials are designed to work across many products and platforms, so that implementers can rely on a consistent approach instead of one-off vendor labels.

At a high level, Content Credentials work like a tamper-evident packet that travels with a file. The packet is digitally signed, which helps tools detect whether the information has been changed since it was attached. When a product supports Content Credentials, it can attach this packet when content is created or edited, and other products can read it later to show a clear history of what happened to the file.

Though often conflated, the C2PA technical specification is distinct from watermarking and fingerprinting technology. When combined, they can form what is referred to as "Durable Content Credentials."

Chapter 2. Content Credentials Capabilities Overview

The C2PA standard for Content Credentials — currently on version 2.4 — supports a broad range of media types and file formats, making it applicable across virtually every category of digital content that an organization is likely to encounter or produce. For images, the spec supports widely used image formats including JPEG, PNG, TIFF, and WebP, among many others. For video, it supports MP4, as well as support for live video streaming and distribution, a significant capability for distributing real-time or recorded communications. Audio formats including MP3, WAV, and AIFF are supported, as are documents such as PDF and common Office file formats. A full list of supported file formats is available in the C2PA technical specification, which can be found here.

Content Credentials can also record a straightforward "change history" for a file—such as whether it was created, edited, cropped, resized, translated, redacted, or published. For transparency needs, one especially important feature is that the standard supports clear statements when AI was used to generate content or to make edits (both significant and minor). When present, those statements can be read by other tools that support Content Credentials, giving everyone a consistent way to spot AI-generated or AI-modified material.

Chapter 3. The C2PA Conformance Program

C2PA runs a formal Conformance Program that helps purchasers confirm whether a product implements the Content Credentials standard correctly and with specific security assurances. Products that complete this program are listed publicly as having passed conformity assessment. Selecting a product that has passed this assessment reduces risk: it provides an independent signal that the product correctly implements the standard and meets a minimum bar of security and assures interoperability. The program covers three categories of participants: generator products (tools that create and attach Content Credentials to digital content), validator products (tools that read and verify Content Credentials), and certificate authorities (the entities that issue the cryptographic signing certificates that underpin the trust model). Conforming products are held to published security requirements and must demonstrate correctness before being listed on the official C2PA Conforming Products List.

The Conformance Explorer allows anyone to browse and search the Conforming Products List and related Trust Lists. The lists can be used to confirm whether a vendor's product has completed the conformance process and, where relevant, whether the product's signing certificates are on the official C2PA Trust List. This can give additional assurance on the security and reliability of C2PA implementations and that those will be detected and treated accordingly by conformant C2PA validators.

While central to the future of the C2PA ecosystem, the conformance program is a relatively new effort that was launched June 4th, 2025. Since its launch, 54 products from 31 companies have passed conformance (as of May 14, 2026), and over 120 additional companies have submitted expressions of interest to participate in the program. C2PA expects the number of assessed products to drastically increase over time as the C2PA ecosystem will use the conformance program for interoperability and security. Buyers/acquirers should be aware that there is a queue to go through the conformance program at the time this document was written.

Chapter 4. Other Implementations

As noted above, not all C2PA implementations have gone through the Conformance program; however, they may still self-assert that they meet the requirements of the C2PA specification. Buyers/acquirers may wish to verify that a product *and* configuration reliably produces, preserves, and displays Content Credentials in the real workflows and interoperates with other systems (as needed) because the standard can be implemented in multiple ways.

Please note the outputs of non-conformant implementations may not always interoperate with other implementations. To verify a non-conformant implementation before selection, ask the vendor to provide a short demo or screenshots showing:

1. how Content Credentials are attached on output,
2. how AI-generated or AI-modified content is indicated,
3. which default settings ensure credentials are applied without relying on individual users, and
4. if the outputs are recognized as carrying valid Content Credentials by downstream tools and platforms.

Chapter 5. How to Get Started: A Step-by-Step Guide

5.1. Identify Your Role in the C2PA Ecosystem

Before selecting tools or updating workflows, determine how you interact with digital content. Some scenarios often involve more than one role:

- **Producer**: You create or publish digital content, such as official photos or AI-generated images. Producers use tools that attach Content Credentials during creation or editing.
- **Validator**: You review or publish content created by others and need to verify its provenance. This includes displaying Content Credentials on public websites or internal review systems.

Understanding your role helps you choose the right tools and set the right expectations with vendors.

5.2. Choose a Tool or Platform That Supports Content Credentials

The most important decision in this process is selecting tools that meet the needs of your workflow by attaching, preserving, or displaying Content Credentials. Start by defining your needs (for example: Content Credentials are applied by default for agency AI outputs; Content Credentials are preserved through your publishing workflow; and staff or the public can verify them easily). When evaluating a tool, one should ask the vendor to demonstrate:

1. **How Content Credentials are attached** when content is created or exported.
2. **How AI-generated or AI-modified content is indicated** in the tool's interface.
3. **Whether Content Credentials are applied automatically** without relying on individuals to enable a setting.
4. **How Content Credentials are preserved** end-to-end across your workflow.
5. **Whether the tool's signing approach is recognized** by verification tools used in your workflow.

These demonstrations should reflect the *actual workflow* you use, not idealized or one-off scenarios.

5.3. Generating and Attaching Content Credentials to AI-Generated Content

When AI-generated content is created by an application that supports Content Credentials, the tool will:

1. Record that the asset was newly created.
2. Attach an assertion identifying the content as AI-generated.
3. Log key details such as the tool used and a creation timestamp.
4. Cryptographically sign the Content Credential and embed it into the file.

The practical workflow is simple:

1. Generate content using your AI.
2. Before publishing, confirm the asset carries Content Credentials. Most tools will indicate this in their interface.
3. Avoid screen-shotting or re-exporting the file through tools that remove metadata, as this can strip the embedded Content Credentials. Always work with the original exported file.
4. If edits are needed, use tools that support Content Credentials so that the edit history can be appended to the existing provenance chain.

5.4. Verifying and Displaying Content Credentials

Whether you are verifying received content or preparing to publish content to the public, the verification step confirms that Content Credentials are present, intact, and trustworthy.

To verify a file:

1. Visit **verify.contentauthenticity.org**, a free, publicly available verification tool that accepts uploaded files and displays their Content Credentials.
2. Upload the file. The tool will indicate whether Content Credentials are present and whether they are valid and/or trusted.
3. Review the provenance summary, which will show who signed the content, when, what tool was used. In addition, be sure to review whether it was flagged as AI-generated or modified.

Verification results:

- **Valid**: The Content Credential is cryptographically intact and neither it nor the digital content has been tampered with, but the signer may not be on the C2PA Trust List.
- **Trusted**: The Content Credential is intact and the signer is on the C2PA Trust List.
- **No Content Credentials found**: The file either was not created with a conformant tool or the Content Credentials were stripped during handling.

You should treat content with missing or invalid Content Credentials cautiously.

5.5. Embedding a Verifier on your Websites

When publishing AI-generated or modified content publicly, displaying Content Credentials to your audience is the final step in the transparency chain. The goal is to allow the public to click on an image or piece of digital content and see its provenance, similar to how the Department of Defense has implemented this on its Defense Visual Information Distribution Service (DVIDS) media platform or platforms like LinkedIn and YouTube display Content Credentials.

1. Link to or embed **verify.contentauthenticity.org** on pages that host AI-generated or modified content, allowing visitors to upload and inspect files themselves. (Other tools that support the C2PA standard are also available for this purpose.)
2. Where technically feasible, work with your web team to display the "**Cr** icon" (the Content Credentials badge, as described here) with AI-generated assets on your site. Clicking the icon surfaces the provenance panel to the user.
3. Include plain-language messaging near AI-generated or modified content explaining what Content Credentials are and what the "**Cr** icon" means — most members of the public will not be familiar with the standard yet.
4. Ensure your implementation meets WCAG accessibility standards.

Chapter 6. For More Information

For more information, clarifications, or questions please contact info@c2pa.org.

Chapter 7. Appendix

Content Credentials are the core of the C2PA standard. They are cryptographically-bound information embedded directly into digital content that records its origins, any modifications made to it, and the tools or processes involved. Because they are digitally signed, any tampering leaves a detectable trace. For AI-generated content specifically, Content Credentials can identify that an image or video was produced by a generative AI model, which model or platform produced it, and when.

Watermarking, as used in this context, refers to imperceptible hidden data embedded within the content itself. Unlike embedded information, a watermark is designed to survive actions that would strip or separate a file from its credentials, such as screen-shotting or re-recording. However, watermarks can only carry a small amount of data, and can in some cases be removed or spoofed. But when present, the watermark serves as a persistent signal that the content is associated with a particular Content Credentials, even if the embedded version is lost.

Fingerprinting creates a numerical value derived from the content's actual pixels, frames, or audio waveforms, similar to how a music-matching service can identify a song from a short sample. The fingerprint is stored alongside the Content Credential and can be recomputed later to attempt to match content back to its provenance record, even if the embedded information has been removed or lost. Unlike watermarking, fingerprinting requires no information to be embedded in the digital content itself.

No single technique is sufficient on its own: embedded information can be stripped, watermarks can be defeated, and fingerprint matching is probabilistic rather than exact. Durable Content Credentials offer the potential to combine all three into a unified, layered approach that ensures provenance information can be recovered no matter where content travels or how it is redistributed.

It is this layered combination of secure metadata, watermarking, and fingerprinting that is possible with the C2PA specification that makes the C2PA technical standard the most comprehensive solution available for establishing transparent, verifiable provenance, including for AI-generated or modified content.