

Watermarks, Content Credentials and provenance

A practical guide to reading the evidence

Understand the terms

Visible labels, AI watermarking and signed records do different jobs.

Check the file

Learn what to inspect before relying on a PDF or presentation.

Know the limits

No mark or signature establishes factual truth on its own.

Start with the question you need answered

A presentation marked CONFIDENTIAL still needs sharing controls.

What should a reader see?

Use a visible notice to communicate status, attribution or intended handling.

What signal was embedded?

A watermark detector looks for a mark created by a particular marking system.

What record can I check?

Signed provenance lets a verifier examine recorded claims, their signature and their binding to an asset.

AI watermarking is not one technique

Ask which generator, media type and detector the claim covers.

A deliberately embedded signal

Marking changes an output in a way the corresponding detector is designed to recognize.

A result with conditions

Reliability depends on the scheme, content and transformations. Test your real distribution path.

A different task from classification

A post-hoc AI classifier estimates origin from content patterns without requiring a deliberately embedded mark.

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

C2PA makes provenance records checkable

The standard is a way to carry and validate evidence about an asset.

Record

A manifest contains claims about the asset, such as recorded creation or editing actions.

Sign and bind

A digital signature protects the claim; cryptographic bindings connect the record to the covered asset content.

Validate and interpret

Check signature, asset integrity and signer trust. Then read what the record actually says.

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

Three terms, three levels of meaning

Content Credentials are a way to inspect provenance, not a truth badge.

Digital provenance

Information about the origin and history of a digital item.

Content Credentials

The user-facing name for provenance information based on C2PA. Available fields depend on the record and the tool.

Content authenticity

A broader question about whether something is what it purports to be. Provenance contributes evidence; context and corroboration still matter.

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

Read a verification result in layers

Illustrative example: a publisher sends a signed report.

1 / Integrity

Does the signed record validate, and does its content binding match this file?

2 / Trust and claims

Who signed it? Is that signer trusted by this verifier? Which origin or edit claims are actually present?

3 / Context

Is this the intended edition? Do other sources support the report's factual claims?

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

PDF watermarks: label the page, check the record

A visible DRAFT stamp communicates status. It does not sign the document.

Visible watermark

Text or an image placed on PDF pages. Check page range, contrast and print appearance.

Digital signature or provenance

A separate mechanism. A conventional PDF signature and a C2PA credential are not interchangeable records.

Distribution check

Inspect and verify the exact version you send. Printing or exporting can change or omit evidence.

[Read more: encypher.com/content-provenance/pdf](https://encypher.com/content-provenance/pdf)

PowerPoint and Keynote: start with layouts

A logo on one slide does not establish provenance for the deck.

PowerPoint

Use the slide master or relevant layout for a repeated visible label; check all layouts used by the deck.

Keynote

Edit the slide layouts used by the presentation and add the intended text or image. Check individual slides.

Export

Open the exported PDF or PPTX. Inspect labels and recheck any separate provenance evidence.

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

Use layers for different jobs

Choose controls from the requirement, not from the word watermark.

Communicate

Visible labels tell readers how a document is intended to be handled.

Check evidence

Signed provenance links recorded claims to an asset. Some systems use watermarks to help recover a provenance record.

Restrict access

Sharing permissions and access controls govern who can retrieve a file. They do not make provenance complete.

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

A five-question release check

Use one non-sensitive file and your actual sharing workflow.

Before release

What should the mark communicate? Which parts of the file does the provenance cover?

At the recipient

Which tool can inspect the evidence? Does the result survive the export and delivery steps you actually use?

Before relying on it

What does this result leave unanswered about authorship, truth, ownership or earlier history?

[Read more: encypher.com/content-provenance](https://encypher.com/content-provenance)

Keep the guides beside the workflow

Four short explainers, with practical steps and primary sources.

Learn the distinction

C2PA vs AI watermarking;
Content Credentials,
provenance and authenticity.

Apply it to files

PDF watermarking; PowerPoint
and Keynote watermarks.

Try a public example

Visit encypher.com/try for the
signed-text demo, or
encypher.com/verify to inspect
a supported signed file.

Encypher explainers and implementation guides

Continue learning with Encypher. Standards and application references follow.

Encypher: What is content provenance? (explainer)

<https://encypher.com/content-provenance>

Encypher: C2PA and watermark verification (implementation guide)

<https://encypher.com/content-provenance/verification>

Encypher: PDF content provenance (implementation guide)

<https://encypher.com/content-provenance/pdf>

Standards and application references

Official specifications and vendor documentation. Checked September 11, 2026.

C2PA 2.4 Explainer, sections 2, 7.2, 7.3 and 7.5

<https://spec.c2pa.org/specifications/specifications/2.4/explainer/Explainer.html>

Google DeepMind: SynthID, how it works

<https://deepmind.google/models/synthid/>

Google Gemini Help: verification results and SynthID limitations

<https://support.google.com/gemini/answer/16722517>

OpenAI: AI text classifier, withdrawal notice and limitations (2023)

<https://openai.com/index/new-ai-classifier-for-indicating-ai-written-text/>

Standards and application references

Official specifications and vendor documentation. Checked September 11, 2026.

C2PA 2.4 Technical Specification, introduction and technical overview

https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html

Adobe: Add watermarks to PDFs in Acrobat on desktop

<https://helpx.adobe.com/acrobat/desktop/edit-documents/add-backgrounds-and-watermarks/add-watermarks.html>

Adobe: Validate digital signatures

<https://helpx.adobe.com/acrobat/desktop/e-sign-documents/manage-digital-signatures/validate-digital-sign.html>

Microsoft: Add a watermark to your slides

<https://support.microsoft.com/en-us/office/add-a-watermark-to-your-slides-1246244d-f465-4e4f-b9f9-49acdae00ff1>

Standards and application references

Official specifications and vendor documentation. Checked September 11, 2026.

Apple: Add and edit slide layouts in Keynote on Mac

<https://support.apple.com/guide/keynote/add-and-edit-slide-layouts-tan7a2b69972/mac>

Apple: Export to PowerPoint or another file format in Keynote on Mac

<https://support.apple.com/guide/keynote/export-to-powerpoint-or-another-file-format-tana0d19882a/mac>

Apple: Open or close a Keynote presentation on Mac

<https://support.apple.com/guide/keynote/open-or-close-a-presentation-tan72232b56/mac>