



Trust in action

Content credentials
prove trust that travels
across circumstances
and time

eBook | 2026



Introduction

Artificial Intelligence has fundamentally changed how digital content is created, edited, published, and consumed.

Images, videos, and audio that once carried an implicit assumption of authenticity can now be generated, manipulated, or impersonated with remarkable realism.

As a result, trust in digital content is eroding.



At the same time, organizations face increasing pressure to demonstrate transparency around digital media.

Regulations such as the EU AI Act Article 50 and the U.S. states laws, together with growing customer and platform expectations, are driving the need for verifiable provenance and authenticity throughout the content lifecycle.



The industry has spent years trying to detect what is fake. The next generation of digital trust focuses on proving what is authentic.

The Coalition for Content Provenance and Authenticity (C2PA) provides an open standard for creating Content Credentials—a cryptographically signed record that documents where content originated, how it has changed, and who published & distributed it.

This paper explores three real-world scenarios that demonstrate how content authenticity creates trust, protects organizations, and enables digital content to carry proof of authenticity wherever it travels.

Use case 1:

Global sporting major events—protecting official content



Scenario

During a major sporting event final, billions of viewers watch a highly anticipated outcome.

Within seconds of a decisive score, official match highlights, photographs, player interviews, and social media content are published by tournament organizers, broadcasters, sponsors, and media partners. At the same time, AI-generated highlight clips, manipulated referee decisions, fabricated player interviews, and fake sponsor advertisements begin circulating across social media.

Fans, broadcasters, sponsors, and media partners all ask the same question:

Which one is official?



Challenge

The tournament organizer and its media partners must ensure that audiences can distinguish authentic content from manipulated or unauthorized versions.

Once official content is downloaded, shared, and republished across multiple platforms, traditional trust indicators quickly disappear.

By the time misinformation is identified, millions of viewers may already have seen it.



Why traditional approaches fall short

Watermarks can be removed. Metadata is frequently stripped during uploads. Social media verification only applies within individual platforms.

Once downloaded and reposted, content becomes difficult to authenticate.

How content authenticity works



Official content integrates the C2PA standard into its publishing workflow.

As authentic content is published, C2PA establishes Content Credentials and cryptographically signs each asset and every published highlight with verifiable information describing:

- Official publisher identity
- Publication timestamp
- Editing history
- Content provenance

Anyone receiving the content can use the tool to independently verify that it originated from the official organization.

Business impact



Protects official media from impersonation



Enables trusted content across distribution channels



Strengthens media partnerships



Protects sponsorship value



Improves fan confidence

Key takeaway



Trust should travel with the content, not remain tied to the publishing platform.

Use case 2:

Camera manufacturer and news media—trust in news

Scenario

A global camera manufacturer introduces cameras capable of embedding Content Credentials directly into photographs captured by journalists.

Images are immediately distributed to major news organizations worldwide.



Challenge

News organizations increasingly require assurance that published images originated from authentic devices and have not been manipulated before reaching the newsroom.

The camera manufacturer must provide trusted proof of origin without requiring that every customer build a complex trust infrastructure.



Why traditional approaches fall short

EXIF metadata is easily modified. File hashes only prove file integrity at the point of capture.

Neither approach establishes trusted device identity.

How content authenticity works



The camera manufacturer provisions trusted device certificates into imaging devices during manufacturing. Each captured image is associated with a trusted device identity from the moment of creation.

As images move into editing and publishing workflows, publishers and editors must add additional Content Credentials that record legitimate modifications while preserving the complete provenance history. Trust now follows the content throughout its lifecycle.

Business impact



Trusted image capture



Stronger confidence for news agencies



Improved evidentiary value

Key takeaway



Content authenticity does not end at capture, it evolves throughout the lifecycle.

Use case 3:

Digital evidence— preserving trust in court



Scenario

A law enforcement agency records body-camera footage during an investigation.

Months later, the footage becomes evidence in court.

Defense attorneys question whether the video has been modified.



Challenge

The agency must demonstrate not only that the video originated from an authorized device and was not fabricated by AI from the start, but also that every subsequent edit, transfer, and review is independently verifiable.



Why traditional approaches fall short

Checksums and hashes confirm file integrity but provide little context.

They cannot explain:



Who handled the content



When changes were made



What edits occurred



Who authorized them

How content authenticity works



First, law enforcement establishes trusted device identity for body cameras.

Next, as evidence moves through the investigation, evidence management systems, prosecutors, and court preparation adds new Content Credentials documenting each authorized workflow step.

The result is an independently verifiable chain of provenance that remains attached to the evidence throughout its lifecycle.

Business impact



Stronger chain
of custody



Increased confidence
in digital evidence



Reduced evidentiary
disputes



Greater
public trust

Key takeaway



Authenticity becomes part of the evidence itself.

A common challenge across every industry

Although these examples represent different industries, they all face the same challenge.

Organizations need to answer five fundamental questions:



Question #1

Who created this content?



Question #2

Where did it originate (imaging device, AI, or software)?



Question #3

Has it been modified (and if so, how)?



Question #4

Who published it?



Question #5

Can anyone independently verify these answers?

Generating compliant Content Credentials requires a C2PA Conforming Generator product(s), extensive security documentation, secure key management, trusted signing certificates, trusted timestamping services, and ongoing compliance with evolving specifications.

For many AI platforms, creative software vendors, publishers, and enterprise organizations, building and maintaining this infrastructure is outside their core business.

Content Credentials help answer these questions through standards-based cryptographic provenance.

However, implementing C2PA is often far more difficult than organizations expect.



Accelerating trusted content with DigiCert

DigiCert helps organizations adopt content authenticity without having to build and operate the underlying trust infrastructure themselves.

Imaging device manufacturers:

Through DigiCert Device Trust Manager, imaging device manufacturers can provision trusted device identities, deploy device certificates, and establish trusted roots that enable content authenticity beginning at the point of capture.

AI platforms, creative software, editors, and publishers:

Through DigiCert Content Trust Manager, organizations can integrate C2PA Content Credential generation and content signing directly into existing workflows using APIs.

Instead of building their own conforming signing infrastructure, organizations can rapidly introduce trusted content authenticity while DigiCert manages the underlying cryptographic trust services.

These capabilities include:



Enterprise-scale
signing infrastructure



Trusted signing
certificates



C2PA conforming
claim generation



Time Stamping
Services (TSA)



Global trust
infrastructure



Long-term
validation support



Worldwide identity
verification



Future-ready
cryptography

Together, Device Trust Manager and Content Trust Manager provide flexible trust infrastructure regardless of where trusted content begins—inside a camera, an AI generation platform, creative software, or a publisher's workflow.

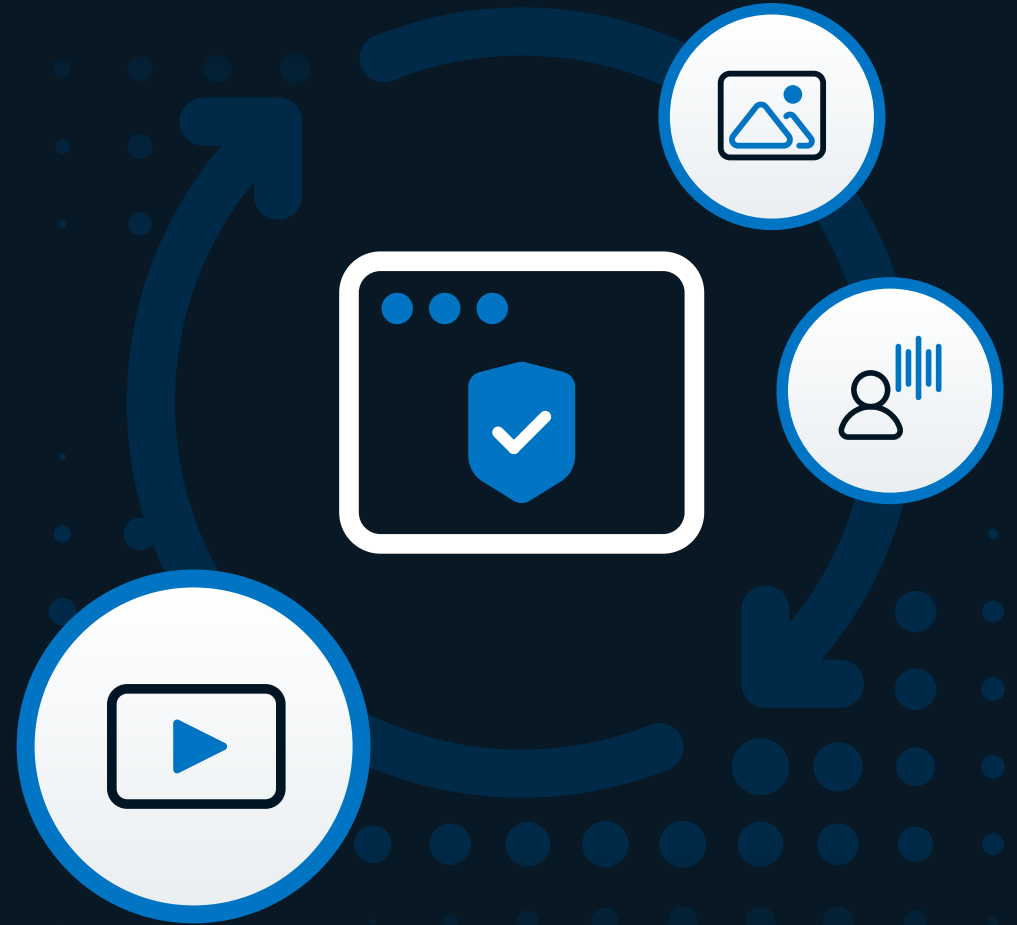
Conclusion

The future of digital trust will not be built by detecting manipulated content after it spreads.

It will be built by establishing verifiable authenticity from the moment trust begins and preserving that trust throughout every stage of the content lifecycle.

Whether content originates from a professional camera, an AI platform, a creative application, or a publisher's production workflow, organizations need a practical way to prove authenticity without building complex trust infrastructure themselves.

DigiCert combines trusted identity, enterprise PKI, device trust, Content Credentials, cryptographic signing, timestamping, and global trust infrastructure into a single platform that enables organizations to deliver one consistent outcome: trust proof that travels.



digicert®