

DigiCert® Content Trust Manager for Media (C2PA)

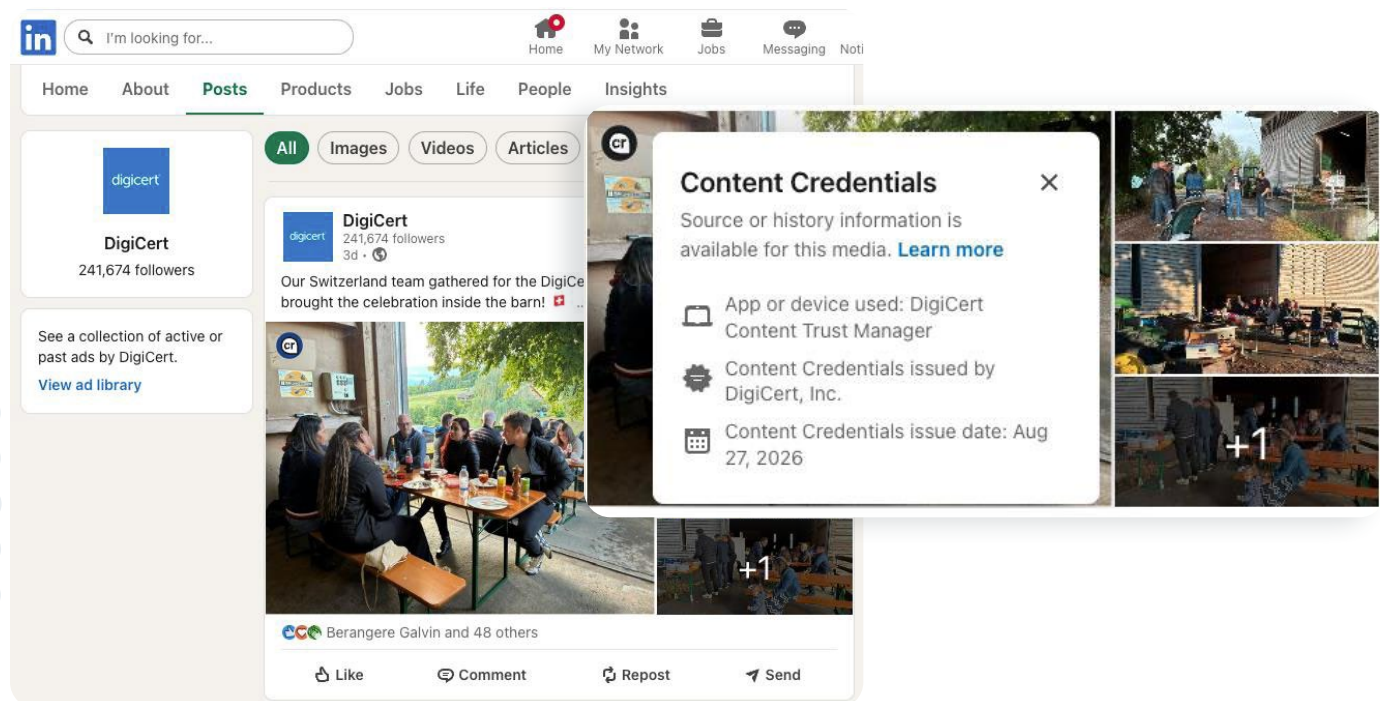


Prove media authenticity with trusted Content Credentials

Overview

Billions of digital assets are created daily, but trust in media is rapidly declining due to manipulation, deepfakes, and generative AI. At the same time, emerging regulations such as the EU AI Act are increasing expectations for transparency around AI-generated and AI-manipulated content. Organizations need a reliable way to prove content authenticity.

C2PA (Coalition for Content Provenance and Authenticity) specifications enable publishers, creators, and consumers to establish Content Credentials: cryptographically signed metadata that establishes provenance, tracks modifications, and ensures integrity across the content lifecycle.



[DigiCert Content Trust Manager](#) enables organizations to sign, verify, and track digital media using the C2PA standard, establishing verifiable provenance across existing content workflows without building and operating their own signing infrastructure. Content Trust Manager is backed by DigiCert's global trust infrastructure, C2PA root of trust, and time-stamping service.

What are Content Credentials?

Under the C2PA framework, content is accompanied by a cryptographically signed manifest that records key provenance details, including:



The creator or
issuing entity



The device or
application used to
generate the content



The time of creation
or publication



Any subsequent edits
or transformations

Content Credentials do not determine whether content is “true.” Instead, they verify that provenance information is authentic, well-formed, and untampered, and that the signer can be validated against trusted lists.

By signing content at the time of creation, editing or publication, organizations can:



Establish verified
origin



Track provenance
across the content
lifecycle



Ensure tamper-evident
integrity



Enable independent,
third-party verification

Key capabilities

Content Trust Manager delivers rich features across content security, authenticity, and governance.



Identity-based trust

- Enables organizations to assert their verified identity in C2PA Content Credentials using CAWG identity credentials
- Connects content to its source by demonstrating to recipients the organization asserting responsibility for published content
- Combines verified organizational identity with C2PA provenance and cryptographic signing so recipients can independently verify the identity assertion
- Builds on DigiCert's global identity validation and PKI infrastructure



Content provenance

- Generates and cryptographically signs C2PA-compliant Content Credentials
- Embeds tamper-evident manifests directly into media files
- Records claims about content creation, modification, and publication
- Allows new provenance entries to be added as content moves through its lifecycle
- Enables Content Credentials to be verified wherever the content travels



Tamper-evident integrity

- Cryptographically binds Content Credentials to the associated media
- Verifies that content matches the identity and provenance claims in its manifest
- Helps recipients assess whether content has remained intact or has been altered



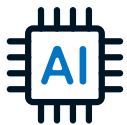
Scalable content signing

- Signs media created across different applications, platforms, and workflows
- Supports API-based hash signing, browser-based signing, and other enterprise signing methods
- Enables high-volume signing without tying organizations to a specific content-creation tool
- Integrates content signing into existing production and publishing workflows



Simplified C2PA Adoption

- Enables applications and platforms to sign through Content Trust Manager without becoming C2PA conforming products themselves
- Provides ready-to-use security architecture and cryptographic key management
- Handles key protection, rotation, revocation, and related operational controls
- Reduces the documentation, audit, and infrastructure burden of building an independent C2PA signing system



AI transparency and regulatory readiness

- Helps organizations identify AI-generated and AI-modified content
- Creates auditable records of content creation, editing, and publication
- Supports emerging transparency expectations such as those associated with the EU AI Act



[Explore the interactive demo](#)

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.