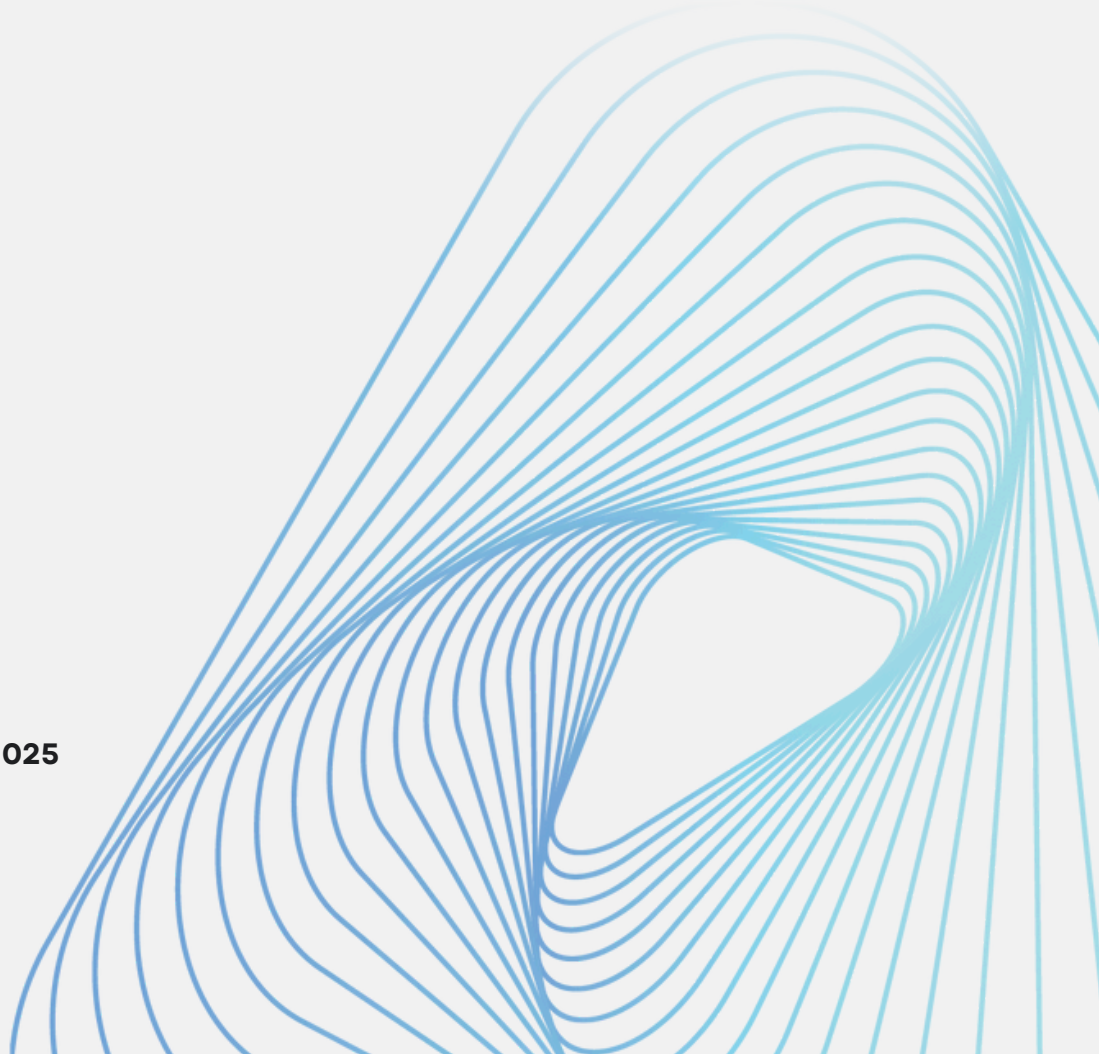
Tauth Labs

Communications and Content Provenance Authentication

A new approach to building trust into high-value communications content and protecting companies, journalists, analysts, clients and other audiences from misinformation, disinformation, imposter content, deepfakes and fraud.



White Paper, October, 2025

Simon Erskine Locke
M. Danish Bilal

Introduction

Communicators have always had to be concerned about protecting their companies from the impact of fake content, misinformation and disinformation.

In a world in which these issues were the exception rather than the rule, media monitoring and social media listening tools were mostly sufficient to identify and address occasional efforts to mislead, manipulate markets and damage reputations.

We are not in Kansas anymore. Generative AI is changing the communications and cybersecurity landscape. The ubiquity of access to sophisticated LLM-based tools that can create, manipulate and post AI-generated content in seconds, and at scale, has reset the risk table.

At the same time this new generation of tools provides communicators with ways to create content – whether documents, images, audio or video – more quickly and efficiently, they are also driving a surge in imposter content, deepfakes and sophisticated fraud.

In this paper we detail the role content provenance authentication will play in helping communicators protect brands, reduce misinformation, disinformation and fraud, and how authentication can be used as a means to differentiate and add value to content.

Warning Signals Are Flashing Red

Leading technology consulting and cybersecurity companies are warning that companies need to pay attention to these new challenges and take action to reduce the reputational and financial risks associated with them.

With exponential increases in AI-generated content and cyberattacks on Americans, trust in digital content is declining. For an industry in which content is key to audience engagement, the path to a “Zero Trust” world is an existential issue.

> As UC Berkeley Professor Hany Farid has pointed out, we are moving from a “trust but verify” to a “verify then trust” world. This has profound implications for the practice of communications and the digital landscape overall.

This new world requires a new set of digital tools to give journalists, analysts, corporate clients and consumers the ability to determine what they can trust. This is as essential to the digital economy as it is to the practice of communications.

Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity (C2PA)

Led by Adobe, the world’s largest technology and media companies, and a growing ecosystem of startups, have been working together as part of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity (C2PA) to address the challenge of building trust into content.

The technologies being used in this process, including user verification, digital watermarking, content credentials and blockchain, are well established. They have been used in different ways as the basis for signing legal documents, proving the origin of content, incorporating information about document creation, and providing immutable proof of authorship and provenance.

C2PA is an industry standard for content authentication built on an open-source platform. The technology standard is being used and implemented by member organizations worldwide and to develop user-focused solutions.

In the same way AI companies are building on large language models, companies, including Tauth Labs, are leveraging C2PA standards to provide authentication services.

Although the underlying technology is complex, its application can be as simple as one-click authentication, and even no-click or automated-content verification. It is this combination of ease of use, a widely adopted authentication standard, interoperability, and flexibility across different types of content, that is leading to the rapid and widespread adoption of these protocols.

How Authentication Technology Works

The simplest way to describe the technology is that it uses a three-step process:

1. organization/personhood verification
2. the integration of a robust digital watermark and content credentials
3. the option of logging authenticated content on blockchain

Once content has been authenticated, credentials can be viewed by the recipients in a number of ways, including through the integration of a trust seal, the download of a browser plug-in or by simply hovering over or clicking on a link.

Authentication builds into a file a digital fingerprint which, when combined with blockchain, makes a piece of content uniquely identifiable. Imagine a digital passport being created for each piece of authenticated content that can include a range of information to confirm its identity.

If we take the analogy one step further, the technology can prove identity for a range of countries (companies) and include information that the issuing organization considers important for its audiences. Using the underlying authentication technology provides a foundation for creating trust marks for different organizations and embedding customized information that would be the digital equivalent of height, eye color and gender.

The C2PA protocols enable the incorporation of a record of changes made to a document through the editing process. The approach is flexible enough to prove the identity of the company or organization issuing the document or maintain anonymity, while including other relevant data, such as geolocation.

Reduce the Risk Fake Content Will Be Shared and Acted Upon

Fake content is powerful and most damaging when it is shared and acted upon. Misinformation, disinformation and fraud are only possible because audiences receiving content are deceived into believing it is real (or want to believe it is true) and do something.

With government and non-government actors involved the social engineering techniques being employed are increasingly sophisticated multidimensional efforts to extract data, compromise technology systems and cause disruptions from which bad actors seek to profit.

Almost three-quarters of adult Americans report they have been subject to cyberattacks according to Pew Research. The losses to the U.S. economy in 2025 alone are projected to exceed $1 trillion according to Cyber Defense magazine.

A key part of the content authentication value proposition is the ability to reduce the likelihood that fake content will be shared before an article is written, a trade is executed or a social media post written.

Fake content will continue to be produced at scale. Giving target audiences a lifeline to be able to know what they can and cannot trust is essential in this environment.

Content authentication needs to be part of a multi-dimensional approach to increasing the security of content and identifying when fake content is shared.

Communication Use Cases

High-value communications content is just one of the many potential applications of the technology. Over time we believe that all digital content will incorporate authentication credentials. In the same way the shift from *http* to *https* has bolstered trust in websites, authenticating content will make it more searchable and more valuable.

In this paper, we focus on one of the many communications use cases for content authentication to illustrate its value proposition – press releases.

Since communicators produce a range of content from releases to corporate videos, it's important to note that authentication can be used across all communications and corporate content formats.

Press Releases

Content authentication built into press releases provides audiences the ability to determine if the release was in fact sent from XYZ company.

The difference between verification and authentication is significant. Today, press release distribution companies have robust verification processes to ensure that the company/individual posting a release on their platform is who they say they are.

Currently, when a release is shared from a communications department, agency or a distribution service, and is no longer in the custody chain of a company email or website, it is not possible for a journalist, client, search engine or LLM to definitively know if it is an authentic release or a release that has been manipulated.

Content authentication changes this dynamic. Incorporating credentials provides a definitive way to quickly and simply confirm that a press release is in fact authentic wherever it is sent on its digital journey.

While audiences receiving a release that does not include content credentials have the ability to go through their own verification process by going to the source, credentials provide an important layer of safety to reduce the risk that fake content will be acted on.

This matters in a world in which speed and automation are driving news and market trading. Content authentication provides a technical basis for journalists, content aggregators, search engines and LLMs to both trust and prioritize authenticated content. Over time, content without credentials will be a “STOP and proceed with caution” sign, in the same way a website without security credentials is today.

Communicators should expect to see a significant ramping up of fake releases and financial communications. The Journal of Accounting and Economics has reported a marked increase in AI-generated fake financial documents being issued around quarterly earnings. We are seeing a rise in fake quotes, statements and CEO deepfake videos.

The now widely-used term “AI slop” includes all content being generated and posted automatically, including fraudulent content. In the same way we have been inundated with spam email, spam content makes it far less likely that content that matters will be seen and acted on. Authentication offers a path to not only validating content but helping it stand out.

Authentication Makes Content More Valuable

The ability to integrate provenance credentials into content is not just a defensive step. Authenticating content will make it more searchable and more valuable in the digital ecosystem.

Part of the power of the C2PA standard and the companies supporting it is the ability for technology platforms to recognize and prioritize content that has been authenticated.

Trust is the foundation of the digital and communications economy. Without trust, audiences will not act on what they see whether an email, press release or a video from the CEO.

There is a built-in incentive for social media, search engines and LLMs to prioritize authenticated content. For content aggregators and organizations that share curated content, authenticated content provides a way to ensure that what they provide customers is trustworthy.

In a world in which the goal of content is to have it shared – potentially as widely as possible – this is a significant benefit.

C2PA Adoption

C2PA is moving from the technology lab into the real world. Companies have been implementing the standards now for around two years, but we are still in the early-adopter phase, as the technology heads toward mass adoption.

C2PA 2.0 standards were rolled out earlier this year and the process of implementing the technology is ongoing. Awareness is growing, but there remains significant work to educate potential users around these standards.

High-profile companies have already adopted C2PA-based authentication for a broad range of uses including Leica, Nikon, Canon and Sony. Agency France Press is authenticating its media content and OpenAI the images it generates. And, LinkedIn is supporting the standards to ensure that metadata for authenticated content posted on the platform is not striped off.

There are now more than 5,000 members of the Content Authenticity Initiative. This includes companies interested in content authentication, as well as those adopting the technology.

Authentication Works for Narrowcast Audiences

The value of content authentication for individual companies is not dependent on reaching mass scale or adoption.

The one-click simplicity of the authentication process when using C2PA standards means that when the technology is implemented organizations can immediately benefit from the security of authentication with target audiences. For communications this will likely include journalists, analysts and clients.

One way to think about this is to view content authentication as an evolution of digital signature technology. When content is authenticated, the equivalent of a digital signature is incorporated into the document in a way that multiple recipients of the document can confirm it is authentic.

From a journalist or analyst perspective they are able to see in the document that it carries a trust mark and link to the authentication details. As discussed earlier in this paper, a trust mark or link to the content manifest can be visually incorporated into a document. For an image or video, the digital watermark can be embedded in a way in which credentials are visible or not visible (requires the use of a verification tool to verify authenticity).

The key takeaway is that authentication works from day one for B2B or narrowcast audiences. As it is more broadly adopted, familiarity will drive audiences and consumers to confirm whether a document has been authenticated without prompting.

Authentication Technology as a Basis for Fraud Detection

Once content has been authenticated it also becomes possible to build new tools to automatically identify content similar to the original version and verify if it is has been faked or manipulated.

Since much of the risk associated with content comes from materials that appear real to audiences, the ability to identify content that looks similar to that which has been authenticated is valuable. The same approach can be applied to images, audio and video.

Custom Solutions: Authenticating Existing Content, Customizing Manifests and Managing Content on Blockchain

It is possible for organizations to authenticate existing content and build in security benefits, customize content manifests for specific use cases, and manage authenticated content on blockchain.

When blockchain is used to create an immutable hash that is connected to individual pieces of content, as we do at Tauth Labs, it is important to be able to manage the repository of authenticated content.

We use Ethereum to log content and provide clients the tools to manage content hashes. Importantly, a significant technical benefit of C2PA combined with blockchain, is that only the content manifest, not the content itself, is stored. This maximizes security and minimizes the storage required on blockchain.

Integrating Content Authentication into Workflows

We have developed core authentication and verification tools. The key to the successful implementation of the technology is its integration into existing workflows. Our tools are designed to be built into CMS and publishing systems, as well as to be used as part of a final step in the authentication process.

When integrated into existing workflows, authentication can be as simple as checking a box before publication or creating a button in a CMS system. The technology integration process can be based on APIs or the development of additional interfaces. As with AI or other technologies, having a clear set of user technology and integration requirements is essential.

This requires a consultative approach to authentication discussions that look at goals and objectives for each client, as well as the desired customization of trust marks and content manifests. Given the use of common core technologies and platforms for CMS systems, the process is relatively straightforward.

For use cases where authentication is a final and separate step in the publishing process, C2PA-based authentication and verification tools can be used outside a company's firewalls if desired.

Content Authentication & the Law

The federal government and legislators across the country are working on a range of laws around AI disclosure, deepfakes and content authentication. In New York at the time of writing, a bill (S7963) was under consideration that would require political communications to include content authentication using C2PA standards.

The legal context for authentication is shifting quickly, but we believe that over time to address the risk of consumers being defrauded, the case for the widespread adoption of content authentication will become stronger, providing further impetus for its use.

Takeaways for Communicators

As we have outlined in this paper, content authentication addresses critical challenges facing content producers in general, and communicators specifically. It provides a path to build trust into content and a way for audiences to verify that it is authentic and trustworthy.

As generative AI is used to exponentially increase the volume of content, providing critical audiences with a lifeline to know what can be trusted is just one dimension of the value proposition of the technology. Other benefits include the ability to differentiate content and make it more searchable as ways to add value. In addition, once content has been authenticated new tools can be developed to help companies identify fake or manipulated content.

We use the example of a press release in this paper for simplicity. The core principles of C2PA-based authentication apply to documents, images, audio and video. And, although our focus here is on communications, the applications are broad. The technology has the potential to be used for all digital content.

If there's one message communicators should take away, it is that the technology represents an even more fundamental shift in the digital landscape than that seen from the integration of security into websites. With content authentication we are building security certificates into individual pieces of content.

About Tauth Labs

Tauth, which is short for trusted authentication, was founded in 2024 to provide clients with access to simple, secure content authentication based on C2PA standards.

We are a contributing member of the Content Authenticity Initiative and the Coalition for Content Provenance and Authenticity.

Our C2PA-based tools can be integrated into workflows and CMS systems. We are focused on developing customized communications, financial and government applications.

The Founders

Simon Erskine Locke, Co-Founder, CEO

Simon Erskine Locke is co-founder and CEO of Tauth.io. Tauth's technology platform enables the trusted authentication of digital content. He is an entrepreneur and writer on communications and marketing issues. He founded CommunicationsMatch™ and Townhub. He is a founder of agencies and a former head of corporate communications functions at Prudential Financial, Morgan Stanley and Deutsche Bank. He is a member of the board of the Foreign Press Association of the United States.

M. Danish Bilal, Co-Founder, CTO

Muhammad Danish Bilal is the co-founder and CTO of Tauth, where he leads the development of a next-generation digital content authentication platform built on blockchain and cryptographic trust standards such as C2PA. With a background in AI infrastructure, blockchain security and decentralized identity, Danish has worked extensively on verifiable computation pipelines, PKI frameworks and smart contract security. He has co-authored research on blockchain-based PKI and Ethereum storage vulnerabilities, and has led deep tech initiatives spanning zero-knowledge proof systems, verifiable credentials and AI agent orchestration for Web3.

Contact Information

Email: slocke@tauth.io or mdanish@tauth.io

Website: www.tauth.io