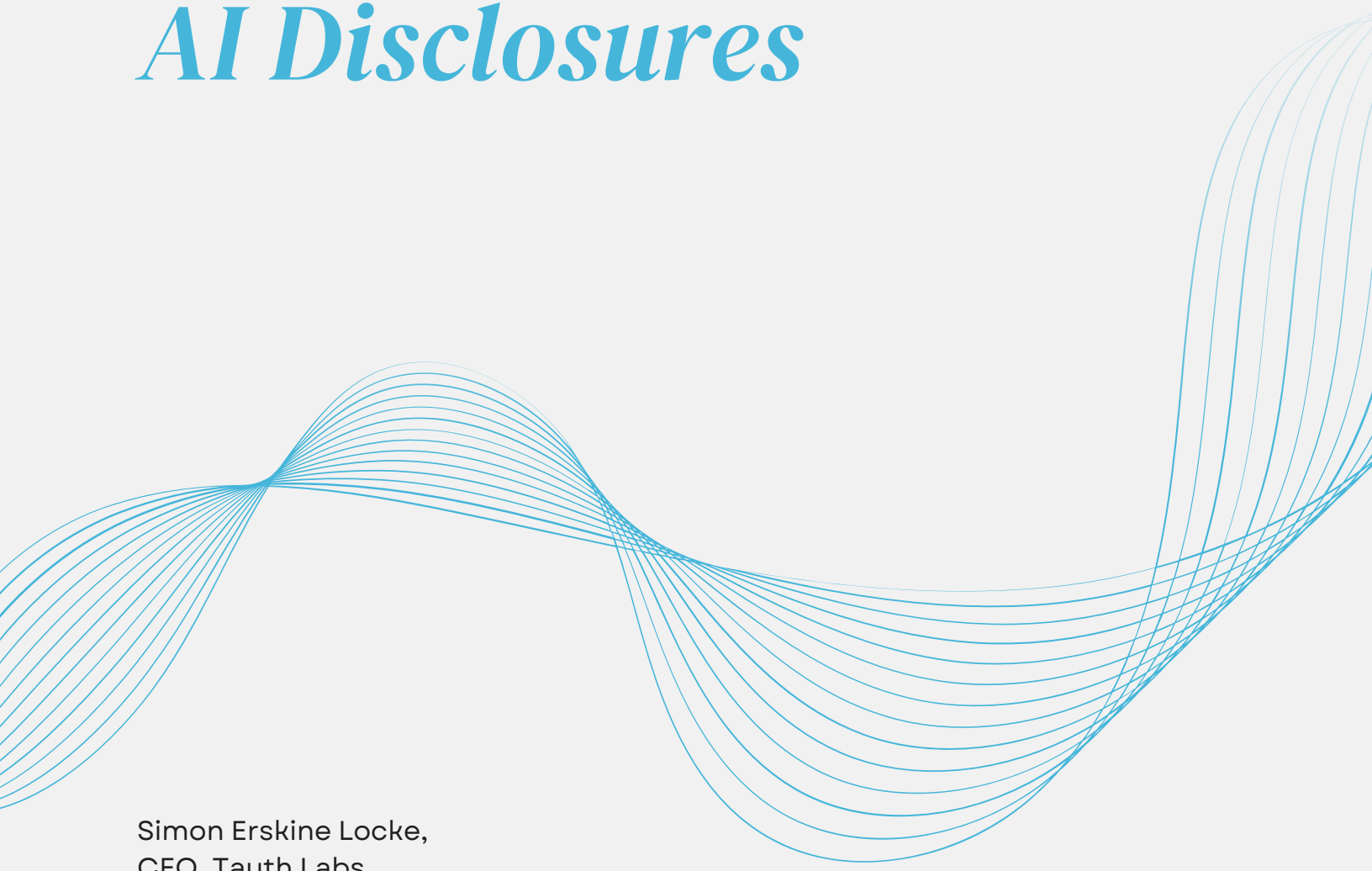


Tauth Labs Content Authentication Issue Brief, August 2026

Content Authentication, the EU AI Act, and AI Disclosures

A series of thin, light blue wavy lines that flow across the bottom half of the page, creating a sense of movement and depth.

Simon Erskine Locke,
CEO, Tauth Labs

M. Danish Bilal
CTO, Tauth Labs

Introduction

The EU AI Act's transparency obligations under Article 50¹ require the disclosure of certain AI-generated or AI-manipulated content distributed in the European Union, subject to specific exemptions². The Act does not only impact European companies. If you are an organization based in the U.S., Asia or other parts of the world that is targeting European audiences, your content is also subject to these rules, which took effect August 2, 2026³. Content authentication not only builds trust in content and makes it more discoverable, it helps address the EU AI Act's transparency requirements by supporting disclosures that are perceivable by both humans and detectable by machine-readable systems⁴.

Importantly, the disclosure process outlined in this paper can also be used to address requirements incorporated into legislation introduced and passed at a State level in the United States, as well as in countries around the world.

Content authentication also protects companies and audiences from shadow content (fake content designed with the intention to deceive or defraud) by providing a way to differentiate between fake and authentic content, and through the trust signal embedded into content makes it more discoverable. See: [Content Authentication: 10 Use Cases](#).

Content Authentication and Disclosure

Tauth Labs Really Simple Authentication protocols provide a means to manually or automatically authenticate AI-generated or manipulated content and meet transparency obligations under the EU AI Act. These vary depending on whether an organization is acting as a “provider” or “deployer,” as these terms are defined under the Act⁵, the type of content involved, and the intended audience. It is important to do a legal/compliance review of the impact on your organization. As a general matter, AI-generated or AI-manipulated content covered by Article 50 must be disclosed in a manner that is both machine-readable and human-perceptible, subject to the Act's exemptions. Tauth Labs' technology is a way to do this robustly for text, images, audio and video.

Providers and Deployers of Content

The EU AI Act differentiates between “providers” - entities that develop AI systems or put them into service, and “deployers” - entities, including publishers, that use AI systems under their own authority⁵. A generative AI system, such as a large language model, must be designed so that its outputs are marked in a machine-readable format and detectable as artificially generated or manipulated - a provider obligation⁶. A chatbot or other AI system intended to interact directly with people must be designed to disclose that they are interacting with AI, unless this is already obvious from the context⁷.

For deployers, an exemption from the text-disclosure obligation exists specifically for AI-generated or AI-manipulated text published to inform the public on matters of public interest where the text has undergone human review or editorial control and a natural or legal person holds editorial responsibility for the publication⁸. The Act does not require disclosure of an editorial process as a condition of the exemption, though publishers may choose to do so as a matter of transparency best practices. Deployers publishing AI-generated or AI-manipulated images, audio, or video content that constitutes a “deep fake” under the Act are separately required to disclose that the content is artificially generated or manipulated⁹.

Labeling Requirements

For AI-generated or AI-manipulated content subject to Article 50 disclosure obligations, embedded authentication credentials (machine-readable marking) and clear human-perceptible labeling are both generally required wherever content is shared with a public audience e.g. a newsroom, website or social media, subject to the exemptions described above². Our C2PA-based tools can both authenticate content, and if AI-generated, incorporate a visible "AI Generated" label consistent with the disclosure requirements. Our approach is designed to support disclosure requirements for text and other applications.

AI-Generated Images, Slides, Reports or Data

Communications, corporate and media publishers' content in general is still primarily human generated, edited and reviewed. The use of AI-generated text, audio and visual content is rapidly growing and used in combination with human generated content. A corporate press release may be written and overseen by a team of professionals, but charts, graphics or data that accompany it generated by AI. Whether disclosure is strictly required under the Act depends on the nature of the AI-generated element: such content will generally trigger the provider's machine-readable marking obligation, but will only trigger a deployer disclosure obligation if it meets the Act's specific definition of a “deep fake” -- content that resembles existing persons, objects, places, entities, or events and would falsely appear authentic⁹; routine data charts and graphics typically do not meet this threshold.

Tauth Labs' content authentication can be used to address disclosures for both the whole post and part of it, regardless of whether a strict legal disclosure obligation applies. With the use of AI for image generation for social media posts rapidly increasing, companies and publishers need to be mindful of where disclosure obligations do and do not apply in each communications channel. Where content that does constitute a deep fake forms part of an evidently artistic, creative, satirical, fictional, or analogous work, the Act requires only a lighter, non-intrusive disclosure rather than a full exemption⁹; best practice, in all cases, will be disclosure.

Building Authentication and AI Disclosure into Publishing Workflows and Newsrooms

Content authentication and AI disclosures can be built into existing workflows within our clients' technology environments. This can be automated if all content is AI generated; through the use of a check box if only some content is AI-generated content; or using an application for specific pieces of content. As options, authentication can also be conducted outside a company's IT environment, and content can be logged on blockchain.

Confidentiality of Content

The confidentiality of content prior to publication is a requirement for most implementations. Our authentication technology ensures that Tauth Labs does not see content prior to its publication at any time. The authentication process is generally conducted within our clients' technology environments and workflows. Publishing is controlled by the company doing the authenticating.

TrustShield

We provide clients the option to incorporate a TrustShield - a visible, clickable proof of authenticity and the AI disclosure built into content, e.g. "Company Name, Authenticated using C2PA. Generated using AI, Click to verify." This can be built into text documents, PDFs, and other forms of content.

Verification Under Organization Name and Within Its Domain

The cryptographic signing of documents as part of the authentication process is completed under the name of the client. Tauth Labs works with clients to create tools to verify the authenticity of releases and view disclosures within their environment, ensuring trust in the process.

Compliance

Legal and compliance have a key role to play in determining disclosure requirements based on each company's situation and use of AI - including whether the company is acting as a provider, a deployer, or both under the Act - which will define how the authentication process is implemented. Since content may be confidential and proprietary until publication, Tauth Labs does not see releases in advance of publication; and the release only becomes public upon publishing by the client, which has full control of the process.

Integrating authentication and disclosure around it helps protect the company; journalists, clients and audiences from the reputational and bottom-line risks from fraud; uses a globally recognized authentication standard; and provides the opportunity to integrate disclosures that meet EU AI and other legislation.

Tauth Labs Technology

Tauth Labs technology is a Certification Authority (CA) for the issuance of content credentials. We are a contributing member to C2PA and the Content Authenticity Initiative. C2PA is a global standard for content authentication supported by the world's largest technology and media companies compliant with NIST and other relevant security standards. The AI Act itself is technology-neutral and does not mandate use of C2PA specifically; C2PA is, however, referenced as a leading technical approach for machine-readable marking in connection with the EU's codes of practice on AI-generated content¹⁰.

Tauth Labs will provide SDKs/APIs required for authentication and verification. There is minimal support required by IT. Implementation generally takes around 4-6 weeks, followed by 1 week of testing and quality checks.

Endnotes and EU AI Act References

Supporting references for “Content Authentication and the EU AI Act” (Tauth Labs, Inc. | August 2026). Citations are to Regulation (EU) 2024/1689 (the EU AI Act).

1. Regulation (EU) 2024/1689 (the “AI Act”), Article 50 – “Transparency obligations for providers and deployers of certain AI systems.”
2. AI Act, Article 50(4). The second subparagraph exempts AI-generated or AI-manipulated text published on matters of public interest from disclosure where the text has undergone human review or editorial control and a natural or legal person holds editorial responsibility for its publication. The first subparagraph provides a separate, lighter disclosure obligation (not a full exemption) for deepfake image, audio, or video content that is evidently artistic, creative, satirical, fictional, or analogous in nature. A further exclusion applies where use is authorized by law for the detection, prevention, investigation, or prosecution of criminal offenses. See also Recital 134.
3. AI Act, Article 113: the transparency obligations of Article 50 apply from 2 August 2026.
4. AI Act, Article 50(2) (machine-readable marking – a provider obligation) and Article 50(4) (human-perceptible disclosure – a deployer obligation, applicable to deepfakes and to certain AI-generated or AI-manipulated text).
5. AI Act, Article 3(3) (“provider”: a natural or legal person, public authority, agency, or other body that develops an AI system, or has one developed, and places it on the market or puts it into service under its own name or trademark) and Article 3(4) (“deployer”: a natural or legal person, public authority, agency, or other body using an AI system under its own authority).
6. AI Act, Article 50(2): providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video, or text content must ensure outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. This obligation does not apply where the AI system performs an assistive function for standard editing or does not substantially alter input data provided by the deployer, or where use is authorized by law for criminal-justice purposes.

Endnotes and EU AI Act References, Continued...

7. AI Act, Article 50(1): providers must design AI systems intended to interact directly with natural persons so that those persons are informed they are interacting with an AI system, unless this is already obvious to a reasonably well-informed, observant, and circumspect person, taking into account the circumstances and context of use. This obligation does not apply to AI systems authorized by law for criminal-justice purposes, unless available for the public to report a criminal offense.

8. AI Act, Article 50(4), second subparagraph: deployers of AI systems that generate or manipulate text published to inform the public on matters of public interest must disclose that the text has been artificially generated or manipulated, unless the text has undergone human review or editorial control and a natural or legal person holds editorial responsibility for its publication, or the use is authorized by law for criminal-justice purposes. The Act does not condition this exemption on disclosing the existence of an editorial process.

9. AI Act, Article 50(4), first subparagraph, and Article 3(60) (defining “deep fake” as AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful). Deployers of such content must disclose that it is artificially generated or manipulated; where the content forms part of an evidently artistic, creative, satirical, fictional, or analogous work, this obligation is limited to disclosure in a manner that does not hamper the display or enjoyment of the work. See also Recital 134.

10. AI Act, Article 50(7): the AI Office is tasked with facilitating EU-level codes of practice to support implementation of the detection and labelling obligations in Article 50, adopted via the procedure in Article 56(6). The Act itself is technology-neutral and does not mandate use of any specific technical standard; C2PA has been referenced as a relevant technical approach for machine-readable marking in that context.

Tauth Labs Disclosure: This paper was written by the authors. Claude was used in its research. It was also used to fact check information and statements incorporated in the paper. Although the authors have made every effort to verify the content, AI does make mistakes. The intention is for the paper to serve as guidance around the general principles of the act and how content authentication can be used to meet disclosure requirements. The specific impact on a company, organization or publisher of the EU AI Act or any other AI transparency legislation needs to be determined through a legal or compliance review.

About Tauth Labs

Tauth Labs helps companies incorporate content authentication into work flows, to address the growing risk of misinformation and content fraud, as well as increase its value and searchability in the new “verify, then trust” digital world. Content authentication can also be used to meet disclosure requirements.

Tauth, short for trusted authentication, is at the forefront of building content provenance authentication applications that are based on foundational C2PA technology standards and developed by the world’s leading technology and media companies. We are implementing customized solutions for high-value communications, financial services, and AI content.

The company is a Certificate Authority (CA) for the issuance of C2PA content credentials. Tauth uses state-of-the-art standards for security, privacy, data-protection, and electronic signature regulations based on C2PA and NIST standards. Robust digital watermark for provenance authentication. Tamper-evident distributed data store (ISO 22739:2024). Developer-friendly SDKs and easily integrable with CMS platforms.

We have written numerous articles and a number of white papers, including “[Communications and Content Provenance Authentication](#),” and “[Trust, Content Authentication, and Financial Services](#),” in which we address a number of common questions about the technology and provide 10 use cases.

Contact us at slocke@tauth.io, tccheevers@tauth.io or visit www.tauth.io