

Contact

Oscar Covers
Policy Advisor Cyber Security
Liaison officer public-private partnerships
+31 655726017
covers@nvb.nl

Position Paper: Artificial intelligence makes source authentication vital

Source authentication is vital to distinguish authentic content from misleading AI-generated content. In this Position Paper, the Dutch Banking Association, explains why source verification is so important and why it should become part of basic hygiene. To make this possible, we need the cooperation of big tech, which is also the driving force behind the recent accelerated AI developments. In line with this, we have also contributed to the EU consultation for the development of guidelines and a code of conduct for transparent AI systems.

Introduction

With the increasing presence of AI, also comes the increase of misleading content and fraud. To protect ourselves from manipulation and fraud, it is crucial that we can distinguish whether information that is used for identification and authentication (in the meaning of verification¹) is real. The importance is easily illustrated with an example.

Every day, we initiate an identification and authentication process (in the meaning of verification) to access, for example, our private, work or financial environments on mobile, computer, etc. These digital environments are becoming increasingly important to us and therefore, it is very important that we can rely on a solid identification and authentication process. If we cannot distinguish reliably between authentic and AI-generated content, it could lead to identities being easily misused or taken over.

Digital environments are increasingly important and therefore, it is essential to be able to rely on a solid identification and authentication process. Financial services are among the first sectors to experience the negative impact of not being able to distinguish reliably between authentic and AI-generated content, for example via identities being easily misused or taken over. However, consequences can and will impact other sectors and society as a whole as well. Therefore, it is necessary to join forces to combat and prevent fake and/or misleading AI-generated documents and information.

Building on existing initiatives

To include authenticity characteristics in content is not new. The music and film industry has gained much experience with the application of digital rights management in relation to intellectual property. The stakes we discuss here are higher: we want to protect the reliability and trustworthiness of content like documents, audio, pictures, video itself.

Our goal can only be achieved through cooperation across sectors, big tech, media platforms, (financial) corporations and other relevant parties or by law. The European Union could take on this assignment, but there are also existing initiatives that could show the way. The Coalition for Content Provenance and Authenticity (C2PA) is an example of such an initiative. The C2PA includes significant platform operators² and develops standards to verify media content origin and history to combat online misinformation, for example through an open technical standard for publishers, creators and consumers to establish the origin and edits of digital content.

Source authentication is essential to combat content manipulation and fraud

Criminals are already deploying generative AI and deepfakes. We can only assume that the risk of AI will only increase fraud and other misuse by criminals in banking and financial services.³ This is especially important looking at the introduction of additional digital techniques and products (like Electronic Identification and Trust Services, 'European Digital Identity Wallet' (EUDIW) as part of eIDAS 2.0. The impact of an EUDIW issued wrongly or an account takeover is likely to be much greater. In addition, the NVB is concerned that the spread of deliberately false or misleading information (disinformation) does not solely lead to fraud, it also further increases the risk imposed to free and democratic societies.

¹ According to GDPR. Current standards, such as ISO/IEC 2382-37:2022, do not use the term 'authentication' to avoid confusion.

² C2PA coalition members: Adobe, Arm, BBC, Google, Intel, Microsoft, OpenAI, Publicis Groupe, Sony and Truepic. And the over 3,000 [members of the Content Authenticity Initiative](#) that support the C2PA standard

³ [Deepfake banking and AI fraud risk | Deloitte Insights](#)

Source authentication, or provenance, enables to verify the creator and origin of content. For example, hardware like a camera can use unique attributes provided securely by the operating system to confirm its authenticity. By appending i.e. a digital signature, the camera enables recipients to verify that photos or videos are genuine and unaltered. This process also helps prevent man-in-the-middle or live deepfake manipulation as hardware and used software authenticate themselves ensuring the video stream comes directly from the source without tampering

From a privacy point of view, it is good to stress that for the intended purpose, it is not necessary for source authentication to be traceable to a personal or device level.

We very much welcome the [C2PA](#) initiative as it comes from the major platform owners themselves. It is important that such a standard is widely accepted and applied as soon as possible.

Legislative perspective

The goal of this position paper aligns with both European and United States legislation.

- The EU AI Act⁴ mandates that AI systems that are used to create deep fakes must clearly disclose that content is artificially generated or manipulated.
- The American Content Origin Protection and Integrity from Edited and Deepfake Media Act⁵ mandates that any AI-generated or manipulated content must clearly disclose its artificial origin to prevent misinformation. It also puts journalists, artists and musicians in control of their content and prohibits tampering with or disabling AI provenance information.

However, criminals, by definition, do not obey the law. Therefore, we argue that not only when AI systems generate content, but in general when content is created, the provenance of content should be captured. So, if someone tampers with original authentic source or content it should lose its authenticity and thereby its trustworthiness. In this regard, we are strong advocates of self-regulation rather than *top-down* legislation.

Although not the primary goal of our position paper, the additional advantage of this approach is that it also provides a means for the protection of original content for creators.

Conclusion

Amidst the accelerated digital and AI developments, it is important to protect the authenticity of content. A careful, but albeit fast implementation is necessary. This is possible when big tech and are driving forces behind AI put their weight behind it and take ownership for their role. European institutions could, possibly should and however do not yet play a pivotal role in this. We should therefore support initiatives like C2PA, where involved companies and organisations show ownership and have taken on the challenge to solve the problem that lies ahead of us.

Dutch Banking Association

The Dutch Banking Association represents the common interests of the banking sector. Banks are important for everyone. We are the connecting link between the banking sector, politics and stakeholders. Together with these parties, we are proactively working on a service-oriented, stable and competitive banking sector.

⁴ https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

⁵ <https://www.commerce.senate.gov/services/files/3012CB20-193B-4FC6-8476-DDE421F3DB7A>