truepic

February 2, 2024

VIA ELECTRONIC FILING

Director Laurie E. Locascio
U.S. Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive Gaithersburg,
MD 20899

Re: AI EO RFI Comments

Dear Ms. Locascio,

Thank you for the opportunity to respond to this important request for information. Truepic is a US technology company specializing in secure content transparency, the highest fidelity method for disclosing the verified origin and history of digital content. We have helped lead the emerging provenance industry and are founding members of the Coalition for Content Provenance and Authenticity (C2PA). We are also members of the Content Authenticity Initiative (CAI) and the Partnership on AI's Responsible Practices Framework for Synthetic Media. Our leadership and participation in all of these organizations highlight our commitment to digital content provenance as the most promising approach to scaling transparency and authenticity in digital content. As noted in the Executive Order and elsewhere, with the growing accessibility of open source and commercial generative AI, synthetic media will continue to flood every aspect of business and society. According to the Partnership on AI and others, it is best to deploy digital content provenance through the C2PA open standard on both synthetic and authentic content. This helps reduce ambiguity in the information ecosystem and empowers content consumers to know what is synthetic vs. authentic.

As a founding and steering committee member of the C2PA, **Truepic supports the C2PA's open specification and asks that NIST consider that standard in its review of existing standards** in relation to the White House Executive Order on Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Truepic also aligns to and supports the C2PA's response to this same Request for Information (RFI).

In this response, we would like to emphasize and respond to specific prompts in Sections 1 and 2 of the RFI around best practices of provenance deployment in synthetic and authentic digital

content and in Section 3 around optimal implementation of standards. **Truepic believes robust security, including attestation, should be part of the media creation process and related to the digital signature**. Securing the creation environment, coupled with the C2PA's cryptographic hashing mechanisms, delivers the highest integrity form of provenance: **secure content transparency**. Secure content transparency will be necessary for many forms of media because content consumers must have confidence in the information that is digitally signed into a media file. Only when the software or platform is secure and attested can there be the highest integrity in the credentials presented. Secure content transparency can be deployed for generative AI platforms and for devices or cameras capturing authentic content.

Best Practices for Secure Content Transparency

Truepic follows a unique process to secure devices before and during the moment of content creation to ensure that the metadata being cryptographically sealed into a media file with the C2PA standard is of the highest integrity and accuracy. We refer to this process as **secure content transparency,** and we believe it is critical in any use case in which the information signed into the file must be authentic.

Truepic specializes in secure mobile technology through our iOS and Android SDKs, but we also have tools to add provenance in cloud- and server-based workflows. The process for authentic media creation begins with validation of the device, platform, or software integrity. Once deemed secure - not jailbroken, rooted, or otherwise compromised - only then can the device, such as a smartphone or tablet, capture or create media. If **secure content transparency** is not implemented, bad data can be fed into the eventual output, thereby undermining the C2PA signature's credibility and utility. Ensuring accurate data from the onset is **foundational to the integrity of the digital signature** and credentials. In addition to device security, additional best practices are also critical, such as using a trusted certificate authority registered on a trust list to back the signature, and using a timestamping authority to provide an accurate, provable time and date a signature was applied.

With a secured device, trusted certificate, and trusted timestamp, content consumers can have a significantly higher level of confidence that the information cryptographically signed with the C2PA open standard is of the highest integrity. That information, known as Content Credentials, can then be ingested by tools and relayed to content consumers, creating a more authentic information ecosystem. We also believe that content consumers should be able to identify the content captured or created with secure transparency vs. other content which may not have been attested and secured in the same way. For platforms that support Content Credentials,

verified metadata provides clear information about the origin and nature (synthetic, authentic, or composite) of digital content to empower trust and safety workflows, like content moderation, and also informs end-users when Content Credentials are displayed.

Examples

Below are specific examples on how unique implementations using Truepic's Software Development Kits (SDKs) to attest software and secure the content are deployed. Our partners across industries rely on this secure implementation of digital content provenance because it is critical for their operations that the data being cryptographically hashed to their files is accurate. Some examples are:

- ***Smartphones*:** In partnership with Qualcomm, Truepic demonstrated how secure content creation and transparency can be deployed on-device, directly from the trusted enclaves in chipsets. The partnership highlights that both synthetic and authentic media creation can be 1) attested, 2) cryptographically sealed, and 3) receive content credentials.
- ***Critical Documentation*:** In Ukraine, Truepic and Microsoft partnered to deploy Project Providence, the first C2PA-compliant documentation platform to assist USAID partners in documenting the destruction of cultural heritage. Deployed as a native mobile app on iOS and Android, the Project Providence platform allows media to be securely captured and shared. Captured media from this platform has been included in 10 different criminal cases by prosecutors and will be critical to remuneration and reconstruction efforts. This example is powered by Truepic's native mobile Lens SDKs, which enable secure capture and C2PA signing in any iOS or Android app.
- ***Operations*:** In the private sector, professional services firms like EXL digitizes hundreds of thousands of claims for the world's largest insurers using Truepic's implementation of content provenance. Private industry also necessitates attested and secure content transparency to successfully increase trust in their digital operations. Similarly, NGOs like the Near East Foundation use Truepic for oversight of a lending program in non-permissive environments.
- **Generative AI:** Generative AI platforms will need similar security at the creation process and Truepic aims to deploy its secure content transparency tools with Gen AI platforms in the coming year. Truepic has already partnered with Hugging Face, Revel.ai and others for early implementations of transparency in synthetic media.

Truepic helps enterprises to securely implement the C2PA at scale. The implementations listed above are cases where the information being cryptographically sealed into a media file with the C2PA standard must be sufficiently authenticated for lasting media integrity. In our opinion, ensuring the security of the content capture environment, through measures like device attestation, is the most robust way to do so.

Challenges

Like all open standards, the C2PA needs to be widely adopted to be most effective. Without widespread adoption across the internet's most-used platforms, inadvertent edits and media processing workflows may disrupt provenance trails. Currently, social media platforms strip metadata out of digital content posted on their sites. By opting to support C2PA, they can effectively disclose to their users whether content has been AI-generated or not, as compared to manual labeling of content, which is sometimes done today through moderation. When media files have Content Credentials, it is for the explicit, net-positive purpose of transparency. If an authentic capture has Content Credentials, it means the creator knowingly opted to add that transparency to their work. If synthetic content has Content Credentials, it means that the generative platform adhered to best practices and committed to transparently mark its outputs.

Another critical challenge is education. We must educate and explain to the general public what Content Credentials mean and what they do not mean. In our estimation, explaining what they mean is as important as explaining what they do not mean. Content Credentials are not instant indicators of truth or falsehood. Content Credentials are a multimodal tool that provides key details about the origin and history of a piece of content to help us evaluate what we see and hear online. They are a prompt to apply our media literacy skills and look at the provenance of digital content before making a decision of consequence, similar to how a shopper may look at a nutrition label before purchasing an item at the supermarket. Government can play a significant role here, helping to establish normalcy around transparency signals in digital content.

In its best practices and recommended implementation of the EO, NIST should keep in mind how implementation can help overcome these challenges. NIST's identification of and recognition of the C2PA can help to increase adoption and further critical educational efforts. Those implementing the C2PA specification should also understand the importance of attested software for high fidelity metadata and authenticated media origin.

We thank you for considering this submission and welcome any questions or follow-up.

Best,

Mounir Ibrahim
EVP, Public Affairs & Impact
Truepic