Google anunció el martes que sus nuevos teléfonos Google Pixel 10 cuentan de manera nativa con compatibilidad para el estándar de la Coalition for Content Provenance and Authenticity (C2PA), lo que permite verificar el origen y la trayectoria del contenido digital.

En ese sentido, se añadió soporte para las *Content Credentials* de C2PA en las aplicaciones Pixel Camera y Google Photos para Android. Según la compañía, esta medida busca reforzar la transparencia en los medios digitales.

Las *Content Credentials* de C2PA son un manifiesto digital con firma criptográfica, resistente a manipulaciones, que ofrece procedencia verificable de archivos digitales como imágenes, videos o audios. Este tipo de metadatos, de acuerdo con Adobe, funcionan como una *"etiqueta nutricional digital"*, ya que aportan información sobre el autor, el proceso de creación y si se utilizó inteligencia artificial (IA) en su generación.

"La aplicación Pixel Camera alcanzó el Assurance Level 2, la calificación de seguridad más alta actualmente definida por el programa de conformidad de C2PA", indicaron los equipos de Seguridad de Android y C2PA Core de Google. *"El Assurance Level 2 para una aplicación móvil, por ahora, solo es posible en la plataforma Android."*

"Los teléfonos Pixel 10 son compatibles con sellos de tiempo confiables generados en el propio dispositivo, lo que garantiza que las imágenes tomadas con la cámara nativa mantengan su validez incluso después de que caduque el certificado, aunque se hayan capturado sin conexión a internet."

Esta funcionalidad se logra gracias a la combinación del procesador Google Tensor G5, el chip de seguridad Titan M2 y las características de seguridad basadas en hardware integradas en el sistema operativo Android.

Google explicó que la implementación de C2PA fue diseñada para ser segura, verificable y utilizable sin conexión, de modo que los datos de procedencia sean confiables, que el proceso no revele información personal y que funcione incluso sin acceso a la red.

Esto es posible mediante:

- Android Key Attestation, que permite a las autoridades certificadoras de Google C2PA (CAs) comprobar que están interactuando con un dispositivo físico auténtico.
- Certificados de Android Key Attestation respaldados por hardware que incluyen el nombre del paquete y los certificados de firma de la app que solicitó la generación de la clave de firma C2PA, verificando así que la petición proviene de una aplicación registrada y de confianza.
- Generación y resguardo de claves de firma C2PA mediante Android StrongBox en el chip de seguridad Titan M2, para ofrecer resistencia contra manipulaciones.
- Atestación anónima respaldada por hardware, que certifica las nuevas claves criptográficas creadas en el dispositivo sin identificar al usuario.
- Certificados únicos para firmar cada imagen, lo que hace *"criptográficamente imposible"* desanonimizar al creador.
- Un componente Time-Stamping Authority (TSA) incorporado en el chip Tensor que permite emitir sellos de tiempo firmados criptográficamente al presionar el obturador de la cámara.

"Las Content Credentials de C2PA no representan la única solución para identificar la procedencia de los medios digitales", señaló Google. *"Son, sin embargo, un paso concreto hacia una mayor transparencia y confianza en los medios, mientras seguimos potenciando la creatividad humana con la ayuda de la IA."*