Echtes Foto oder KI? Pixel 10, Galaxy S25 und das Etikett C2PA - was es leistet und wo es versagt

Von Glieks-Redaktion · Veröffentlicht am 18.11.2026

Google baut das Herkunftsetikett C2PA in die Pixel-10-Kamera ein, Samsung unterstützt es im Galaxy S25 - doch Screenshots löschen es, Experten zweifeln und ein Sicherheitsforscher fälschte Signaturen. Der Stand der Debatte.

Das Nährwertetikett fürs Foto

Stellen Sie sich vor, jedes Foto trüge ein Etikett: wer es aufgenommen hat, womit, und was seitdem daran verändert wurde. Genau das verspricht der Standard C2PA (Coalition for Content Provenance and Authenticity). Er bettet nach TrueScreen eine signierte Herkunftsangabe („Manifest“) in Bilder, Videos, Audio und Dokumente ein, mit Angaben zu Werkzeug, Urheber und Bearbeitungen sowie einer kryptografischen Signatur. Jede Bearbeitung in einem kompatiblen Programm hängt ein neues Manifest an, sodass eine Kette entsteht [3]. Für Nutzer heißt die sichtbare Seite „Content Credentials“ [3].

Gegründet wurde die Koalition im Februar 2021 von Adobe, Arm, BBC, Intel und Microsoft; im Januar 2026 zählte sie laut TrueScreen mehr als 6.000 Mitglieder und Partner, zu den Geräten gehören unter anderem das Samsung Galaxy S25, Nikon-Z-Modelle und die Leica M11-P [3]. Wie weit die einzelnen Unternehmen den Standard tatsächlich umsetzen, schwankt stark [3].

Pixel 10: Das Etikett im Kamera-App

Google hat C2PA laut Börse Express (September 2025) direkt in die Kamera-App des Pixel 10 integriert und beschreibt es als erstes Mal, dass ein Hersteller solche Echtheitswerkzeuge in die eigene Kamera-App einbaut. Ergänzend setzt Google DeepMinds SynthID ein: ein unsichtbares Wasserzeichen in KI-erzeugten Medien, das Komprimierung, Zuschneiden und Farbkorrektur überstehen soll; der Prozessor Tensor G5 und der Sicherheitschip Titan M2 sollen die Daten manipulationssicher halten. Die Credentials sollen in Google Fotos, Lens und der Suche sichtbar werden; Google plant, den Ansatz auf Video und Audio zu erweitern [1]. Experten warnen laut dem Bericht vor zu hohen Erwartungen, und wer will, könne weiter Open-Source-Werkzeuge ohne Wasserzeichen nutzen [1].

Die Kritik: Ein Etikett ist keine Wahrheit

Born City fasst im Januar 2026 die Skepsis zusammen: Kennzeichnung könne ein falsches Sicherheitsgefühl erzeugen. Metadaten seien fragil, ein Screenshot oder eine neue Videokodierung könne die Herkunftsangaben entfernen, Hersteller setzten den Standard uneinheitlich um, manche kennzeichneten nur ausdrücklich KI-bearbeitete Bilder, und nicht gekennzeichnete Inhalte würden womöglich blind für echt gehalten. Kriminelle oder staatliche Akteure hielten sich kaum an Kennzeichnungsregeln [2]. Als Ergänzungen nennt der Beitrag Medienkompetenz, Erkennung anhand von Spuren in den Fälschungen selbst und Schutz auf Betriebssystemebene [2]. Die zitierten Studien, nach denen die meisten Menschen gute Deepfakes auch mit Warnhinweis nicht erkennen, werden dort nicht benannt [2].

TrueScreen, ein Anbieter von Zertifizierungs- und Beweissicherungsdiensten, ergänzt: Die meisten Plattformen komprimieren Uploads neu und entfernen Manifeste, Screenshots löschen sie völlig; C2PA dokumentiere Verlauf, nicht Wahrheit, denn auch eine gestellte Szene könne mit einer konformen Kamera ein gültiges Manifest erhalten. Zudem könne jeder ein Zertifikat erwerben und Inhalte signieren; ein vertrauenswürdiges Zertifikat koste rund 289 Dollar im Jahr [3]. Das ist ein Anbieter mit Eigeninteresse, der eigene Dienste als Ergänzung versteht [3].

Der Angriff auf die Pixel-Signatur

Eine deutsche Zusammenfassung vom 25. August 2026 berichtet über die Arbeit eines Sicherheitsforschers: Wer Root-Zugriff auf ein Android-Gerät hat, könne beliebige Dateien signieren, obwohl die Schlüssel in der Hardware (StrongBox) liegen; Prüfungen wie Key Attestation und Play Integrity ließen sich über Softwarelücken oder preiswerte Hardware-Fehlerinjektion umgehen. Als Beleg wurde ein KI-Bild als echtes Pixel-Foto verifiziert; Google habe den Bericht als „Won't fix“ geschlossen, aber ein Kopfgeld gezahlt [4]. Die Einschätzung „nicht zu beheben“ stammt vom Autor; in Kommentaren wurde laut der Zusammenfassung auch eingewendet, C2PA sei nie dafür gedacht gewesen, eine auf einen Bildschirm gerichtete Kamera zu erkennen [4]. Welche Modelle betroffen sind, nennt die Quelle nicht, ich habe die Originalarbeit nicht geprüft [4].

Wussten Sie schon ...?

... dass die EU-Transparenzpflichten nach Artikel 50 der KI-Verordnung laut TrueScreen seit 2. August 2026 gelten, mit Übergangsfrist bis 2. Dezember 2026 für schon am Markt befindliche Systeme [3]?

... dass eine C2PA-Signatur laut TrueScreen keine qualifizierte elektronische Signatur nach eIDAS ist und deshalb nur der freien Beweiswürdigung des Gerichts dient [3]?

... dass nach Born City wenige Sekunden Audio reichen, um eine Stimme zu klonen [2]?

... dass SynthID laut Börse Express automatisch greift, wenn Werkzeuge wie Imagen oder der Magic Editor in Google Fotos Inhalte erzeugen oder bearbeiten [1]?

Was Sie sich abschauen können: Fotos prüfen wie ein Profi

Ob ein Bild echt ist, entscheidet selten ein einzelnes Merkmal. Fragen Sie: Woher stammt es? Gibt es das Bild an anderer Stelle früher? Passt es zu Ort und Zeit? Wer verbreitet es? Fehlen Credentials, heißt das nicht, dass das Bild falsch ist, und vorhandene belegen nur den Verlauf. Wer in Verein oder Betrieb Bilder veröffentlicht, kann eine kurze Regel aufschreiben: Eigene Fotos mit Datum und Quelle ablegen, bearbeitete Bilder kennzeichnen, bei KI-Bildern die Herkunft nennen. Glieks kann eine solche Bildregel als Dokument, eine Prüfcheckliste und eine Bilder-Ablageliste vorbereiten. Echtheitsprüfungen von Fotos nimmt Glieks nicht vor.

> **Merken Sie sich:** Content Credentials dokumentieren den Verlauf eines Bildes, nicht seine Wahrheit [3] - ein fehlendes Etikett beweist ebenso wenig [2].

Was Glieks für Ihre Bildregeln tun kann

- **Bildregel für den Verein** - Ein einseitiges Dokument zum Umgang mit Fotos und KI-Bildern.
- **Checkliste für fragliche Bilder** - Eine Checkliste mit Fragen zur Herkunft.
- **Bilder-Ablageliste** - Eine Tabelle mit Quelle, Datum, Rechten und Bearbeitung.

- **Meldung zusammenfassen** - Stichpunkte mit Angabe, wer was behauptet.

Direkt ausprobieren: https://glieks.ai/glieks-news/echtes-foto-pixel-10-c2pa

Quellen

1. Börse Express: Pixel 10: Google startet Kampf gegen KI-Fälschungen (Stand: 26.09.2025, abgerufen am 18.11.2026)
2. Born City: Deepfakes: Warum Smartphone-Kennzeichnung nicht ausreicht (Stand: 31.01.2026, abgerufen am 18.11.2026)
3. TrueScreen (Anbieter von Zertifizierungsdiensten): C2PA: Funktionsweise, Verbreitung und strukturelle Grenzen (Stand: 2026-08-19 (aktualisiert 2026-11-09), abgerufen am 18.11.2026)
4. Zeli (deutsche Zusammenfassung): C2PA-Kameras scheitern an der Realität: Android-Sicherheit ist gebrochen (Stand: 25.08.2026, abgerufen am 18.11.2026)

Diesen Beitrag online lesen: https://glieks.ai/glieks-news/echtes-foto-pixel-10-c2pa

Angaben ohne Gewähr. Die Glieks-News fassen öffentlich zugängliche Quellen in eigenen Worten zusammen. Keine Rechts-, Steuer- oder Anlageberatung - maßgeblich sind die verlinkten Quellen. Dieser Beitrag entstand mit KI-Unterstützung auf Grundlage der genannten Quellen.