

C2PA: STORIES OF TRUST & TRADEOFFS

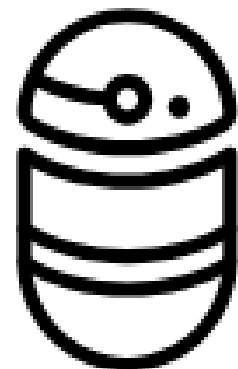
Kate Kaye, World Privacy Forum
Kate@WorldPrivacyForum.org



C2PA...



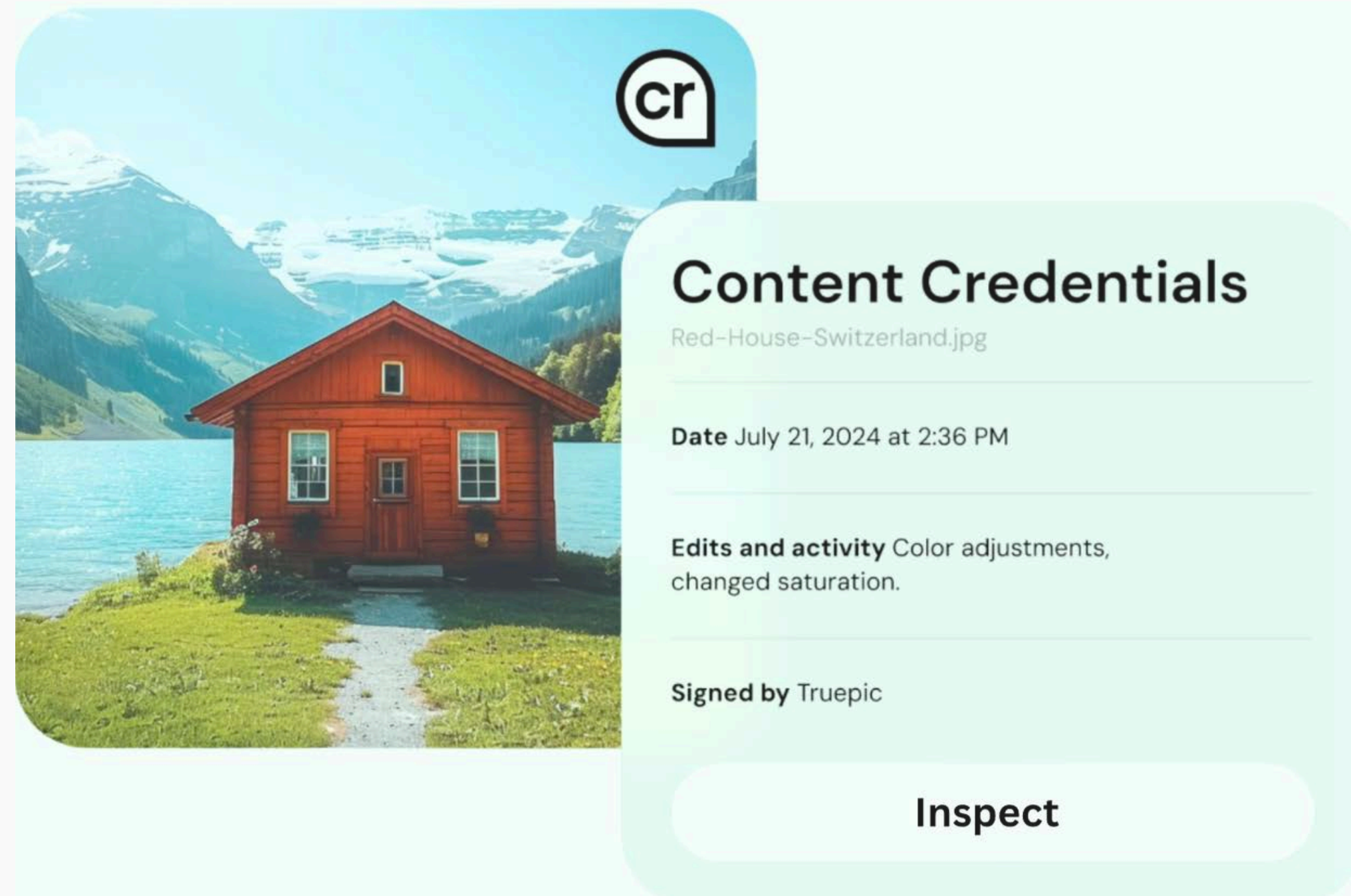
content credentials



**C2
PA**

**Coalition for
Content Provenance
and Authenticity**

MORE THAN “NUTRITION LABELS” FOR HUMANS TO READ



Our team is really excited about C2PA.

September 1, 2025



9/1/25, 10:30 AM

Hi everyone! Our team is really excited about C2PA. It aligns directly with what we're building, and we'd love to get more involved.

To start, we're particularly interested in how we can contribute to the iOS platform SDK. If someone could point me toward the best way to get involved there, that would be amazing.

We're also hoping to better understand what's required to submit a request to be added to the anchors list, and what that process looks like.

Looking forward to learning more and contributing where we can!



3



(and honestly a little alarming).

@ [redacted] Hello. Any idea why I might be seeing that my CC are broken on my website? Does this have something to do with any updates, certificate changes etc? Here is what I see. Thanks 📷

[redacted] 1/25, 7:41 PM

It's not just you. Pictures signed in 2021, 2022 cannot be validated. I even have some examples from 2025 that use the 2.2 version of the spec that are no longer verifiable.

[redacted] 12/11/25, 8:28 PM

Thanks that's helpful (and honestly a little alarming). Since this isn't uncommon and you've seen it before:

1. In your experience, what's the most typical root cause when untouched local originals suddenly fail verification / verifier regression, cert chain/trust store changes, missing timestamping, or something else?
2. Practically, what do you recommend creators/publishers do when this happens?
 - Re-sign and redistribute new assets?
 - Wait for verifier fixes / trust store updates?
 - From a user trust standpoint, "Invalid / may have been tampered with" reads like not authentic. Is there guidance on how verifiers should message trust-chain / cert issues vs actual content modification? Right now it looks indistinguishable.

- From a user trust standpoint, "Invalid / may have been tampered with" reads like not authentic.



Content summary

ⓘ This image was generated by an AI tool.

Process

The app or device used to generate this content recorded the following information:

App or device used

OpenAI-API

AI tool used

✖ DALL-E

Actions

- Converted asset
The format of the asset was changed
- Created
Created a new file or content



ANYONE CAN BUILD WITH C2PA.

WHAT C2PA DOES



WHAT'S IN C2PA METADATA?

```
"exif:GPSLatitude": "39,21.102N",  
"exif:GPSLongitude": "74,26.5737W",  
"exif:GPSAltitudeRef": 0,  
"exif:GPSAltitude": "100963/29890",  
"exif:GPSTimeStamp": "18:22:57",  
"exif:GPSDateStamp": "2019:09:22",
```

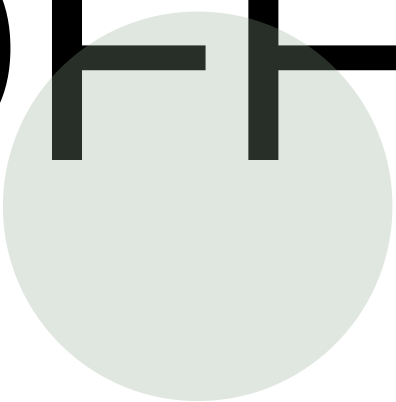
```
"action": "c2pa.created",  
"when": 0("2023-02-11T09:00:00Z"),  
"softwareAgent" : {  
  "name": "Joe's Photo Editor",  
  "version": "2.0",  
  "operating_system": "Windows 10"
```

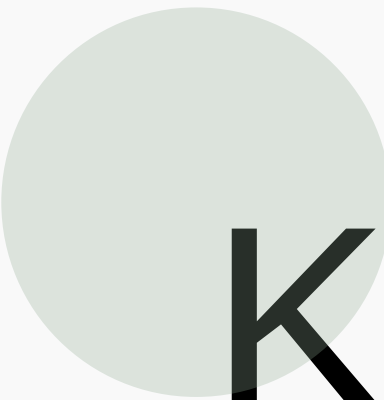


WHO CAN ACCESS C2PA METADATA?

(A DRM STARTUP STORY)

IP PRIVACY TRADEOFFS

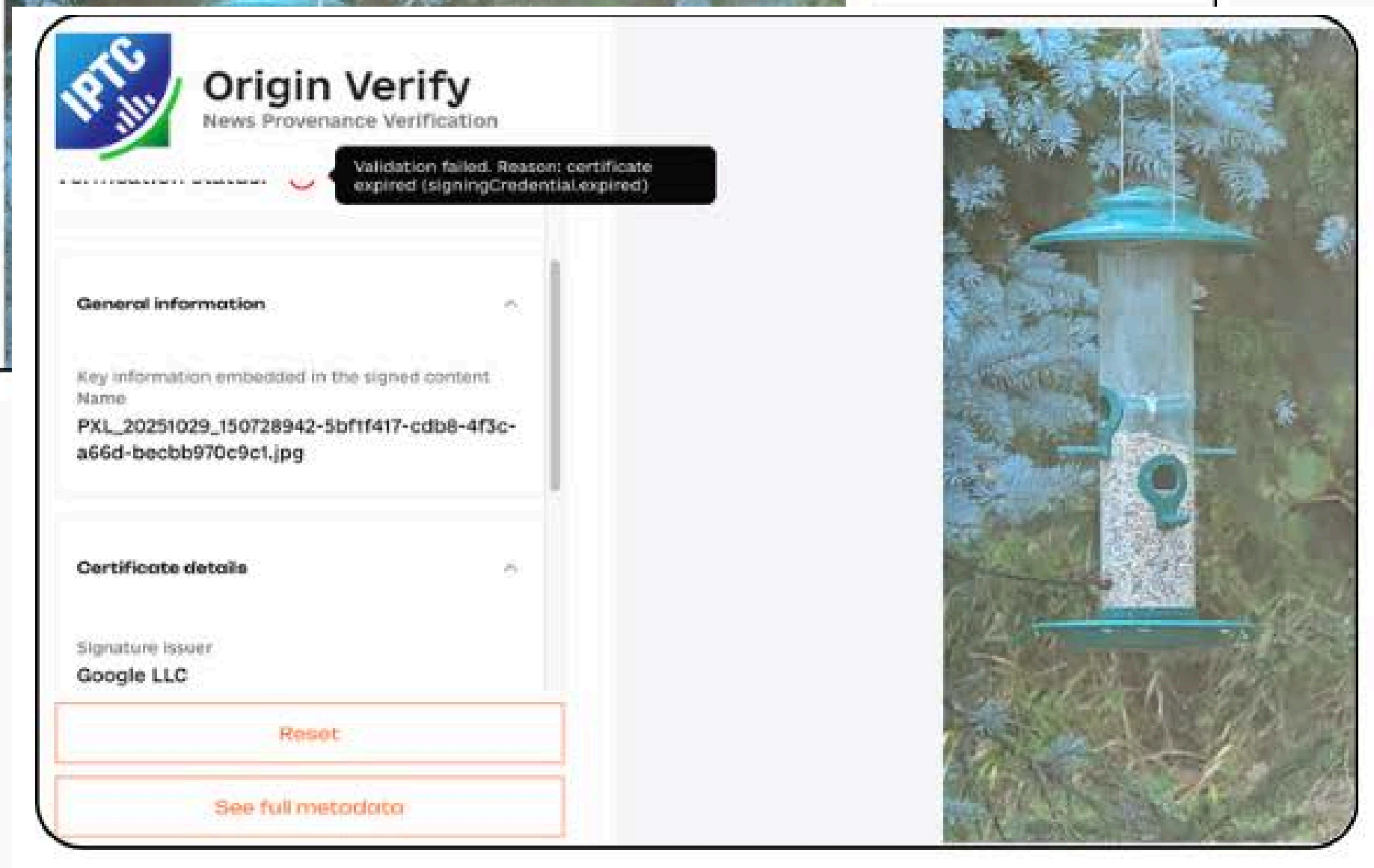
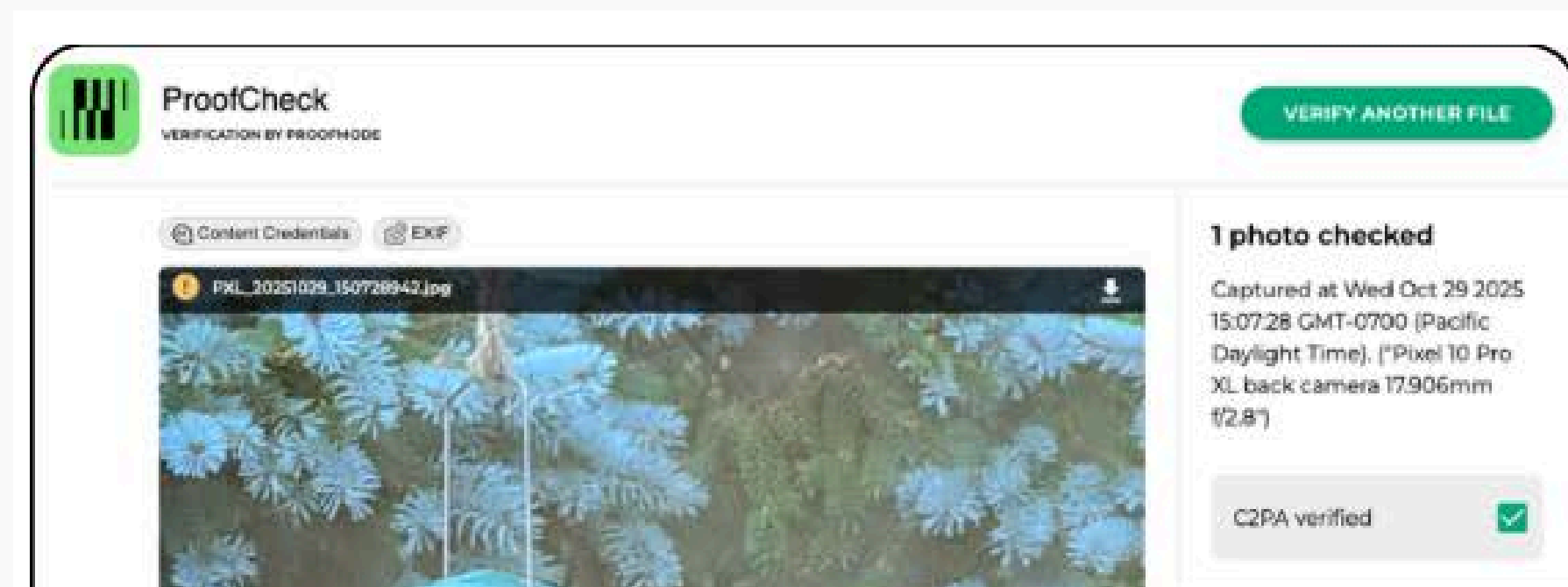




1-2-3 THINGS TO KNOW ABOUT C2PA

1. NO AI DETECTION
2. WIDE DATA ACCESS
3. NO FACT-CHECK FOR *TRUTHINESS*

THE MANY VERSIONS OF C2PA



VALID
OR
NOT?

WHO
CONTROLS
C2PA
DECISIONS?





THE C2PA TRUST PROCESS

NO C2PA METADATA?

Asset Journey

Untrusted edit



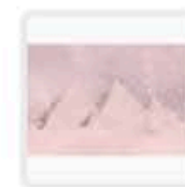
Something unknown or untrusted happened to the manifest

Capture/Create



Image had been created/captured using a C2PA-compliant software

User Experience



Invalid

Call out invalid C2PA data

View more

Image of invalid data from captured February 11, 2026 from C2PA User Experience Guidance for Implementers 2.0

a little alarming).

- From a user trust standpoint

“Invalid / may have been tampered with”

reads like not authentic.



WHAT ARE YOUR C2PA TRADEOFFS?

GET OUR IN-DEPTH REPORT AND PODCAST

WorldPrivacyForum.org

C2PA
REPORT



C2PA
EXPLAINER
PODCAST

