An Introduction to the Content Authenticity Initiative

IPTC Photo Metadata Conference 2020

Andy Parsons, Adobe
WHAT I’LL COVER TODAY

• What is the Content Authenticity Initiative?
• How it Works
• CAI Technology
• Where We Are Now
• What’s Next
What is the CAI?
“Falsehood flies, and the truth comes limping after it.”

Jonathan Swift, d. 1745
The mission of the CAI is to develop the industry standard for verifiable content attribution. By augmenting subjective judgments about authenticity with objective facts about how a piece of content came to be, the CAI aims to help content consumers make more informed decisions about what to trust.
Shared View of Facts and Truth

A few decades ago, we got information from fixed print and trusted sources. Now all media is digital, therefore all media is suspect.
Our Current Situation

• Advances in Technology
• Proliferation of Content
• Speed of Dissemination
• Content intended to Deceive
• Lack of Transparency
EDUCATION
DETECTION
ATTRIBUTION
Detection

Detection is a long-term challenge because it leads to an arms race.

The Deepfake Detection Challenge has gotten to an 65% accuracy rate which falls well short of needs.
Attribution is the who, the what, and the how
OUR GOAL

Setting the industry standard for digital content attribution
In May 2019, Nancy Pelosi was “Cheapfaked” into appearing drunk and slurring her words – Facebook refused to take down the video. Regulators felt pressure as debate raged as to what responsibility tech played in viral misinformation with a focus on synthetic media.
How it Works
Creator’s view in Photoshop
A view on social media
CAI DESIGN GOALS

- Create only the minimum required novel technology
- Do not require cloud storage (of assertions, claims or assets), but allow for it
- Allow flexibility in the nature of information stored (i.e. assertions of various types)
- Both claims and assertions must be able to be consistently hashed
- Allow for multiple assertions of the same type
- Allow for assertions to be redacted by subsequent claims
- Maintain a trail of claims across multiple tools, from creation through modification, publication, distribution
- Support all standard asset formats including images, video, audio, and documents
CORE TECHNOLOGIES

- JSON
- eXtensible Metadata Platform (XMP)
- Multihash
- HashLink
- JPEG universal metadata box format (JUMBF)
- Cryptographic Message Syntax (CMS)
- CMS Advanced Electronic Signatures (CAdES)
• Based on a simple structure for storing and accessing cryptographically verifiable metadata.

• This metadata comprises facts regarding asset creation, authorship, edit actions, capture device details, software used and many other subjects. Facts make up the provenance of a given asset.
**CLAIMS AND ASSERTIONS**

- Assertions represent distinct facts
- Claims wrap assertions into verifiable units
It is expected that each of the actors in the system that create, receive or process an asset will produce one or more assertions about what they did, when they did it, and (if possible) on behalf of whom.

- An assertion is labelled data
- Typically (though not required to be) in a JSON-based structure
- Certain assertions may be redacted by subsequent assertions, but they cannot be modified once made as part of a claim.
- The set of assertions for a given claim on an asset is called the assertion store
SOME DEFINED ASSERTIONS

- Identity
- Date of Claim
- Thumbnails
  - Acquisition
  - Claim
  - Ingredient
- Locations
  - Broad
  - Precise
- Camera Information
- Copyright
- Actions
- Cloud Data
- Ingredients
- XMP
- ClaimReview
• Gathers together all the assertions about an asset from an actor at a given time
• May also include one or more hashes of the asset itself
• May also a reference to the previous claim.
• It has all the same properties as an assertion including being assigned a label (cai.claim)
• May be either embedded into the asset or in the cloud.
• Cryptographically hashed and that hash is signed to produce the claim signature.
A CLAIM ILLUSTRATED

CAI Claim Block

CAI Store

CAI Assertion Store

cai.claim.thumbnail.jpg

cai.identity

cai.location.broad

cai.actions

CAI Claim

```json
{
  "recorder": "Photoshop",
  "signature": "self#jumbf=as_adbe_1",
  "assertions": [
    "self#jumbf=as_adbe_1/c ai.claim.thumbnail.jpg?hl=76142BD62363F",
    "self#jumbf=as_adbe_1/cai.identity?
    hl=459195dcDAFAF64Bd4A0",
    "self#jumbf=as_adbe_1/cai.location.broad?
    hl=1234567890",
    "self#jumbf=as_adbe_1/cai.actions?
    hl=ABCDEFEDCBA"
  ]
}
```

Claim Signature

Signed by: Adobe
Time: 2020-06-05T10:37:00-07:00
Hash: fa31...
PUTTING IT ALL TOGETHER

1. Create original asset
2. Create assertions (hashing each one), write assertion store back to file
3. Calculate one or more hashes over the asset data
4. Create claim data structure (JSON)
5. Sign the claim and store it in the CAI Data block
6. Store the signature URL (\rcai_claim) in the XMP
IS IPTC SUPPORTED?

- We already support some IPTC fields via standard XMP
- We welcome working with the IPTC to support additional fields
Where We Are
3 areas of focus:

- Standards Specifications
- Partner Prototypes
- Adobe Creative Cloud
What’s next?
Upcoming milestones

- Photoshop Beta
- Partner Prototypes (to be announced)
- Expanding set of collaborators
A true CAI consortium.

- Clear charter
- Founding activities currently underway
- An open membership model
- 4-6 working groups (to start)
Join us!

- Restoring trust requires ongoing engagement of diverse communities
- Upcoming announcements on how to participate
- We regard the IPTC as a key stakeholder
Thank you!

HTTPS://CONTENTAUTHENTICITY.ORG

@CONTENTAUTH

@ANDYPARSONS

ANDYP@ADOBE.COM