IPTC and Media Provenance

W3C Authentic Web workshop

6 May 2025

IPTC: Providing the technical foundation for the media ecosystem

accessintelligence
Adobe
AFP
AP
APA
BBC NEWS
Bloomberg
DATAGROUP
dpa
DW Deutsche Welle
EBU
gettyimages
glide PUBLISHING PLATFORM
Google
KEYSTONE SDA
LSEG DATA & ANALYTICS
The New York Times
PLUS PICTURE LICENSING UNIVERSAL SYSTEM
pa media group
QNA
REUTERS®
VCG
XINHUA

IPTC's Voting Members
(we also have over 50 Associate, Startup and Individual members)

- The IPTC is an open, non-partisan, non-political organisation dedicated to promoting interoperable standards and best practices in the news and media industries
- We are a registered non-profit organisation funded by member subscriptions
- Founded in the UK in 1965
- Members from 22 countries

What does the IPTC do?

Standards

We create and maintain some of the key technical standards used by the news and media industries

Events

We run member meetings/conferences twice a year, plus the Photo Metadata Conference, webinars and special events

Tools

We create software tools, libraries and online services that enable organisations to get the most out of our standards

Partnerships and advocacy

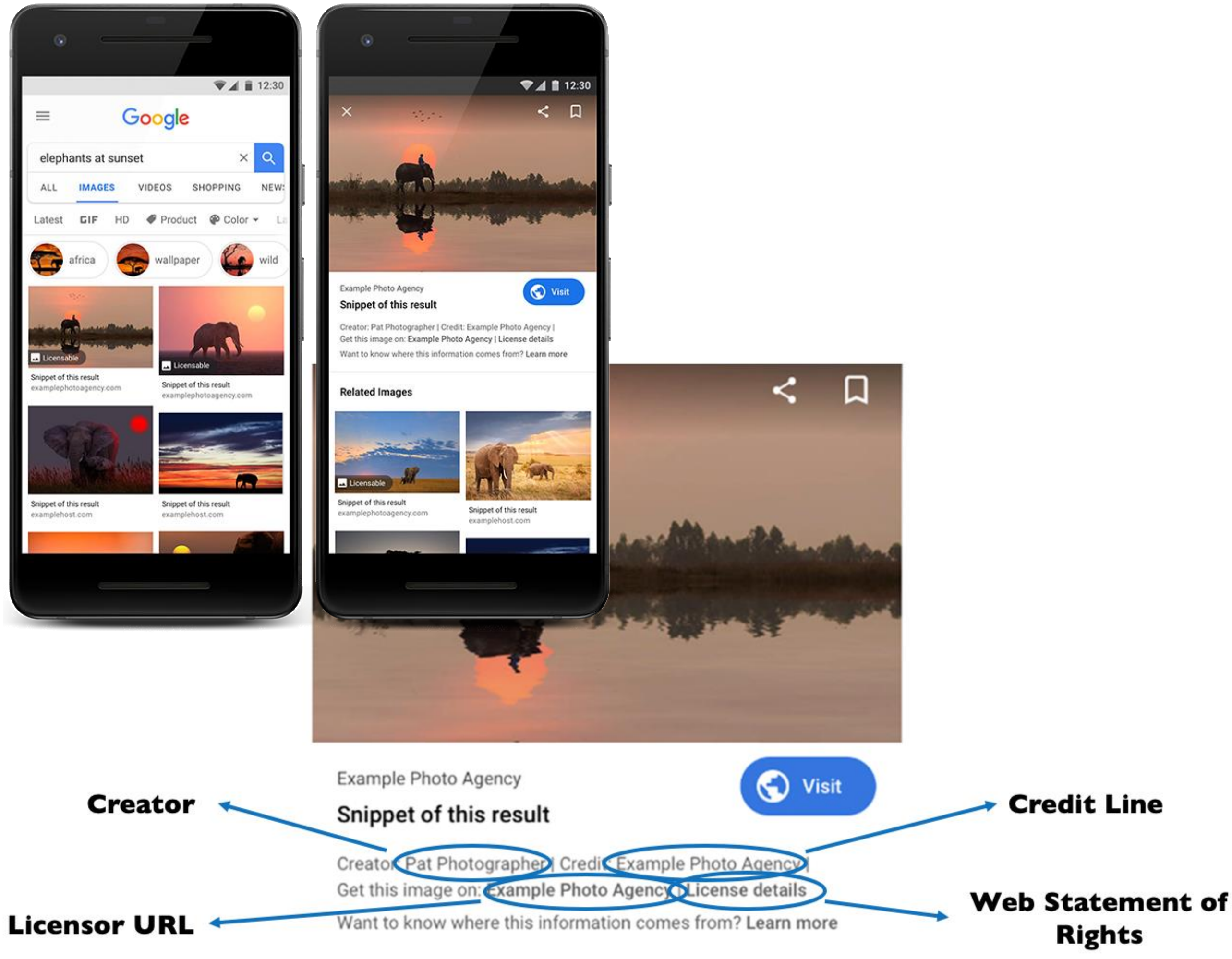
We work with third parties such as Google, Adobe, W3C, ISO, schema.org to promote the needs of our industry

Knowledge sharing and collaboration

We act as a forum for members to collaborate and share experiences

Why is the IPTC taking this on?

- We have a strong history in photo/video metadata, especially for the news industry
- Our IPTC Photo Metadata standard is supported by major platforms, hardware and software makers
- Our properties are used to signal generative AI content from all major AI engines
- We see provenance as the next step in our work to manage and protect metadata for content owners



Example Photo Agency

Snippet of this result

Creator: Pat Photographer | Credit: Example Photo Agency |
Get this image on: Example Photo Agency | License details
Want to know where this information comes from? Learn more

Creator

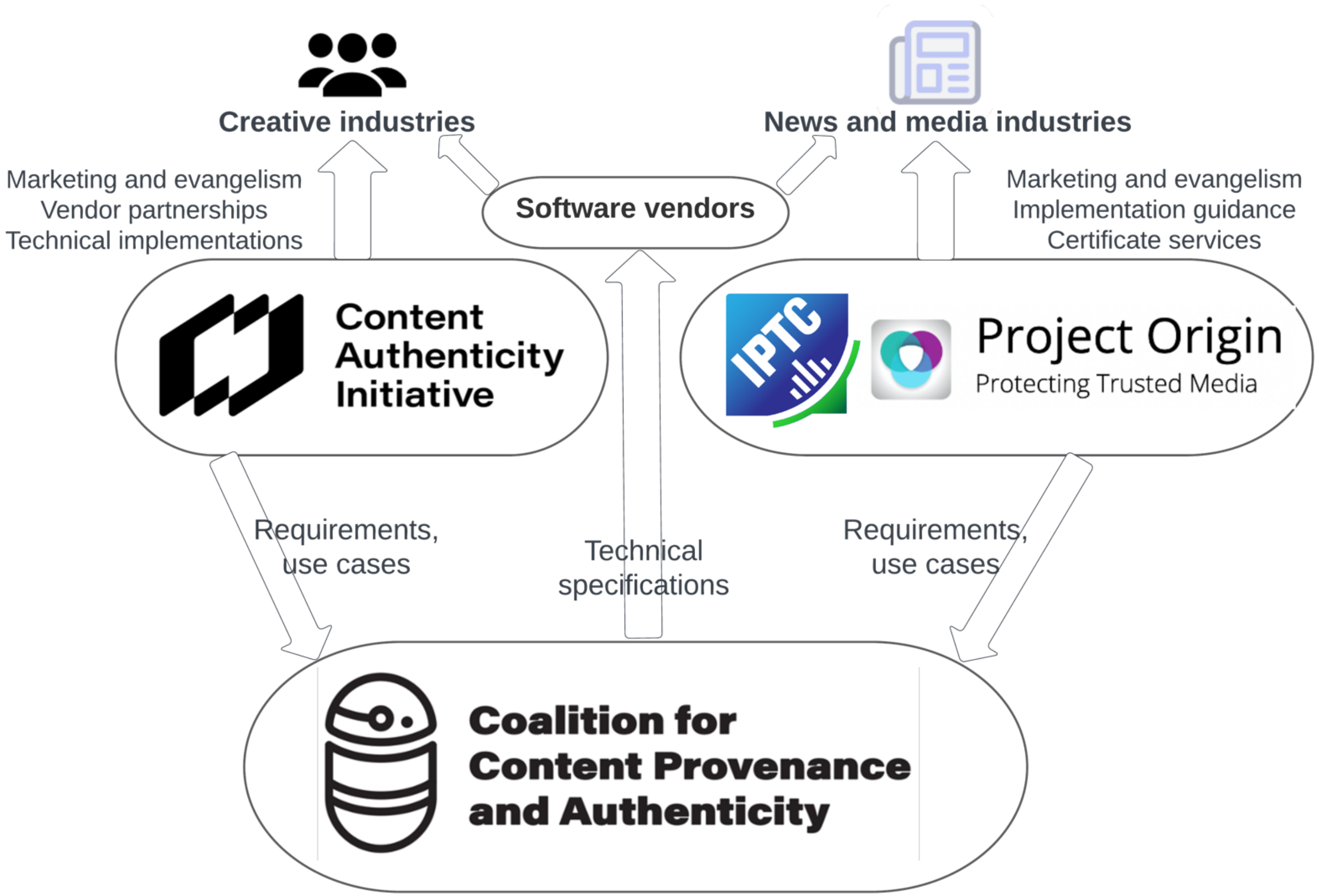
Credit Line

Licensor URL

Web Statement of Rights

C2PA, CAI, Project Origin, IPTC:
How does it all fit together?

- Project Origin + Content Authenticity Initiative (CAI) joined together to create C2PA in 2021
- Project Origin was simply a collaboration agreement between a small number of companies: it had no structure to scale
- So the IPTC “adopted” Project Origin: its work now continues as the IPTC Media Provenance Committee



Definitions

- Our approach to “credibility”:
  - Ensuring that consumers / readers understand ***who published*** a piece of content
  - Note that ***we do not make any claims as to whether signed content is “true” or “factual”*** – we’re simply surfacing who published the content
- Use cases:
  - ”Miscontextualised” image/video published on social media. Users/platforms can surface the original context of the media to help users understand that someone is attempting to manipulate them
  - Publisher can add additional metadata to describe verification work performed, associated links

Three C2PA Workflows

1. Ideal C2PA workflow: “glass-to-glass”
   - Camera -> newsroom workflow systems -> publishing tools -> distribution platforms
   - C2PA manifests used and maintained at each step of the process
   - This is the eventual goal, but requires all publisher tools to be upgraded
2. Stamping workflow: “We published this”
   - Use existing newsroom systems, add a publisher C2PA signature as the last step before publishing
   - Publisher can add metadata signalling that they created/published/endorse the content
   - Avoids potential issues around redaction. Simplest way to get started today.
3. C2PA in, C2PA out – black box in between
   - Read C2PA manifests on ingest to help to verify content sources. Remove all C2PA metadata for processing through internal systems.
   - Add a publisher signature at publish time (same as “we published this” workflow)

Three C2PA Workflows

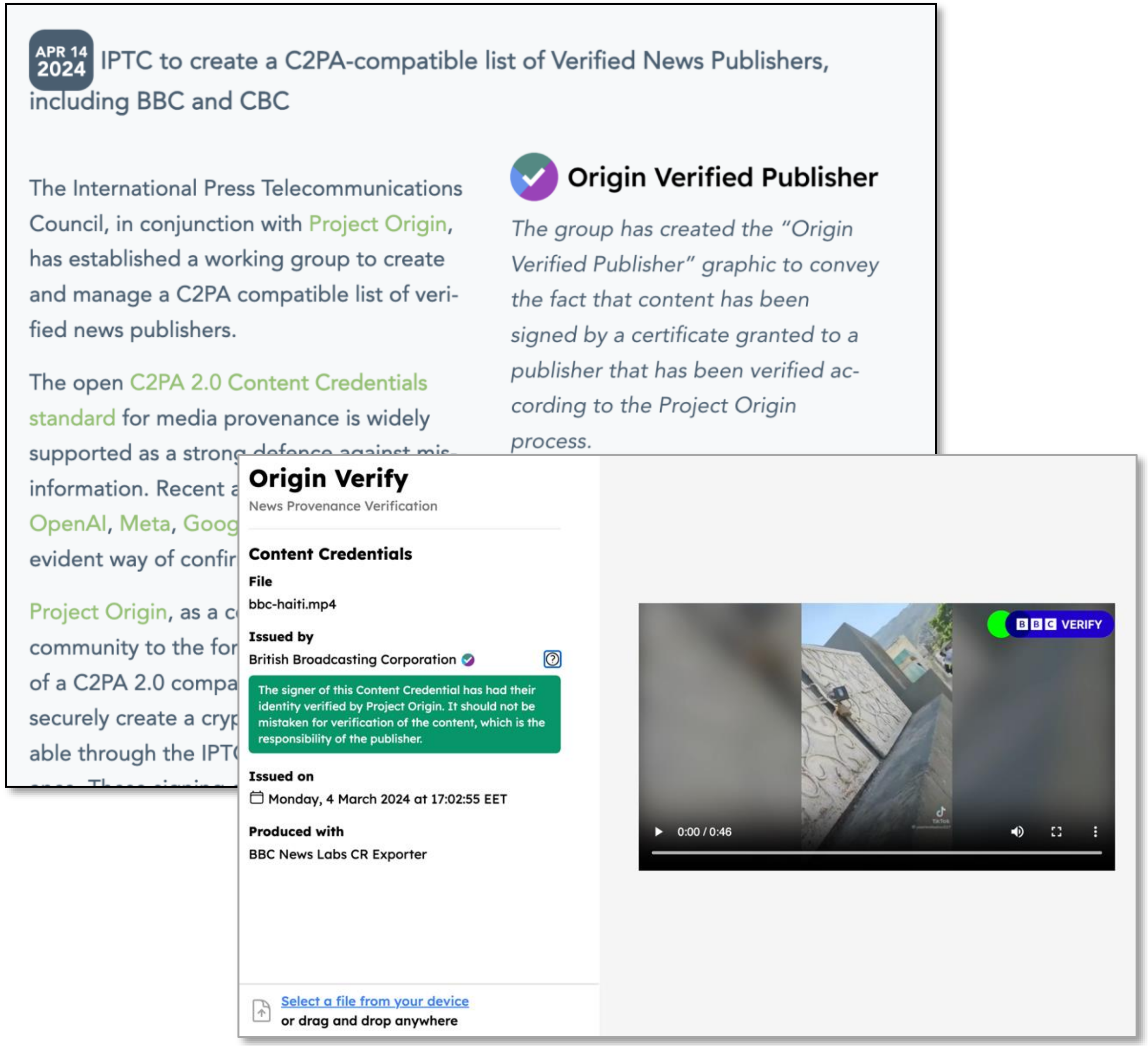
1. Ideal C2PA workflow: “glass-to-glass”
   - Camera -> newsroom workflow systems -> publishing tools -> distribution platforms
   - C2PA manifests used and maintained at each step of the process
   - This is the eventual goal, but requires all publisher tools to be upgraded

2. Stamping workflow: “We published this”
   - Use existing newsroom systems, add a publisher C2PA signature as the last step before publishing
   - Publisher can add metadata signalling that they created/published/endorse the content
   - Avoids potential issues around redaction. Simplest way to get started today.

3. C2PA in, C2PA out – black box in between
   - Read C2PA manifests on ingest to help to verify content sources. Remove all C2PA metadata for processing through internal systems.
   - Add a publisher signature at publish time (same as “we published this” workflow)

IPTC Origin Verified News Publisher List

- We created an IPTC-hosted “Trust List” of “Verified News Publisher” certificates
  - We verify that organisations are genuine news publishers before putting certificates on the list
- We help news organisations to obtain certificates and learn how to sign their content
- We have created a set of certificate and signing tools and have launched a validator at https://originverify.iptc.org/
- One of the main tasks of the Committee is to work out how this will scale to a large number of media publishers



APR 14 2024 IPTC to create a C2PA-compatible list of Verified News Publishers, including BBC and CBC

The International Press Telecommunications Council, in conjunction with Project Origin, has established a working group to create and manage a C2PA compatible list of verified news publishers.

The open C2PA 2.0 Content Credentials standard for media provenance is widely supported as a strong defence against mis-
information. Recent a
OpenAI, Meta, Goog
evident way of confir

Project Origin, as a c
community to the for
of a C2PA 2.0 compa
securely create a cryp
able through the IPTC

Origin Verified Publisher

The group has created the “Origin Verified Publisher” graphic to convey the fact that content has been signed by a certificate granted to a publisher that has been verified according to the Project Origin process.

Origin Verify

News Provenance Verification

Content Credentials

File

bbc-haiti.mp4

Issued by

British Broadcasting Corporation ✓ ⓘ

The signer of this Content Credential has had their identity verified by Project Origin. It should not be mistaken for verification of the content, which is the responsibility of the publisher.

Issued on

Monday, 4 March 2024 at 17:02:55 EET

Produced with

BBC News Labs CR Exporter

Select a file from your device
or drag and drop anywhere

IPTC Origin Verified News Publisher List: Roadmap

- Phase 0 (early 2024)
  - Proof of concept
  - Only BBC, CBC certificates on our list
- Phase 1 (Sep 2024 – mid-2025)
  - Exploratory stage – 15+ news organisations in various stages of onboarding
  - “end-entity” certificates on our list – aiming for 20-30 publishers by mid-2025
  - High-touch verification process: “Friends and family” news orgs
- Phase 2 (late 2025 onwards)
  - Make the system more scalable
  - Partner with Certificate Authorities – we put their “intermediate certificates” on our list – similar to the way web browsers handle HTTPS certificates
  - Scalable verification processes currently being defined

Who is on the VNP list so far?

BBC NEWS

CBC Radio-Canada

francetélévisions

AFP

DW Deutsche Welle

IPTC

WDR

Around 10 more publishers are in the pipeline

Process to obtain a certificate and add it to the Verified News Publishers List (Phase 1 - today)

1. Obtain an organisational email-signing or document-signing certificate using a well-known Certificate Authority (we currently recommend the “PersonalSign2 Department” certificate from GlobalSign, about €200-300)
   - The CA has a vetting process which verifies that the request comes from the named organisation
   - GlobalSign currently offer CSR-based certificates (host keys in Hardware Secure Module) or PKCS#12 secure keys (publishers must protect their private key themselves)
2. Sign some test content using your private key and certificate
3. Fill in a short form on iptc.org. Send the certificate and test content to IPTC.
4. IPTC checks the certificate and test content, verifies that you are a news publisher (currently a simple process) and uploads the cert to the VNP list
5. Sign and publish your content. (The certificate is embedded in all signed content, along with publisher metadata assertions)
6. When verified using a supporting validator, the tool loads the current VNP certificate list and checks for the presence of the certificate.

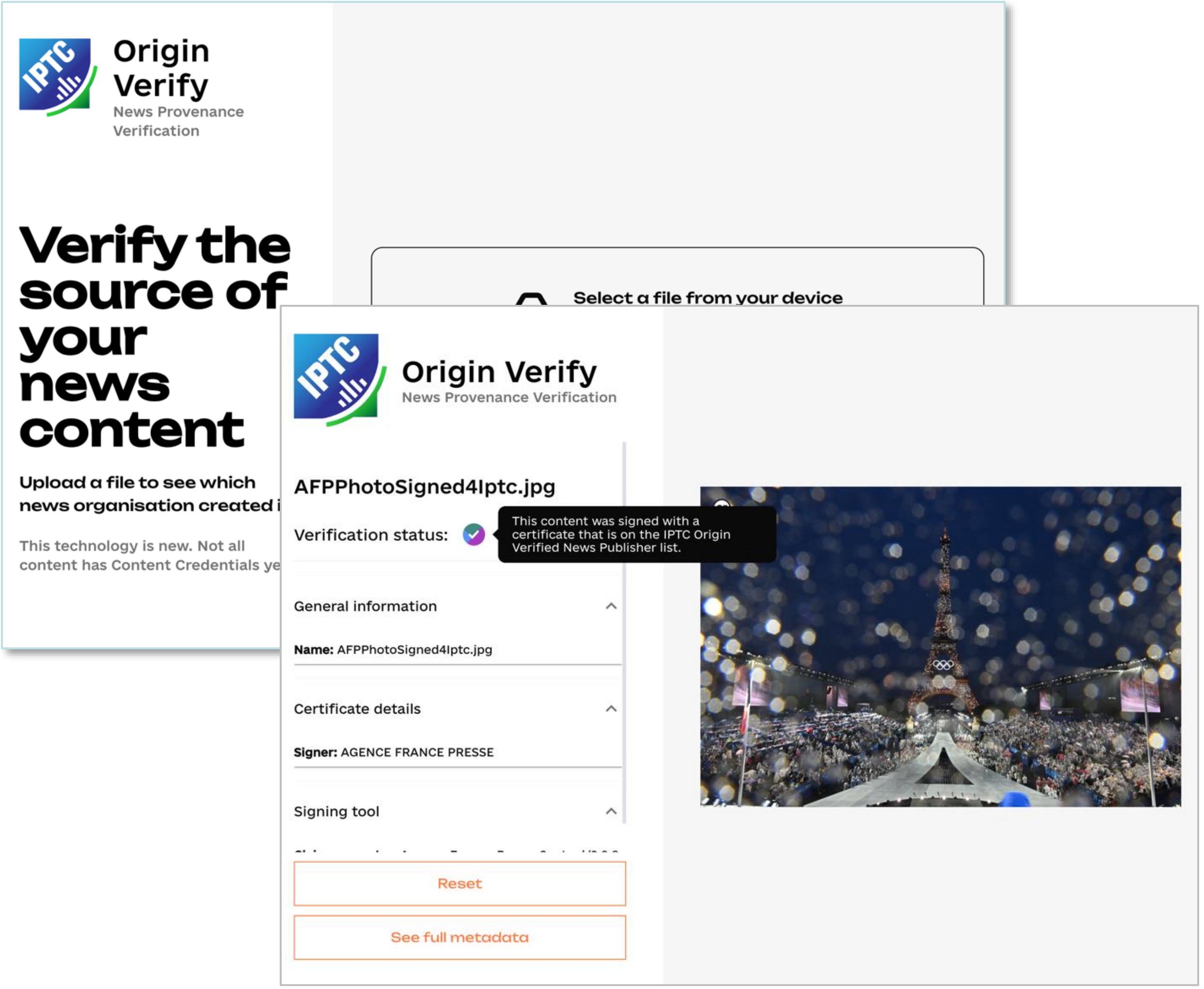
Process to obtain a certificate and add it to the Verified News Publishers List (Phase 2 – late 2025+)

1. Obtain a Verified News Publisher* certificate from a well-known Certificate Authority
   - The CA has a vetting process which verifies that the request comes from the named organisation
   - We would continue to support CSR-based certificates (host keys in Hardware Secure Module) or PKCS#12 secure keys (you must protect your private key yourself)
2. Sign your content using your private key and certificate
   - The certificate is embedded in all signed content
3. Sign and publish your content.
4. When verified using a supporting validator, the tool loads the current VNP certificate list and checks for the presence of the certificate.

** This would be a new type of x.509 certificate that doesn’t yet exist. It would be similar to the Web server certificate infrastructure whereby site owners buy a certificate directly from a CA, undergoing some vetting process. We are currently speaking with CAs to establish these systems and processes.*

Tools and services to support publishers: Origin Verify Validator

- We have created our own validator, **originverify.iptc.org**
- Shows whether content has been tampered since being signed
- Shows the owner of the certificate used to sign the content
- Shows some basic metadata: publisher, publish time, caption, alt text
- Works with images and video files



Origin Verify

News Provenance Verification

Verify the source of your news content

Upload a file to see which news organisation created i

This technology is new. Not all content has Content Credentials ye

Origin Verify

News Provenance Verification

AFPPhotoSigned4Iptc.jpg

Verification status: ✓

This content was signed with a certificate that is on the IPTC Origin Verified News Publisher list.

General information

Name: AFPPhotoSigned4Iptc.jpg

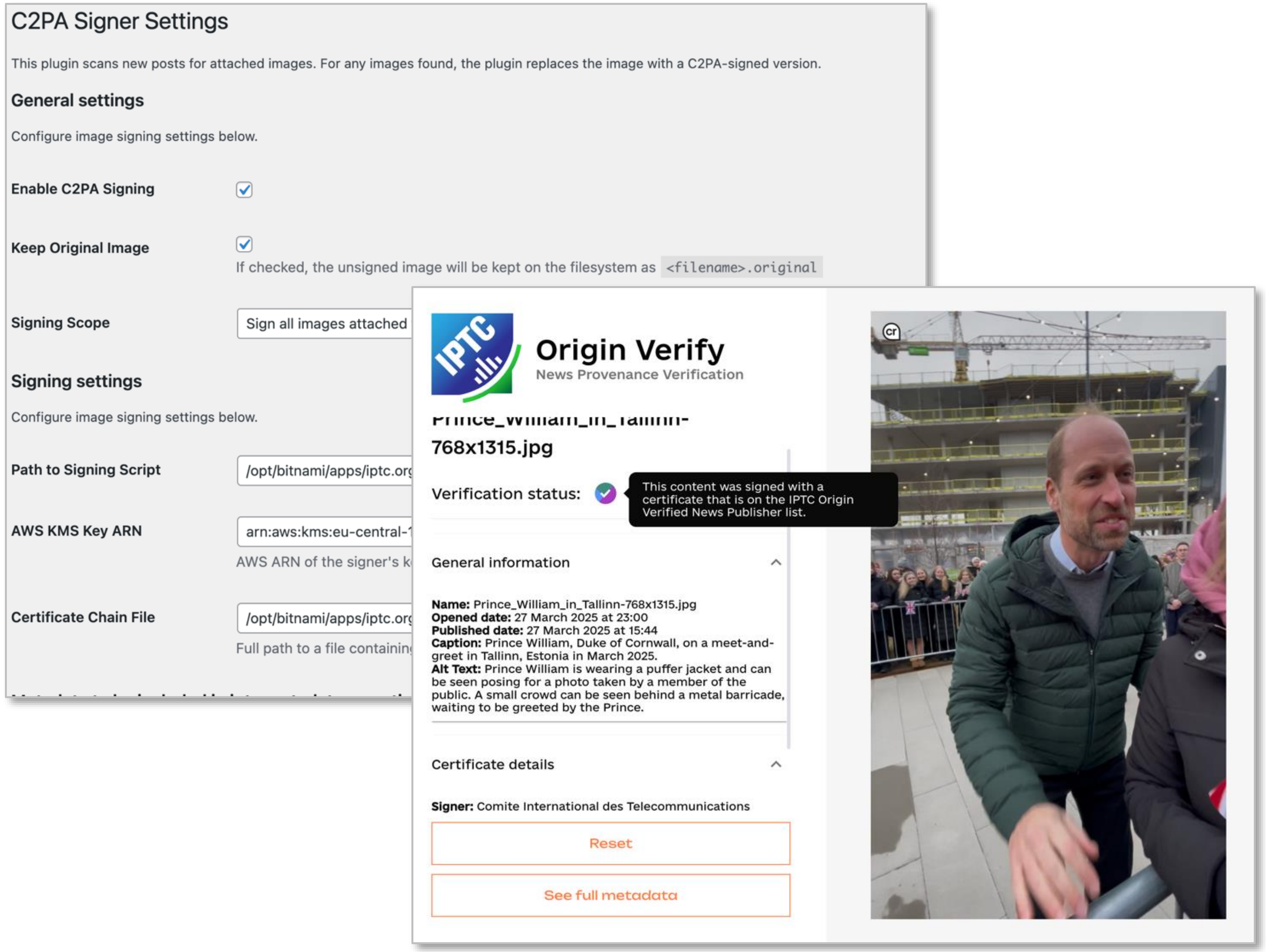
Certificate details

Signer: AGENCE FRANCE PRESSE

Signing tool

Tools and services to support publishers

- IPTC has created a set of tools to help publishers to obtain certificates, sign content, add publisher assertions
- We have created a Wordpress plugin that uses our signing tools to automatically sign every image published on every news post
- It also extracts caption, alt text and publish date from the Wordpress metadata and adds them to the assertions inside the signed manifest
  - Can be configured by options in the plugin settings
- We are now using this on iptc.org
  - We might be the first publisher to routinely sign all content that we publish!



C2PA Signer Settings

This plugin scans new posts for attached images. For any images found, the plugin replaces the image with a C2PA-signed version.

General settings

Configure image signing settings below.

Enable C2PA Signing ☑

Keep Original Image ☑
If checked, the unsigned image will be kept on the filesystem as `<filename>.original`

Signing Scope: Sign all images attached

Signing settings

Configure image signing settings below.

Path to Signing Script: /opt/bitnami/apps/iptc.org

AWS KMS Key ARN: arn:aws:kms:eu-central-1
AWS ARN of the signer's k

Certificate Chain File: /opt/bitnami/apps/iptc.org
Full path to a file containin

Origin Verify
News Provenance Verification

Prince_William_in_Tallinn-768x1315.jpg

Verification status: ✓
This content was signed with a certificate that is on the IPTC Origin Verified News Publisher list.

General information

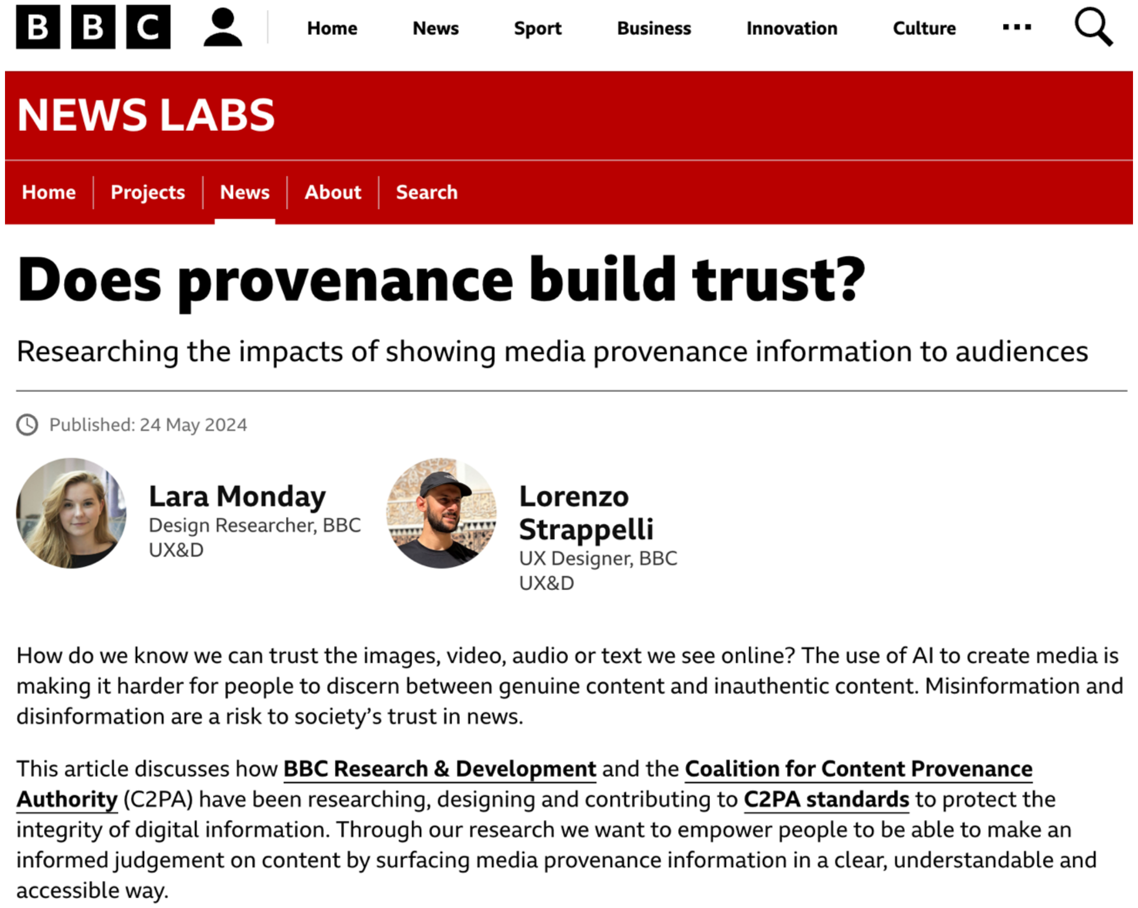
Name: Prince_William_in_Tallinn-768x1315.jpg
Opened date: 27 March 2025 at 23:00
Published date: 27 March 2025 at 15:44
Caption: Prince William, Duke of Cornwall, on a meet-and-greet in Tallinn, Estonia in March 2025.
Alt Text: Prince William is wearing a puffer jacket and can be seen posing for a photo taken by a member of the public. A small crowd can be seen behind a metal barricade, waiting to be greeted by the Prince.

Certificate details

Signer: Comite International des Telecommunications

Does it work?

- UX studies (BBC, CBC, forthcoming study from Project Reynir in Norway) show that users generally trust content more when “content credentials” are attached
- BBC: “we were encouraged by a self-selecting, limited audience trial of 1,200 people who answered three multiple choice questions. Their answers suggested that:
  - 83% trust the media more after seeing our Content Credentials
  - 96% found our Content Credentials useful
  - 96% of users say they found our Content Credentials informative”



Does provenance build trust?

Researching the impacts of showing media provenance information to audiences

Published: 24 May 2024

Lara Monday
Design Researcher, BBC UX&D

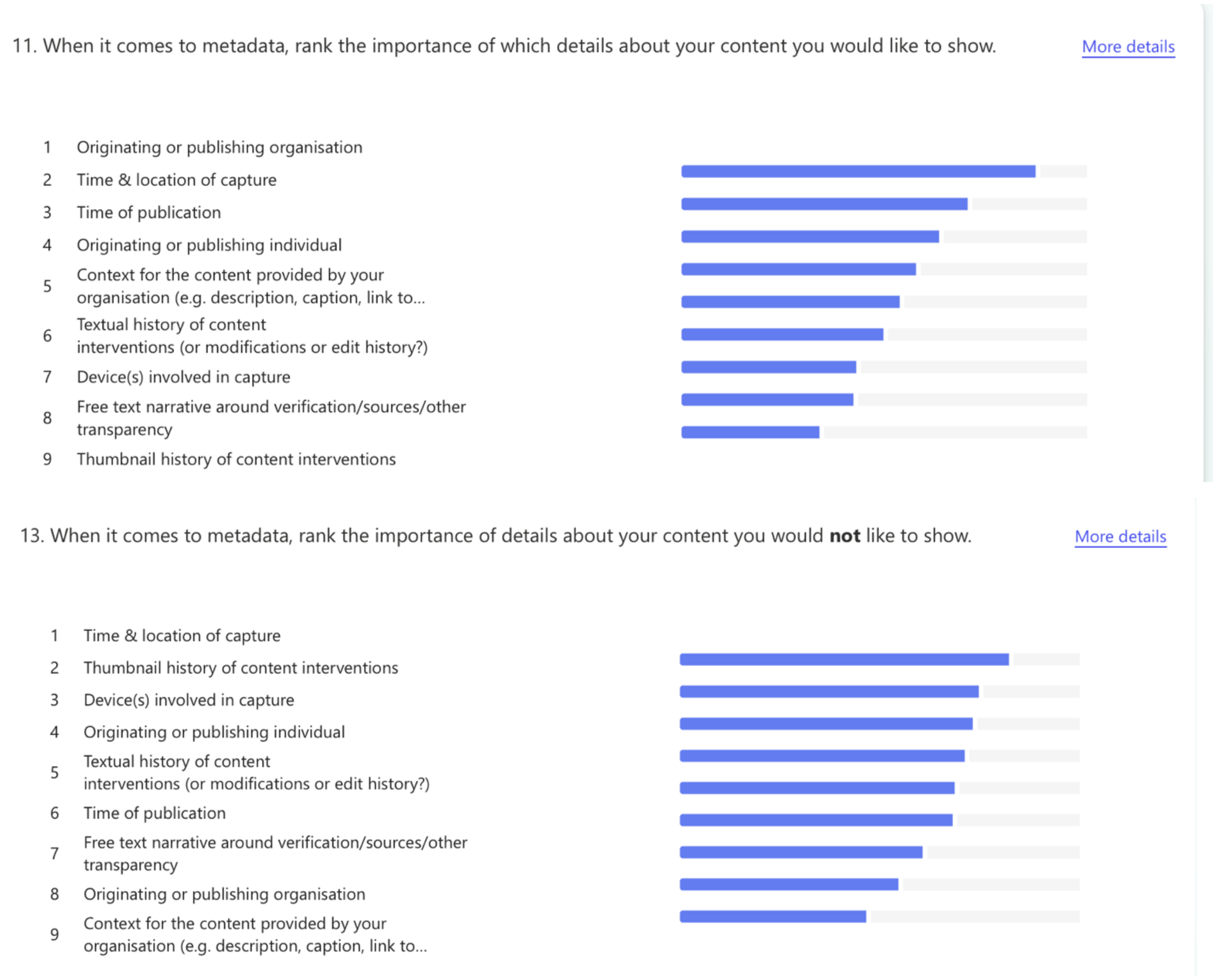
Lorenzo Strappelli
UX Designer, BBC UX&D

How do we know we can trust the images, video, audio or text we see online? The use of AI to create media is making it harder for people to discern between genuine content and inauthentic content. Misinformation and disinformation are a risk to society’s trust in news.

This article discusses how **BBC Research & Development** and the **Coalition for Content Provenance Authority** (C2PA) have been researching, designing and contributing to **C2PA standards** to protect the integrity of digital information. Through our research we want to empower people to be able to make an informed judgement on content by surfacing media provenance information in a clear, understandable and accessible way.

What are our next steps?

- Creating best-practice guidelines for how publisher metadata should be added to Verified News Publisher signed content
  - Juan les Pins in mid-May (IPTC Spring Meeting)
  - New York City in early June (CAI / IPTC Authenticity Summit)
  - Workshop in Norway in Sept
- Onboarding new publishers, evangelising our work
- Further work with the industry
- Plans to scale up our processes for Phase 2 of the VNP list



11. When it comes to metadata, rank the importance of which details about your content you would like to show. More details

1 Originating or publishing organisation
2 Time & location of capture
3 Time of publication
4 Originating or publishing individual
5 Context for the content provided by your organisation (e.g. description, caption, link to...
6 Textual history of content interventions (or modifications or edit history?)
7 Device(s) involved in capture
8 Free text narrative around verification/sources/other transparency
9 Thumbnail history of content interventions

13. When it comes to metadata, rank the importance of details about your content you would **not** like to show. More details

1 Time & location of capture
2 Thumbnail history of content interventions
3 Device(s) involved in capture
4 Originating or publishing individual
5 Textual history of content interventions (or modifications or edit history?)
6 Time of publication
7 Free text narrative around verification/sources/other transparency
8 Originating or publishing organisation
9 Context for the content provided by your organisation (e.g. description, caption, link to...

Results of a survey of publishers undertaken by the BBC in 2024

What do we ask from W3C?

- Recommendations for how we can work towards getting C2PA and our trust lists supported by the Web Platform
  - Ideal would be support in browsers – a la the HTTPS “padlock” in location bar
- Help us to work towards a standardised API that covers how C2PA signals can be exposed as part of the Web API
- Help in evangelising our work and the benefits of signing content

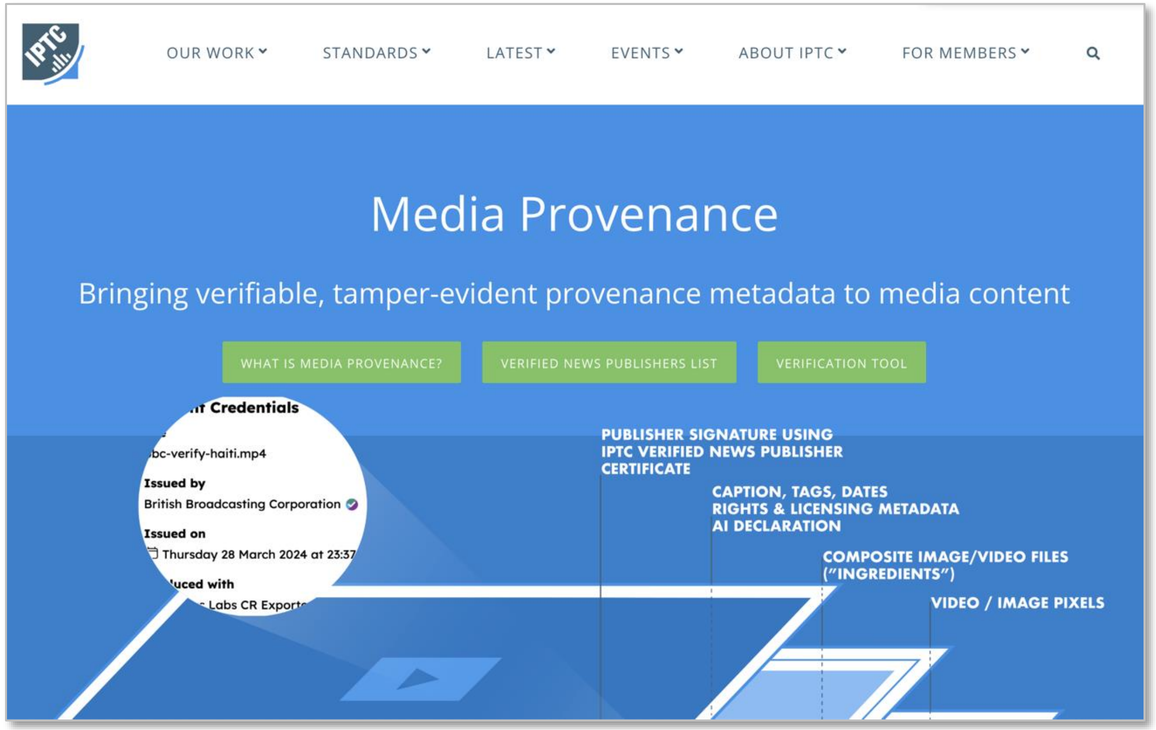
Contact us for more info

https://iptc.org/media-provenance/

https://iptc.org/verified-news-publishers-list/

https://iptc.org/about-iptc/contact-us/

Email Brendan Quinn: mdirector@iptc.org



Media Provenance

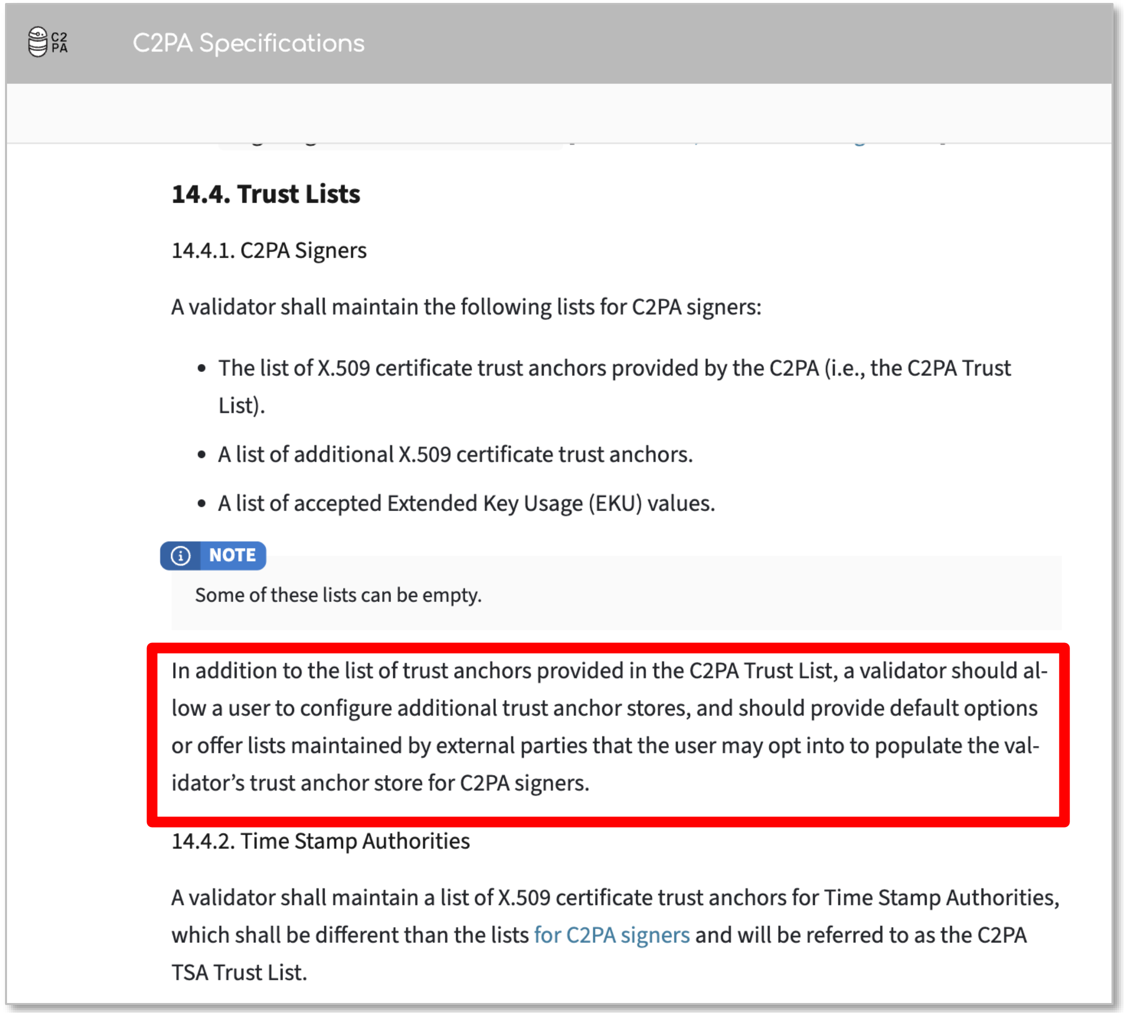
Bringing verifiable, tamper-evident provenance metadata to media content

OUR WORK
STANDARDS
LATEST
EVENTS
ABOUT IPTC
FOR MEMBERS
WHAT IS MEDIA PROVENANCE?
VERIFIED NEWS PUBLISHERS LIST
VERIFICATION TOOL
nt Credentials
bc-verify-haiti.mp4
Issued by
British Broadcasting Corporation
Issued on
Thursday 28 March 2024 at 23:37
luced with
Labs CR Export
PUBLISHER SIGNATURE USING IPTC VERIFIED NEWS PUBLISHER CERTIFICATE
CAPTION, TAGS, DATES RIGHTS & LICENSING METADATA AI DECLARATION
COMPOSITE IMAGE/VIDEO FILES ("INGREDIENTS")
VIDEO / IMAGE PIXELS

Appendices

IPTC Verified News Publisher List: Compatibile with C2PA 2.1 and beyond

- For version 2.0, C2PA made a change that removed the ability for an organisational certificate to be added to the “C2PA Trust List.” The intent is that the C2PA Trust List will contain certificates for hardware and software tools only.
- The IPTC Verified News Publishers List is an “additional trust list” according to the C2PA 2.2 spec.
- Our assertions and manifests are compliant with the 2.2 version of the specification



14.4. Trust Lists

14.4.1. C2PA Signers

A validator shall maintain the following lists for C2PA signers:

- The list of X.509 certificate trust anchors provided by the C2PA (i.e., the C2PA Trust List).
- A list of additional X.509 certificate trust anchors.
- A list of accepted Extended Key Usage (EKU) values.

NOTE

Some of these lists can be empty.

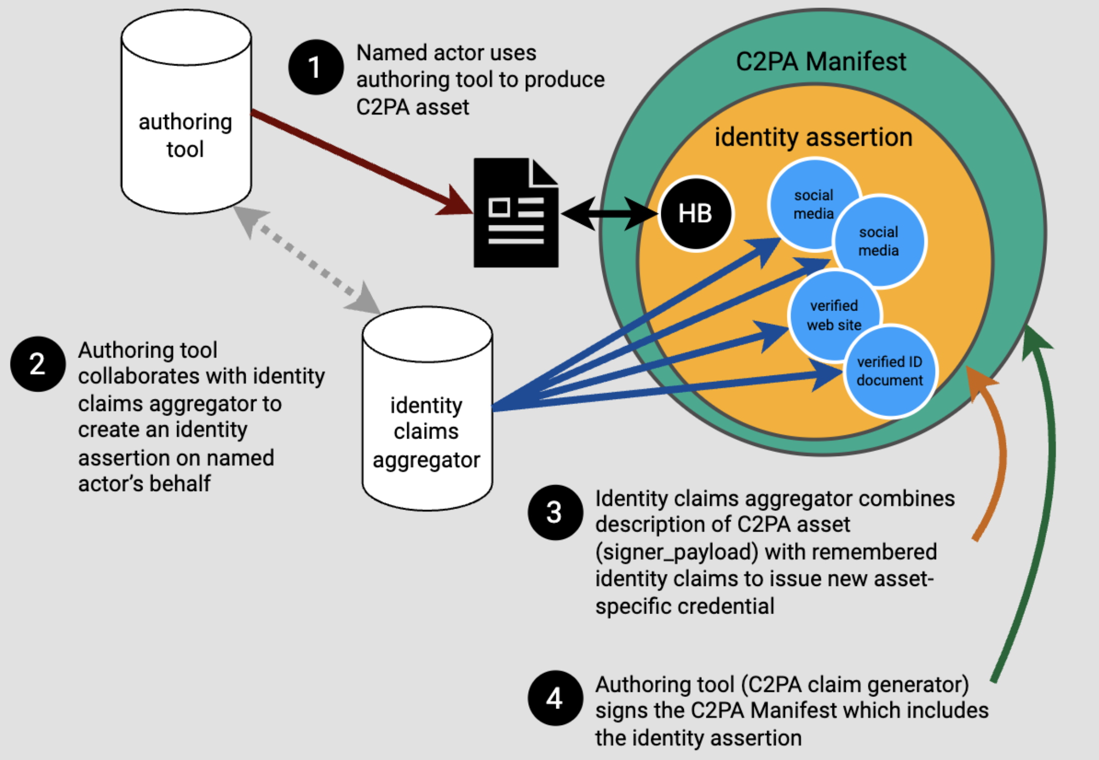
In addition to the list of trust anchors provided in the C2PA Trust List, a validator should allow a user to configure additional trust anchor stores, and should provide default options or offer lists maintained by external parties that the user may opt into to populate the validator’s trust anchor store for C2PA signers.

14.4.2. Time Stamp Authorities

A validator shall maintain a list of X.509 certificate trust anchors for Time Stamp Authorities, which shall be different than the lists for C2PA signers and will be referred to as the C2PA TSA Trust List.

Creator Assertions Working Group (CAWG) and Identity Assertions

- Because all means of identifying individuals and organisations were removed from the C2PA 2.0 spec, the spin-off group Creator Assertions Working Group (CAWG) was initiated to incubate the parts removed from the spec.
- Two CAWG projects interest us:
  - The **cawg.metadata** assertion for generic metadata properties (anything that can be expressed in JSON-LD, including IPTC, Exif, schema.org and more)
  - The **cawg.identity** assertion which allows named actors to sign some or all assertions in a C2PA manifest



1 Named actor uses authoring tool to produce C2PA asset

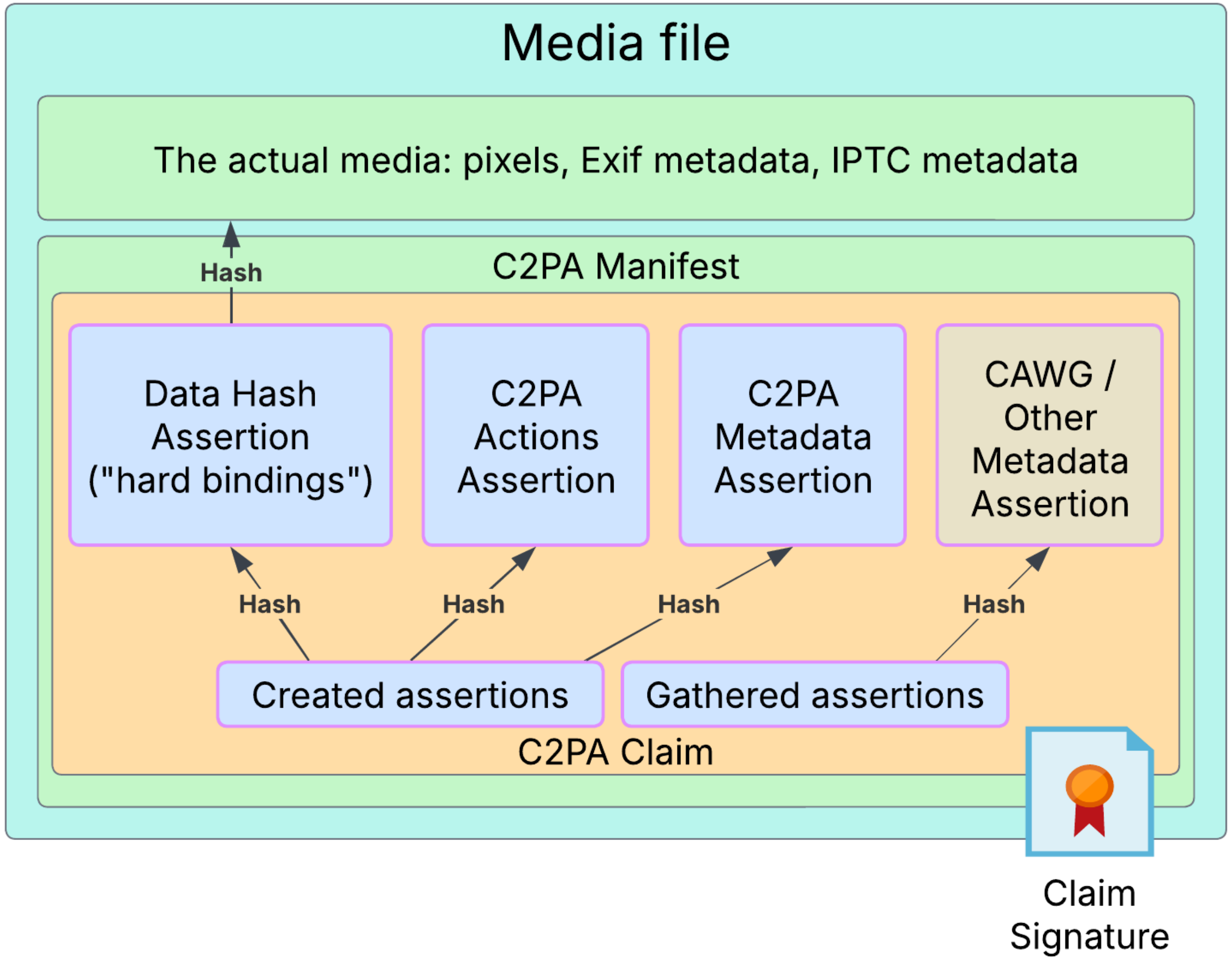
2 Authoring tool collaborates with identity claims aggregator to create an identity assertion on named actor's behalf

3 Identity claims aggregator combines description of C2PA asset (signer_payload) with remembered identity claims to issue new asset-specific credential

4 Authoring tool (C2PA claim generator) signs the C2PA Manifest which includes the identity assertion

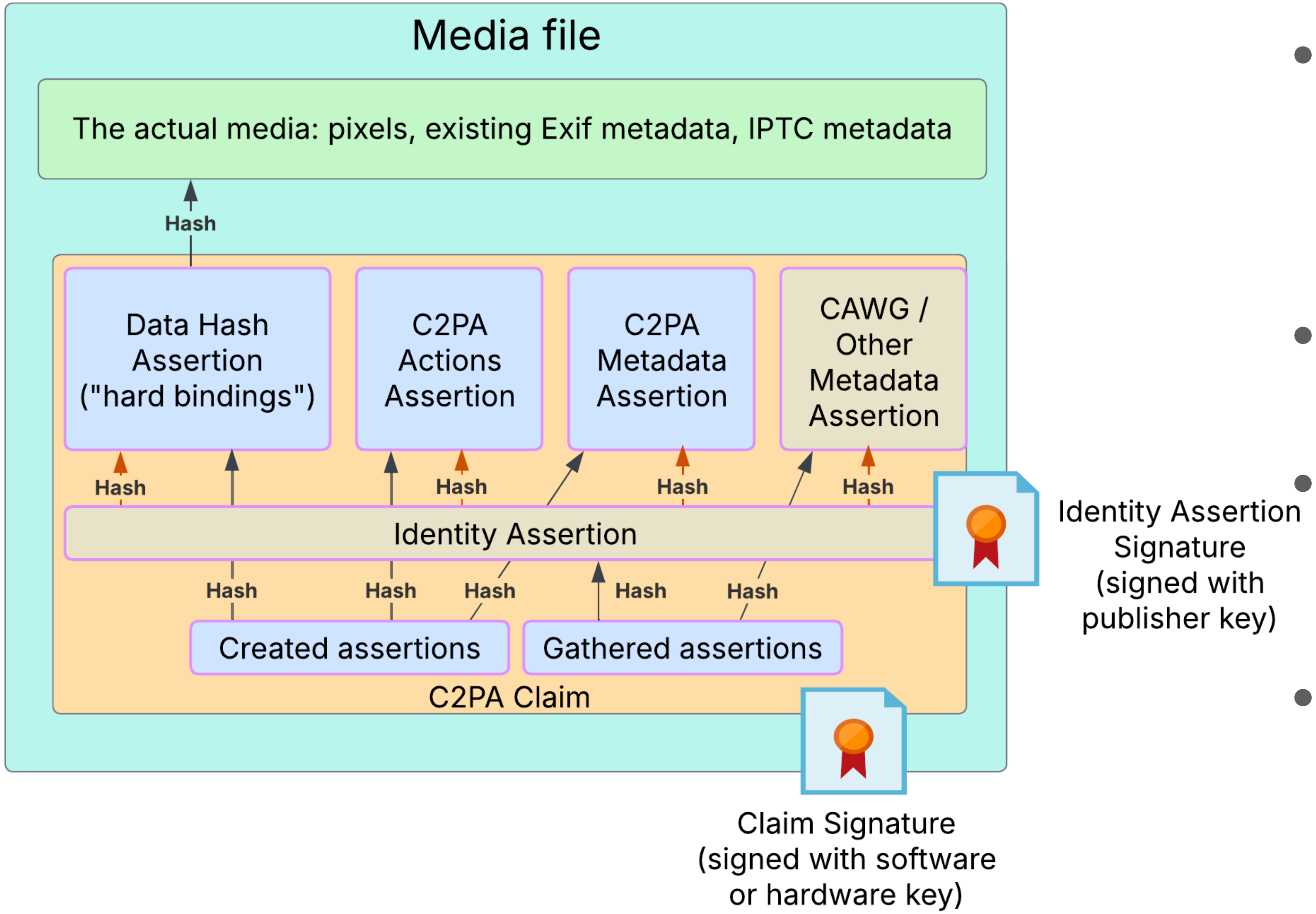
Figure 7. Creating content using identity claims

Standard C2PA model (used today for VNP)



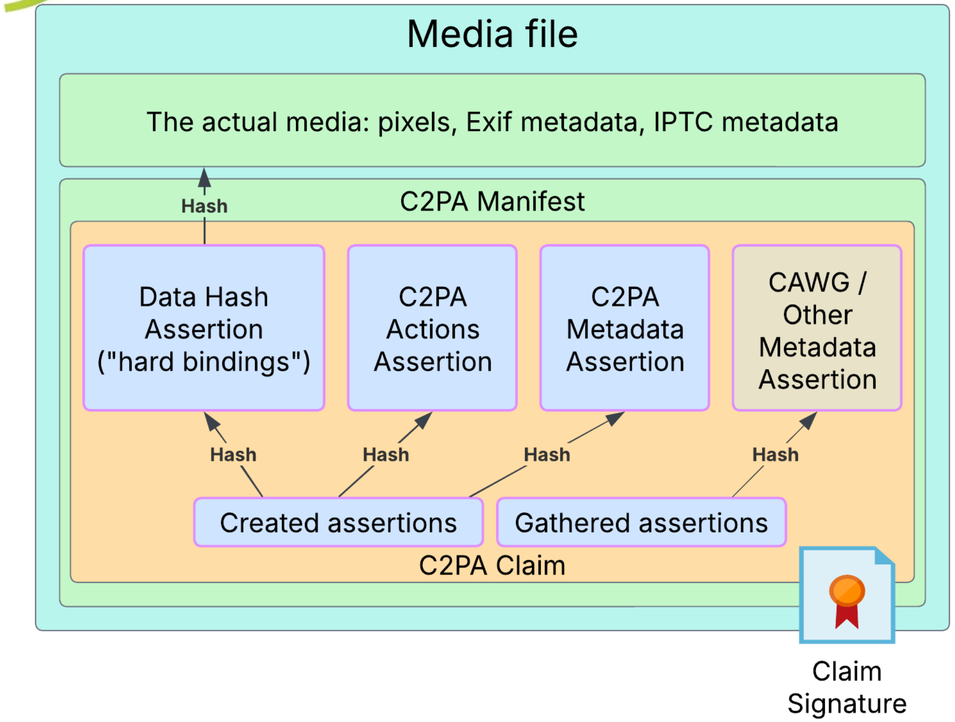
- Content is signed using any entity's key
- Validator checks whether the key's certificate is on a known trust list
- C2PA spec mandates one trust list (for hardware/software) – others are optional
- IPTC Verified News Publisher List is one such optional "additional trust list"
- This is the model that we support today – with the publisher as the signer

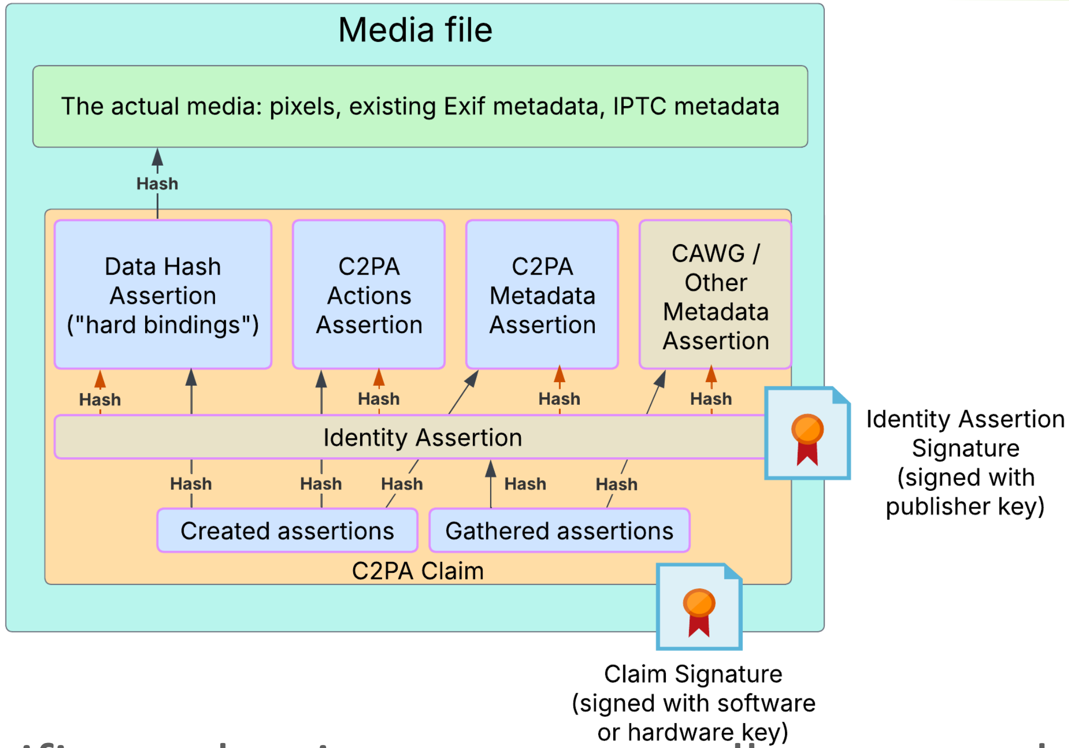
CAWG Identity Assertion model


Media file
The actual media: pixels, existing Exif metadata, IPTC metadata
Hash
Data Hash Assertion ("hard bindings")
C2PA Actions Assertion
C2PA Metadata Assertion
CAWG / Other Metadata Assertion
Hash
Hash
Hash
Hash
Identity Assertion
Hash
Hash
Hash
Hash
Hash
Created assertions
Gathered assertions
C2PA Claim
Identity Assertion Signature (signed with publisher key)
Claim Signature (signed with software or hardware key)

- Main assertion is signed with a key matching a certificate on the C2PA Trust List (i.e. a software system)
- Identity Assertion is signed by a publisher key
- Validator can check the main manifest’s key against the C2PA Trust List
- Validator still needs to look up the certificate of the Identity Assertion signer

The two approaches are not so different…





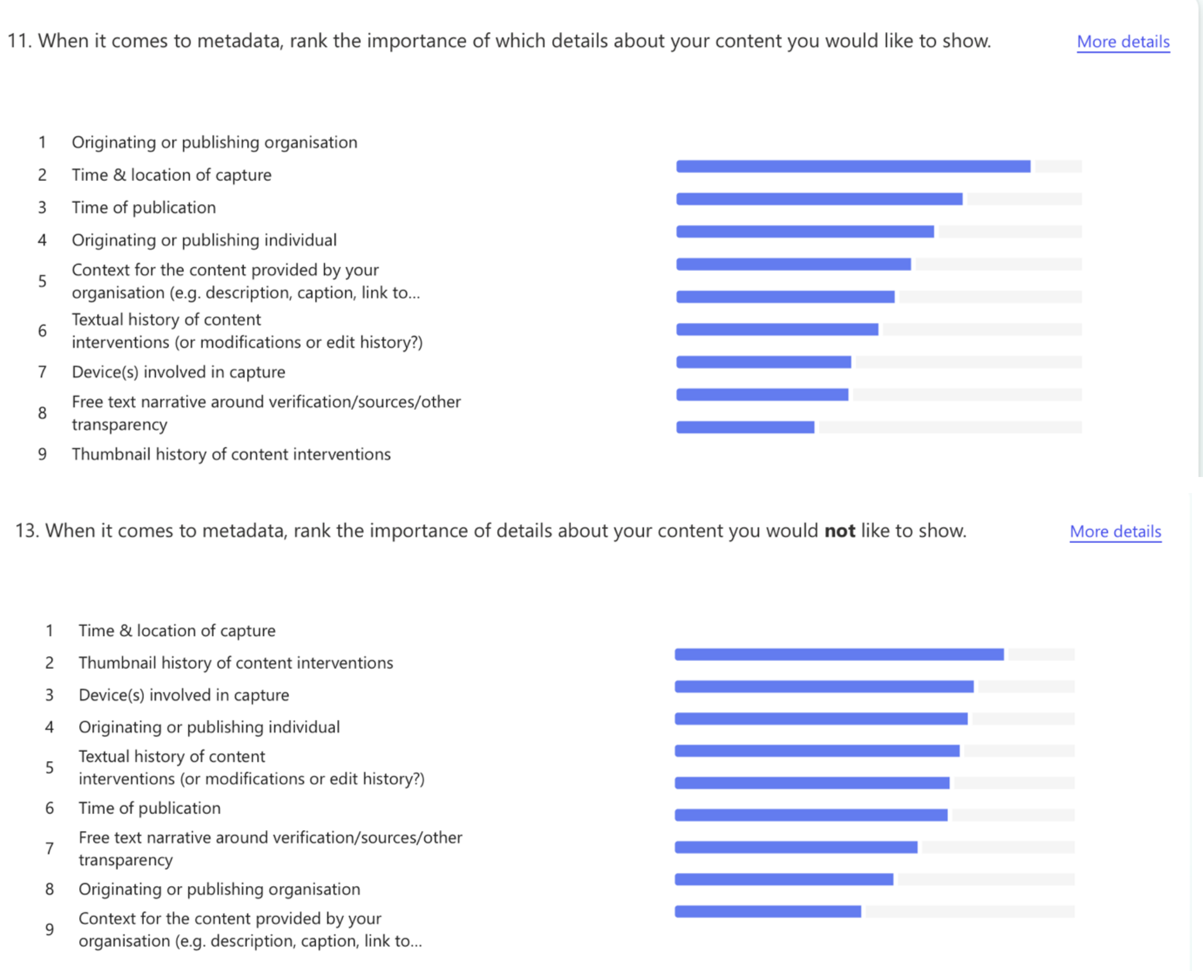
Media file
The actual media: pixels, existing Exif metadata, IPTC metadata
Hash
Data Hash Assertion ("hard bindings")
C2PA Actions Assertion
C2PA Metadata Assertion
CAWG / Other Metadata Assertion
Hash
Hash
Hash
Hash
Identity Assertion
Hash
Hash
Hash
Hash
Hash
Created assertions
Gathered assertions
C2PA Claim
Identity Assertion Signature (signed with publisher key)
Claim Signature (signed with software or hardware key)

In either case, publishers need an x.509 certificate that is on an externally-managed Trust List

So publishers can get a certificate today and use it either to sign content directly today, or to sign identity assertions in the future if they choose

What are our next steps?

- Finalising best-practice guidelines for how metadata should be added to Verified News Publisher signed content
  - We are running / have run workshops with publishers: Paris in early April, Antibes in mid-May, New York City in early June, Norway in September
- Onboarding new publishers and evangelising our work
- Working out requirements for Phase 2 to be able to scale up our processes



11. When it comes to metadata, rank the importance of which details about your content you would like to show. More details

1 Originating or publishing organisation
2 Time & location of capture
3 Time of publication
4 Originating or publishing individual
5 Context for the content provided by your organisation (e.g. description, caption, link to...
6 Textual history of content interventions (or modifications or edit history?)
7 Device(s) involved in capture
8 Free text narrative around verification/sources/other transparency
9 Thumbnail history of content interventions

13. When it comes to metadata, rank the importance of details about your content you would **not** like to show. More details

1 Time & location of capture
2 Thumbnail history of content interventions
3 Device(s) involved in capture
4 Originating or publishing individual
5 Textual history of content interventions (or modifications or edit history?)
6 Time of publication
7 Free text narrative around verification/sources/other transparency
8 Originating or publishing organisation
9 Context for the content provided by your organisation (e.g. description, caption, link to...

Results of a survey of publishers undertaken by the BBC in 2024

We are looking at many practical questions and issues around C2PA implementation for the news industry

- How do we set up a public key infrastructure that can scale to thousands of publishers?
- Who should be included on the “Verified News Publisher List”, i.e. who should be able to receive a certificate?
  - The entertainment media and advertising industries are both interested in what we are doing
  - We hope that there will be a generic mechanism for “verified organisations” that makes this moot
- Do we need cooperation from the platforms (TikTok, X, Telegram, browser makers etc) to make this work at scale?
- What metadata should be mandatory, if any, in a Verified News Publisher “best practice” media item? Should these be different for video vs still images?
- How do we restore metadata / assertions that have been stripped out of the image by bad actors? How do we identify images that have been slightly altered, e.g. cropped so that the digital hash no longer matches?
  - The C2PA spec supports “soft binding” techniques such as watermarking, asset registries, tamper-resistant “perceptual” hashes etc, known as “Durable Content Credentials”. But they have not yet been implemented on an open, industry level.
- How do we educate users to understand, and seek out, these provenance signals?