



Preserving Media Provenance Metadata with C2PA

Pam Fisher, Lead, IPTC Video Metadata Working Group

pamfisher@gmail.com

29 April 2025



Introducing IPTC

(International Press and Telecommunications Council)

IPTC Voting Members include:



IPTC Liaison Partners include:



- IPTC (<https://iptc.org/>) is the global standards body of the news media, providing the technical foundation for the news ecosystem
- An open, non-partisan organisation dedicated to promoting interoperable standards and best practices in the news and media industries
- Founded in 1965 in the UK, IPTC is a non-profit organisation funded by member subscriptions
- Members join as voting members, affiliate members, or individuals



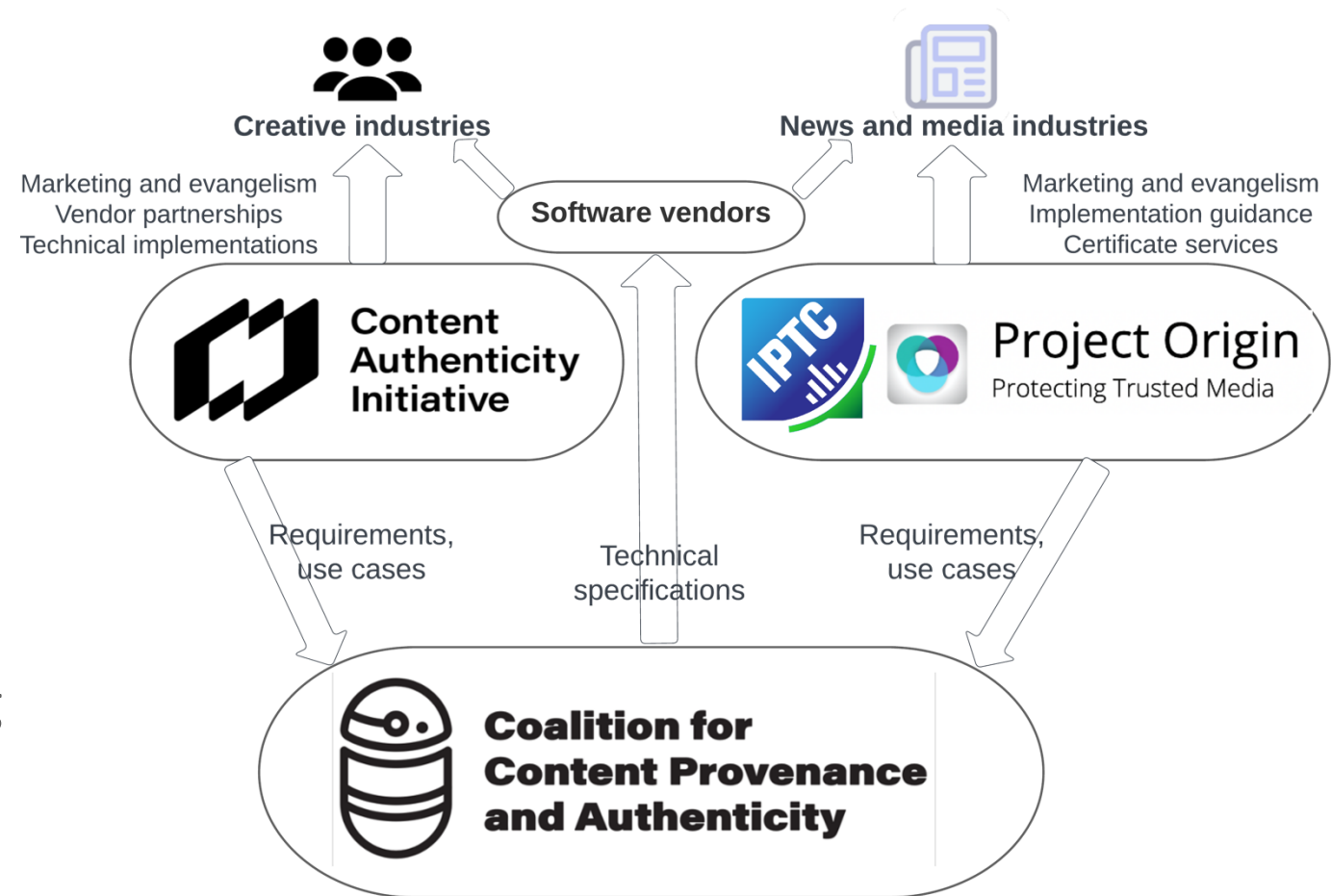
First, some acronyms and background

- **CAI - Content Authenticity Initiative:** <https://contentauthenticity.org/>
 - Founded and led by Adobe (2019)
- **Project Origin:** <https://www.originproject.info/>
 - Founded by: BBC, CBC/Radio-Canada, The New York Times, and Microsoft (2019)
- **C2PA – Coalition for Content Provenance and Authenticity:** <https://c2pa.org/>
 - Unifies the efforts of the **Content Authenticity Initiative** and **Project Origin** to provide technical foundation for trust in media (v 1.0 - 2021)
- **CAWG - Creator Assertions Working Group:** <https://cawg.io/>
 - Builds on the work of the C2PA by defining additional assertions that allow content creators to express individual and organizational intent about their content
 - Now (March 2025) a working group within DIF – the Decentralised Identity Foundation



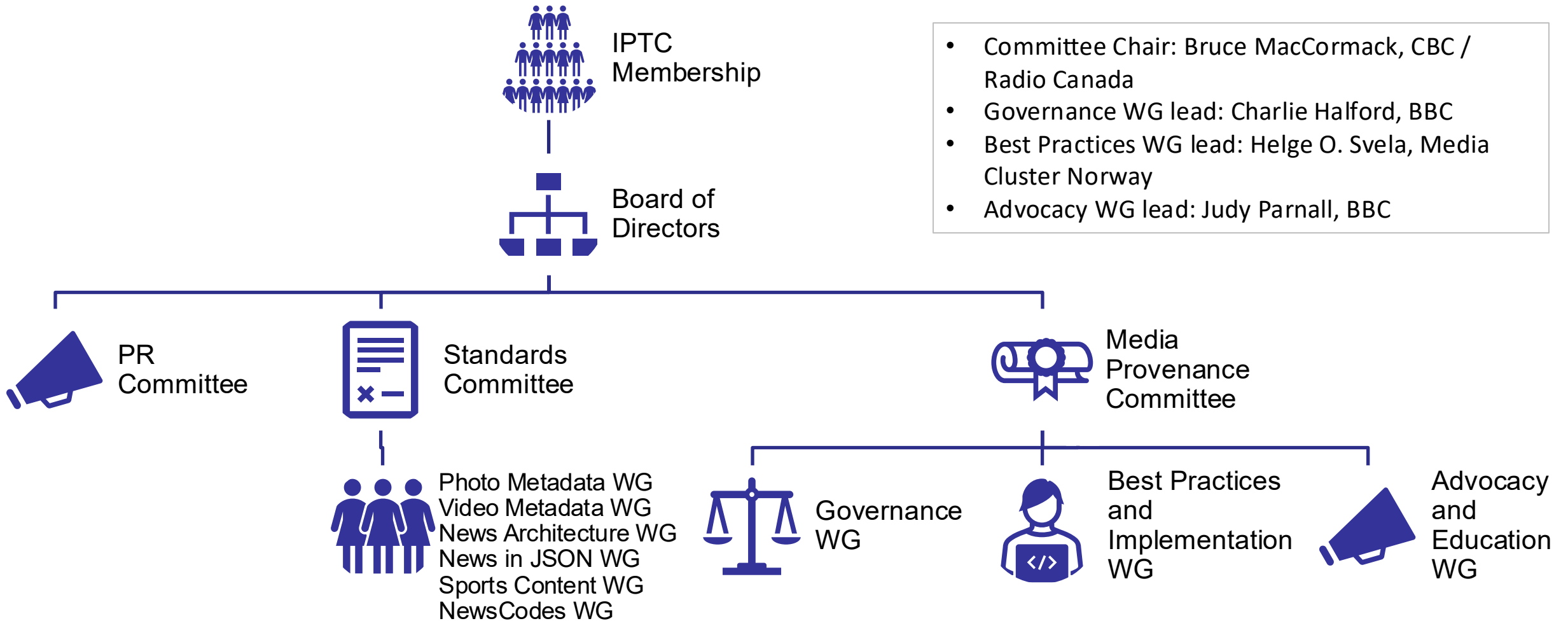
C2PA, CAI, Project Origin, IPTC: How does it all fit together?

- Project Origin + CAI joined together to create C2PA – Coalition for Content Provenance and Authenticity
- 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
- The work now continues as the IPTC Media Provenance Committee
- “Project Origin” and “Origin” branding remain



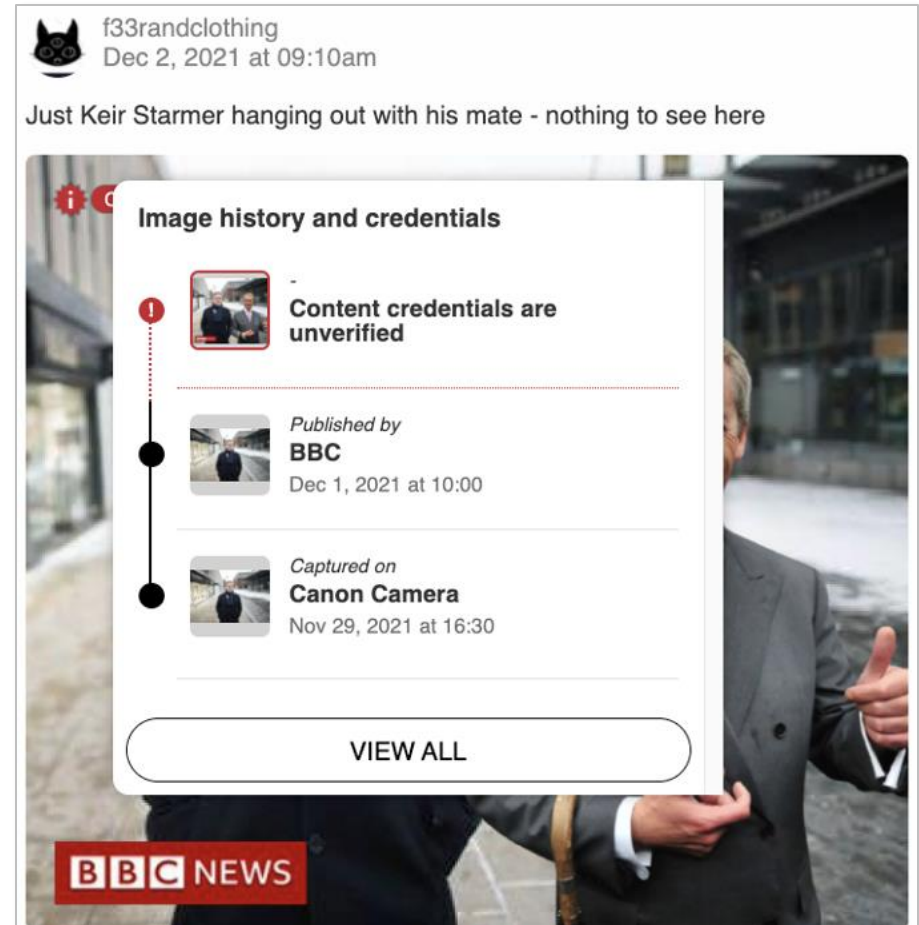


IPTC Media Provenance Committee



Proving what's real is easier than detecting what's fake

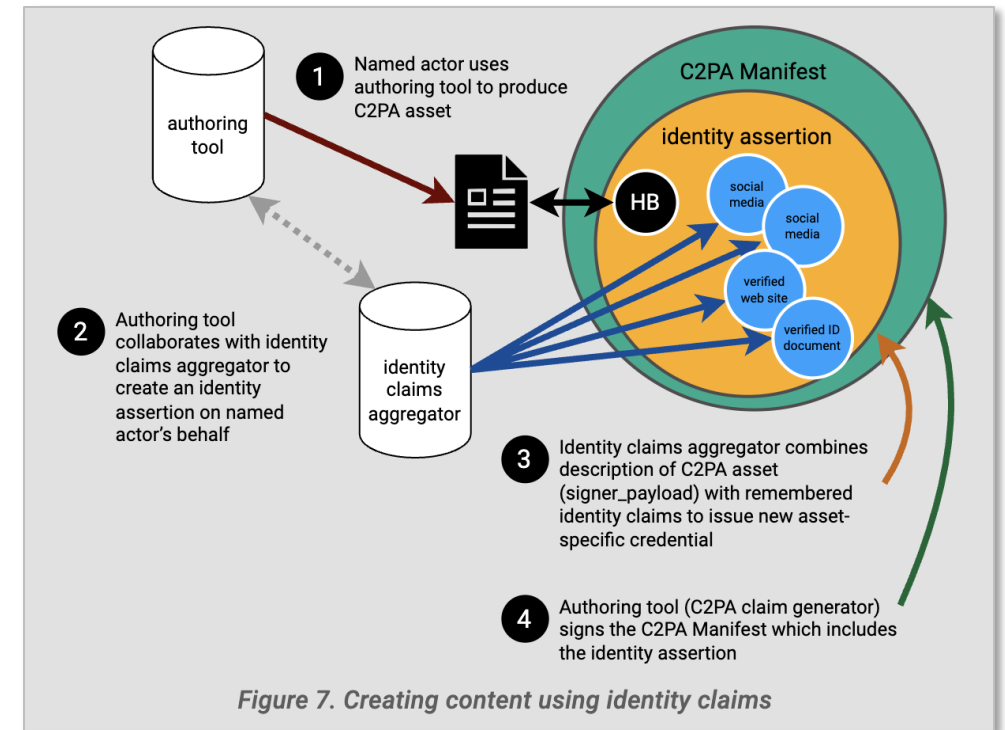
- Overall, the approach is to digitally sign content
- These embedded, secure credentials are called “assertions”
- Signed assertions become “claims” embedded in the C2PA “manifest”
- If the media has been modified, the digital “hash” no longer matches, and this will be highlighted to users
- The aim is for this technology to be built into websites, browsers and online platforms



Source: BBC mockup

Creator Assertions Working Group (CAWG) and Identity Assertions

- C2PA alone now covers **only hardware and software** provenance, not creators, producers and publishers**
- Because all means of identifying individuals and organisations were removed from C2PA, the spin-off group Creator Assertions Working Group (CAWG) was initiated to incubate the parts removed from the spec.
- Two significant CAWG projects are:
 - The **cawg.metadata** assertion for generic metadata properties (any metadata that can be expressed in JSON-LD, including IPTC, EXIF, schema.org and more)
 - The **cawg.identity** assertion allows named actors to sign some or all assertions in a C2PA manifest

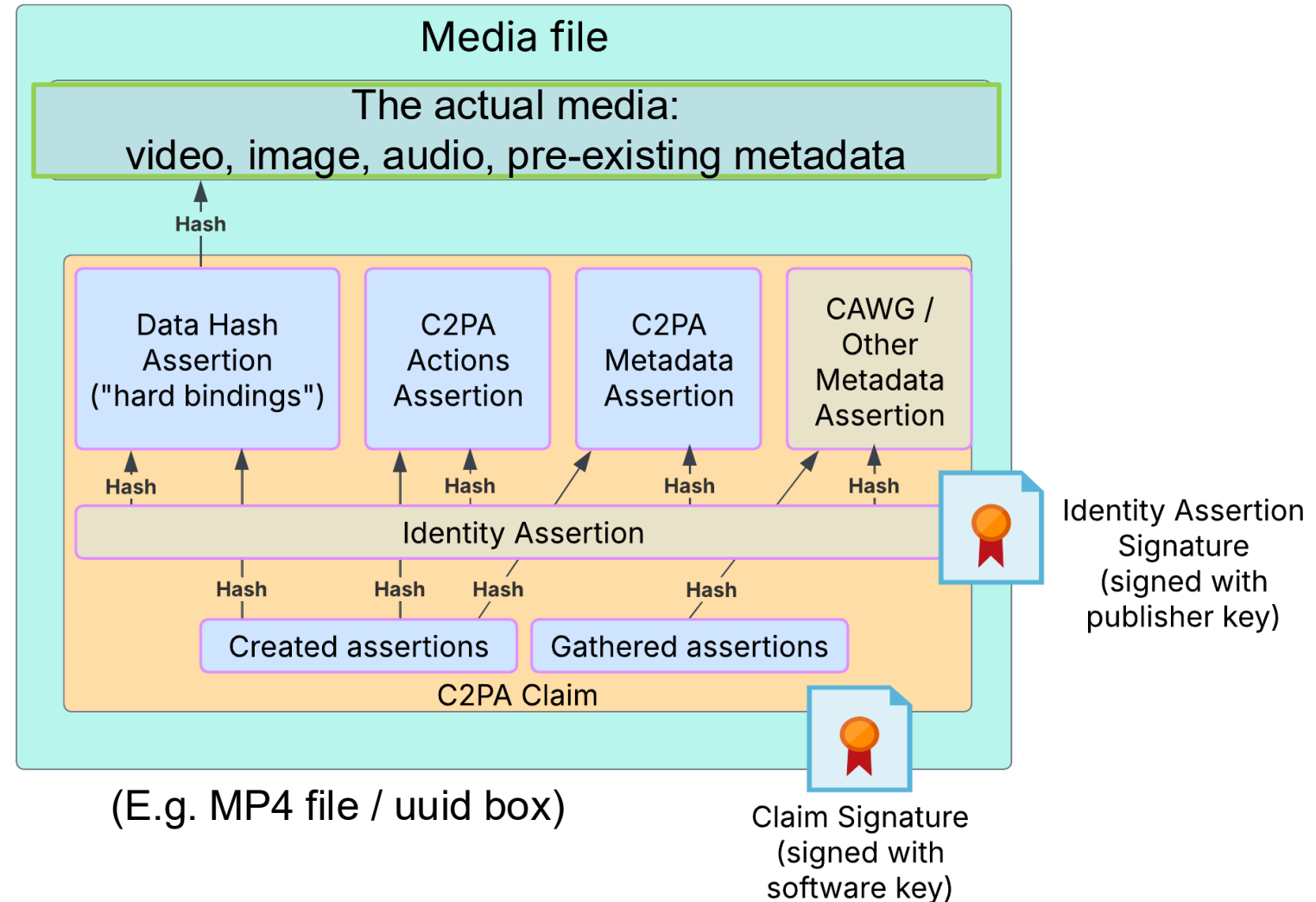


** C2PA v 2.0 section 5.2.2 (Jan 2024): “This version represents a significant departure from previous versions. It reduces the use of the term “actor”, which no longer represents humans and organisations. In addition to validator-configured trust lists, it also introduces a new default trust list, the “C2PA Trust List”, which is intended to cover certificates issued to hardware and software”

Overall C2PA-ready media file

The C2PA manifest:

- C2PA claim signature(s) from hardware and software
 - E.g. Sony camera, Final Cut Pro)
- Identity assertion signature(s) from publisher (cawg.identity)
 - E.g. New York Times
- Any other metadata (cawg.metadata)
 - E.g. EIDR ID, title, description, rights info)





Creating C2PA assertions

- Open tools for creating C2PA and embedding assertions:
 - <https://www.iptc.org/std/videometadatahub/generator/>
 - <https://opensource.contentauthenticity.org/docs/c2patool/>

IPTC Video Metadata Hub Generator

This tool shows the capabilities of IPTC's Video Metadata Hub standard. VMHub can be expressed in JSON (as well as other formats). As you enter video metadata into the form, you can see the corresponding VMHub JSON appear.

For more information, see the [IPTC Video Metadata Hub pages on iptc.org](#) or the [Video Metadata Hub User Guide](#). Discuss this tool on the [public iptc-videometadata email discussion group](#).

Please note that this tool demonstrates only a small subset of the available fields in IPTC video Metadata Hub. The full VMHub spec includes many more fields such as Episode/Season/Series, fields for People shown, model release and rights information, transcripts, and much more.

Enter video metadata

Date created: Language: Video Identifier:

Title:

Headline:

Description:

Keywords:

Location:

Alt Text:

Creator:

Copyright Notice:

Copyright Owner: Copyright Year:

Credit Line:

Contributor:

Digital Source Type:

View the generated Video Metadata Hub data

Choose output format:

Save this JSON-LD block to a file and add it to your video using the `c2patool` command `c2patool <input video file> -m iptc-vmhub-assertion.json -o <output video file>`

```
{
  "@alg": "es256",
  "@private_key": "es256_private_key",
  "@sign_cert": "es256_certs.pem",
  "@ta_url": "http://timestamp.digicert.com",
  "@claim_generator": "IPTC Video Metadata Hub Generator with c2patool",
  "@title": "Video signed with c2patool",
  "@assertions": [
    {
      "@label": "stds:iptc",
      "@data": {
        "@context": {
          "iptc4kmpCore": "http://iptc.org/std/iptc4kmpCore/1.0/xmlns",
          "iptc4kmpExt": "http://iptc.org/std/iptc4kmpExt/2008-02-29/",
          "dc": "http://purl.org/dc/elements/1.1/",
          "photoshop": "http://ns.adobe.com/photoshop/1.0/",
          "plus": "http://ns.safelink.org/ldf/xmp/1.0/",
          "xmp": "http://ns.adobe.com/xap/1.0/",
          "xmpDM": "http://ns.adobe.com/xmp/1.0/DynamicMedia",
          "xmpRights": "http://ns.adobe.com/xap/1.0/rights"
        },
        "dclanguage": "en"
      }
    }
  ]
}
```

Content Authenticity Initiative

C2PA command line tool

C2PA Tool, `c2patool`, is a command line tool for working with C2PA [manifests](#) and media assets (audio, image or video files).

Use the tool on a file in one of the [supported formats](#) to:

- Read a summary JSON report of C2PA manifests.
- Read a low-level report of C2PA manifest data.
- Add a C2PA manifest to the file.

For a simple example of calling `c2patool` from a Node.js server application, see the [c2patool-service-example](#) repository.

CAI open source SDK

Getting started >

Understanding manifests >

C2PA Tool v

Using C2PA Tool

Supported media formats

Using a manifest file



The C2PA ecosystem is still evolving

- C2PA Claims are validated using an independent “**Trust List**”
 - Currently, a “CAI Temporary Known Trust List”, but this will cease working this year (many current demos use this, but will time out shortly)
 - The v.2.0 –compliant **C2PA Trust List** (hardware and software) will launch “**during 2025**”
 - C2PA v.2.1 spec provides for “additional trust list” anchors
 - IPTC Origin Verified News Publishers List is an “additional trust list” compliant with the [C2PA 2.1 spec](#). More info here: <https://iptc.org/verified-news-publishers-list/>
 - Discussing extending to wider entertainment community, ideally collaborating with EIDR



Origin Verified Publisher

- There are a handful of **validators**, largely open source:
 - <https://contentcredentials.org/verify> (from CAI)
 - <https://originverify.iptc.org/> (from IPTC / Origin)
 - Also several integration tools (e.g. Wordpress plug-in)



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
- Current VNP trust list (+10 in process):

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 misinformation. Recent attacks on OpenAI, Meta, and other major tech companies have shown an evident way of content provenance.

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



Deutsche Welle



Radio-Canada

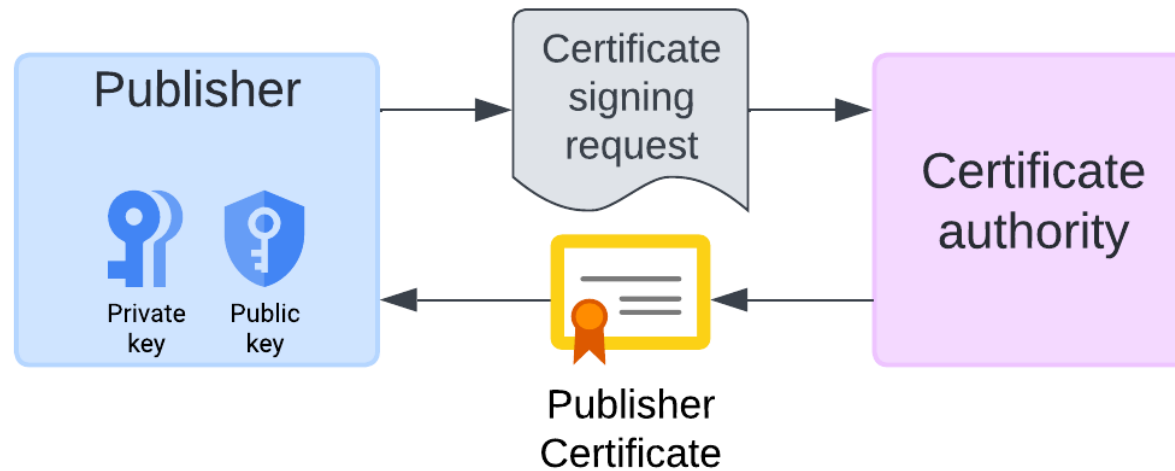




How does a publisher join the Verified News Publishers Trust List?

- The current process is in the early stages and limited to news publishers

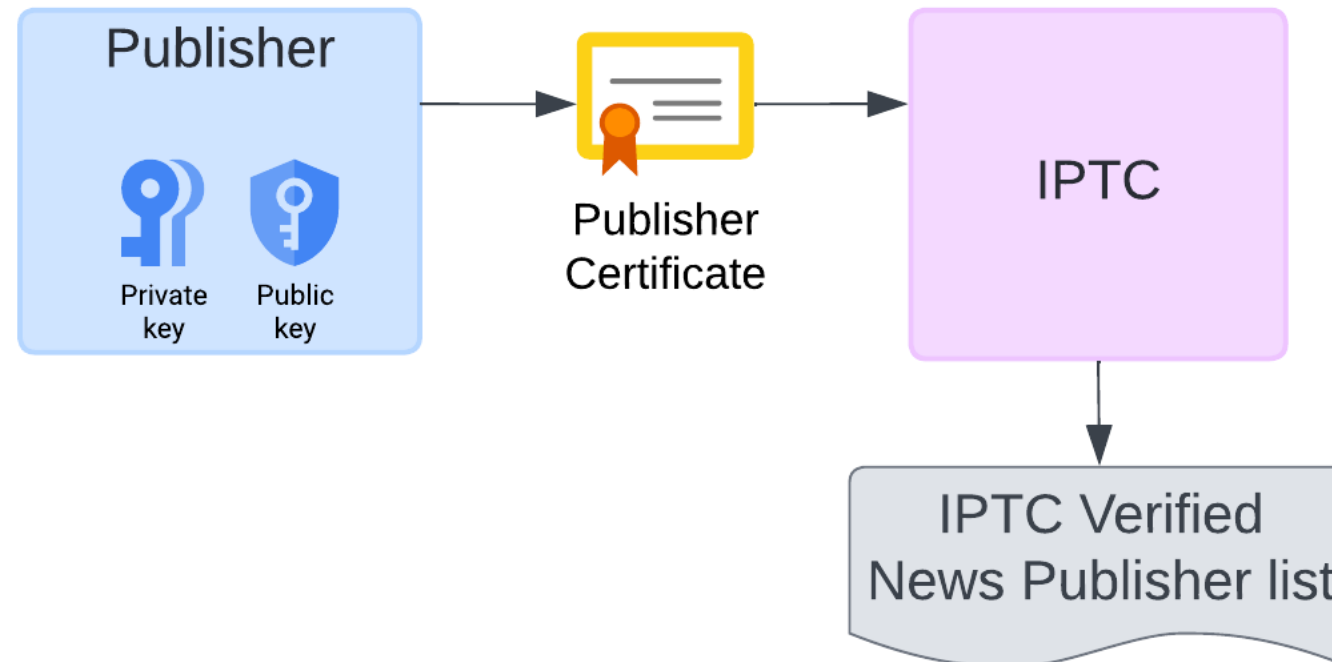
Step 1. Obtain an organisational document- or email-signing certificate from an approved Certificate Authority





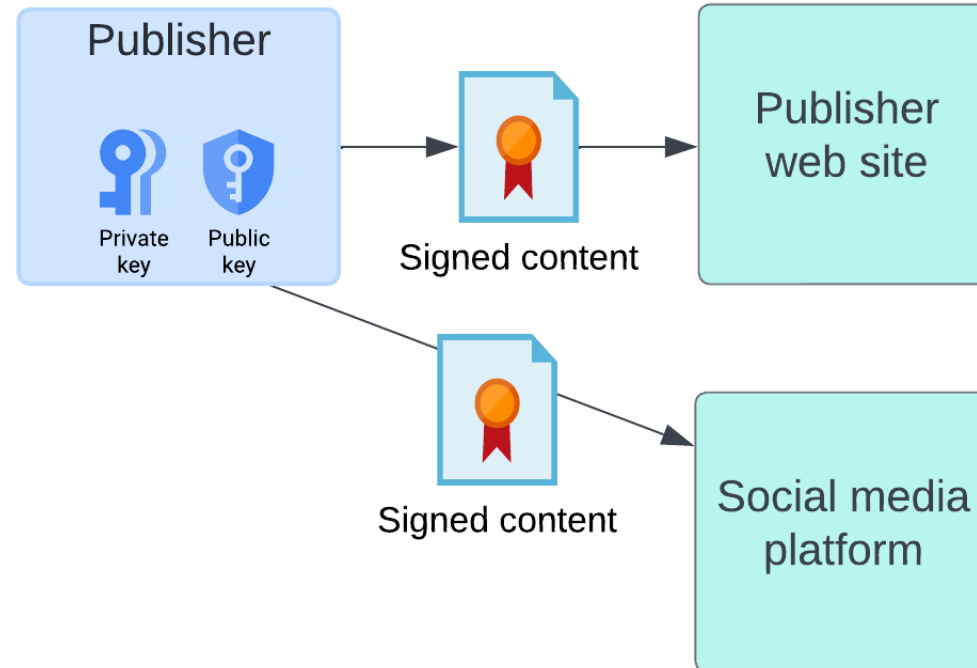
How does a publisher join the Verified News Publishers Trust List?

Step 2. Send the certificate to IPTC for approval as a Verified News Publisher



How does a publisher join the Verified News Publishers Trust List?

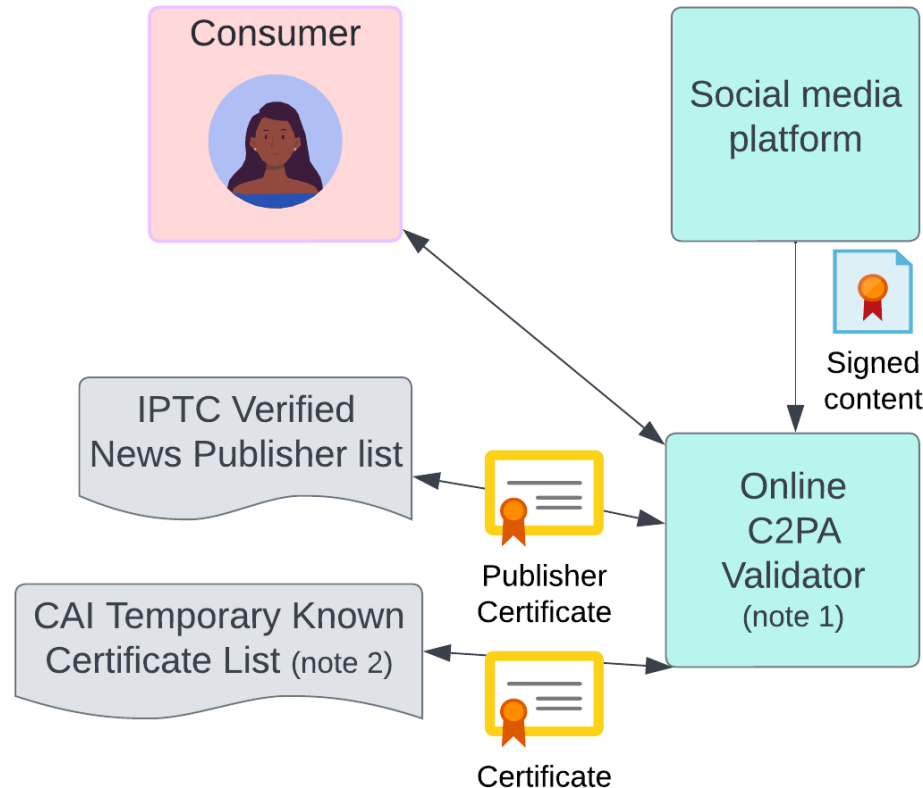
Step 3. Sign content using publisher private key. Publish content





How does a publisher join the Verified News Publishers Trust List?

Step 4. Consumer checks content using a C2PA validator. Validator consults the IPTC Verified Publisher List.



Notes

1. Not all C2PA validators currently support the IPTC list. The IPTC validator at originverify.iptc.org supports both the CAI and IPTC lists.
2. The CAI Temporary Known Certificate List will soon be replaced by the C2PA Trust List, certifying software and hardware that has passed a compliance audit.



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

The screenshot displays the Origin Verify Validator interface. At the top left is the IPTC logo and the text "Origin Verify News Provenance Verification". The main heading reads "Verify the source of your news content". Below this, it says "Upload a file to see which news organisation created it" and "This technology is new. Not all content has Content Credentials yet". A file selection button "Select a file from your device" is visible. The file "AFPPhotoSigned4Iptc.jpg" is shown with a verification status of "Verified" (indicated by a green checkmark). A tooltip states: "This content was signed with a certificate that is on the IPTC Origin Verified News Publisher list." The interface includes expandable sections for "General information" (Name: AFPPhotoSigned4Iptc.jpg), "Certificate details" (Signer: AGENCE FRANCE PRESSE), and "Signing tool". At the bottom, there are "Reset" and "See full metadata" buttons. On the right, a preview of the image shows the Eiffel Tower at night with bokeh lights.



Tools and services to support publishers: IPTC Media Provenance wiki

- We have created an internal wiki for IPTC members
- Includes a step-by-step guide helping publishers to obtain certificates and add them to the Verified News Publishers list
- Includes guides on tech and tools, but also info on workflows and help to explain benefits of C2PA to newsrooms

The image displays two screenshots of the IPTC Media Provenance wiki. The top screenshot shows the 'Tech & Implementation issues' page, which is a parent page for content related to implementing C2PA. The bottom screenshot shows the 'Obtaining a certificate from GlobalSign' page, which provides a high-level summary of the process. A search bar in the bottom screenshot shows the search term 'globalsign' and the result 'Obtaining a certificate from G...' is highlighted. The page content includes a list of steps for obtaining a certificate from GlobalSign.

Tech & Implementation issues

Owned by [Brendan Quinn](#) ...
Last updated: Feb 12, 2025 · 10 people viewed · 1 link

Parent page for all content related to actually implementing C2PA and working out how to

Obtaining a certificate from GlobalSign

Owned by [Brendan Quinn](#) ...
Last updated: Mar 14, 2025 · 5 min read · 7 people viewed · 0 link

According to our updated Phase 1 policy for the IPTC Origin Verified News Publishers List, publishers can now obtain a certificate directly from a Certificate Authority and obtain Verified News Publisher approval in two parallel processes.

The first Certificate Authority that we have identified is GlobalSign. Their "Personal Sign 2 Department" email-signing certificate meets our (newly updated) criteria. AFP and IPTC have both gone through this process with this certificate type, so we know that it works.

High-level summary of the process

1. Buy a "PersonalSign 2 - Department" certificate from GlobalSign. Go through the GlobalSign vetting process.
2. Obtain a private/public keypair. For this step you have two options:
 - a. Generate a public/private keypair using AWS Key Management Service. Generate a Certificate Signing Request (CSR) using your private key (we provide a tool to help with this process)
 - b. Alternatively you can let GlobalSign generate the keypair for you and sent it to you via a secure download from their website.
3. When your certificate application has been approved by GlobalSign, submit your CSR to



Tools and services to support publishers: Wordpress plugin

- 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!

The image shows a composite of three elements related to the C2PA signing process:

- C2PA Signer Settings:** A configuration panel for the Wordpress plugin. It includes sections for 'General settings' (with 'Enable C2PA Signing' and 'Keep Original Image' checked), 'Signing Scope' (set to 'Sign all images attached'), and 'Signing settings' (with fields for 'Path to Signing Script', 'AWS KMS Key ARN', and 'Certificate Chain File').
- Origin Verify:** A verification interface for the file 'PRINCE_WILLIAM_IN_TALLINN-768x1315.jpg'. It shows a 'Verification status' of 'Verified' with a green checkmark. A tooltip states: 'This content was signed with a certificate that is on the IPTC Origin Verified News Publisher list.' Below this, 'General information' is expanded to show: '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.', and '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' are also visible, showing the 'Signer: Comite International des Telecommunications'. Buttons for 'Reset' and 'See full metadata' are at the bottom.
- Image:** A photograph of Prince William in a green puffer jacket, standing in front of a construction site with a crane.



What are the next steps?

- Be patient! Media provenance using C2PA is worth supporting, and broad adoption will become feasible over the next 6-18 months
- Many, many organizations and individuals are working on this through the initiatives discussed – there is substantial support
 - Most welcome new members, including IPTC!
- Begin planning for adoption now

Thank you!

Pam Fisher – pamfisher@gmail.com, 310-927-4479

For more information on Media Provenance at IPTC: <https://iptc.org/media-provenance/>