



C2PA and Media Provenance updates

Brendan Quinn
Managing Director, International Press
Telecommunications Council (IPTC)



What problem are we trying to solve?

Publishers are constantly fighting against being misrepresented

The screenshot displays the CBC News website interface. At the top, there is a navigation bar with the CBC logo, a search bar, and a 'Sign In' button. Below this, a red banner contains the word 'NEWS' and a list of categories: Top Stories, Local, Climate, World, Canada, Politics, Indigenous, Business, and The National. The main content area features a news article titled 'Canada's new prime minister Mark Carney announces new federal relief initiative to help offset the devastating cost of US tariffs to Canadians'. The article is attributed to Madeleine Cummings and includes a timestamp. A large photograph of Mark Carney speaking at a podium is positioned below the headline. To the right of the article, there is a sidebar with a 'CBC NEWS' logo and a 'BEING BLACK IN CANADA' section. Below the article, there are two more sections: 'Canada Crypto Fund' and 'ombudsman'. The 'Canada Crypto Fund' section includes a photo of Mark Carney and text about the initiative. The 'ombudsman' section provides a link to learn more about CBC's journalistic standards.

Countering distrust in news media

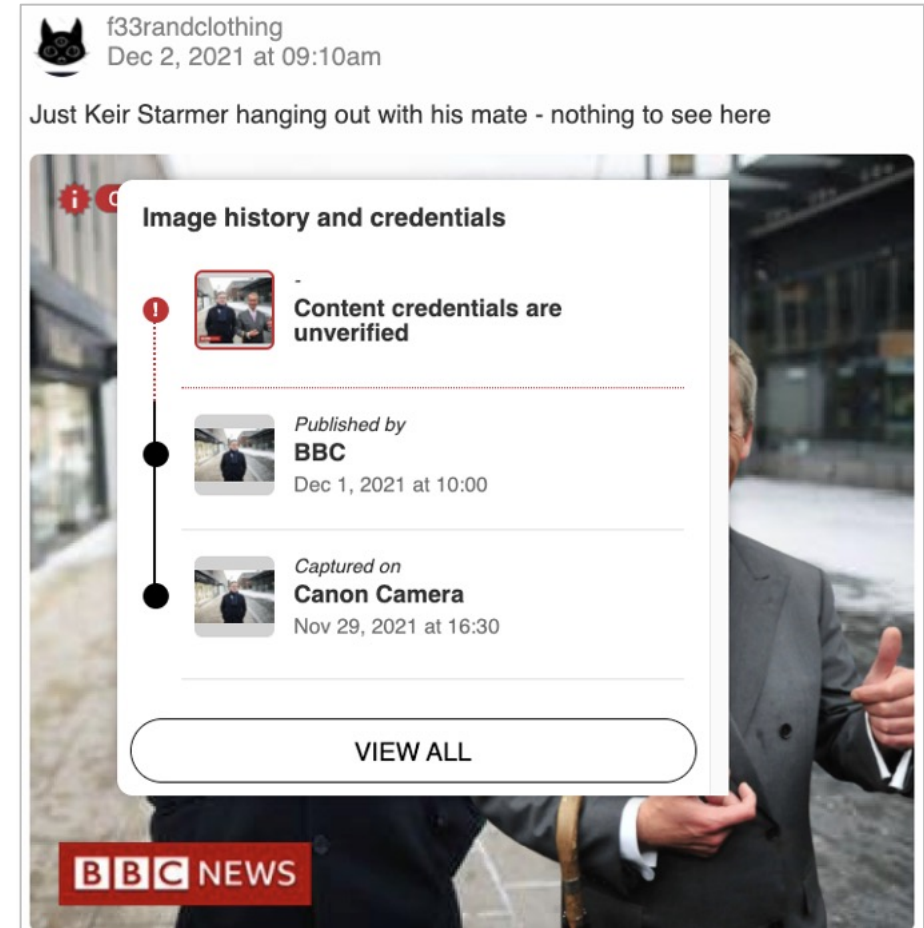
- Trust in the news is at an all-time low
 - “just 40% of our respondents across all 47 markets say they trust most news” (Reuters Institute Digital News Report, 2024)
 - 59 per cent of respondents say that they are concerned about fake news online
- AI-generated fake news, misinformation and disinformation is getting harder to detect
 - It’s becoming an arms race, with no end in sight





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

- Our approach is to digitally sign content that is produced by news publishers
- If the media has been modified since it was signed, the digital “hash” no longer matches, and it will be highlighted to users
- The aim is for this technology to be built into websites, browsers and online platforms



Source: BBC mockup



C2PA progress since previous Photo Metadata Conference in May 2024



IPTC Origin Verified News Publisher List

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 supported as a strong defense against misinformation. Recent announcements from **OpenAI**, **Meta**, **Google** and others have shown an evident way of confirming the authenticity of content.

Project Origin, as a co-founder of the C2PA community to the forefront of the C2PA 2.0 compatible Content Credentials, securely create a cryptographic signature through the IPTC, which can be verified through the IPTC, which can be verified through the IPTC.

Origin Verified Publisher

The group has created the "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



Currently in the process of joining:



Origin Verified Publisher



TE REO
IRIRANGI
O AOTEAROA





Tools and services to support publishers



Verify the source of your news content

Upload a file to see which news organisation created it

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

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

[Reset](#)

[See full metadata](#)

Origin Verify Validator
<https://originverify.iptc.org>

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

Signing Scope

Signing settings

Configure image signing settings

Path to Signing Script

AWS KMS Key ARN

Certificate Chain File

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

[Reset](#)

[See full metadata](#)

IPTC C2PA WordPress plugin
(not yet released publicly)



France Télévisions signing daily news content

franceinfo:



Radio • Live



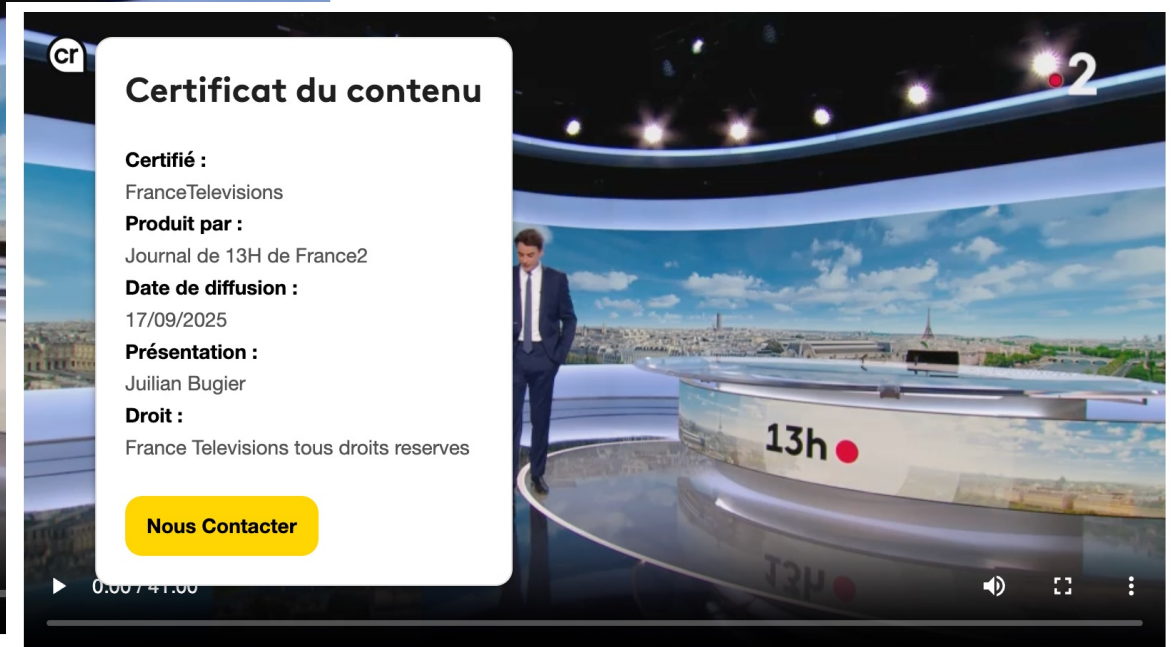
Services ▾



Mon espace ▾

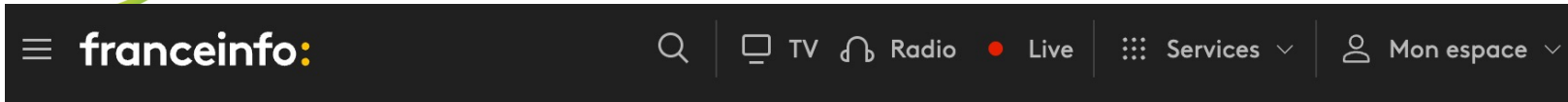
Dernière édition du JT de 13h

- [C2PA-signed content page](#)
- [Announcement \(in English\)](#)





France Télévisions signing daily news content



Dernière édition france.tv&vous



The Lab News R&D Tech Content Open Innovation Transformation Méta-Média

< Back

France Télévisions adopts the C2PA standard to authenticate its content... and receives the EBU Technology Award.

Tech | Published on September 16, 2025

With the development of generative AI, it is becoming increasingly difficult to make a difference between authentic videos and those generated by AI when browsing the internet. In its commitment to transparency, France Télévisions wants to be able to guarantee its content to its audiences by adopting the C2PA protocol.

Share this article!

X

in

envelope

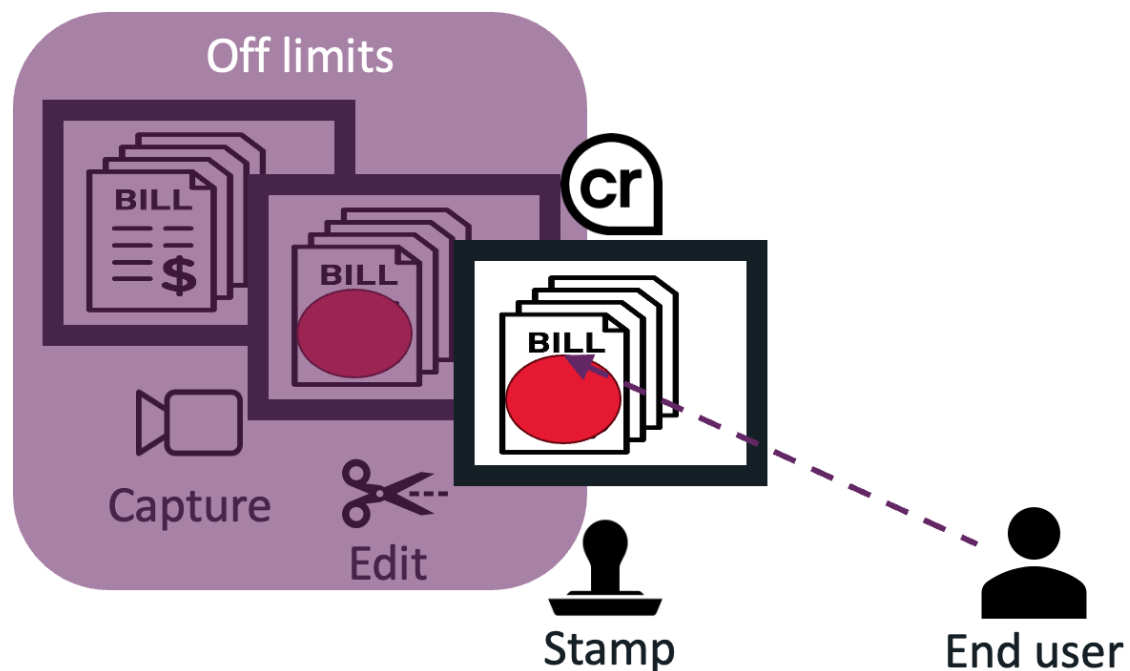
link

- [C2PA-signed content page](#)
- [Announcement \(in English\)](#)



IBC Accelerator: Stamping Your Content

Stamping creates a 'Trust' point



Champions

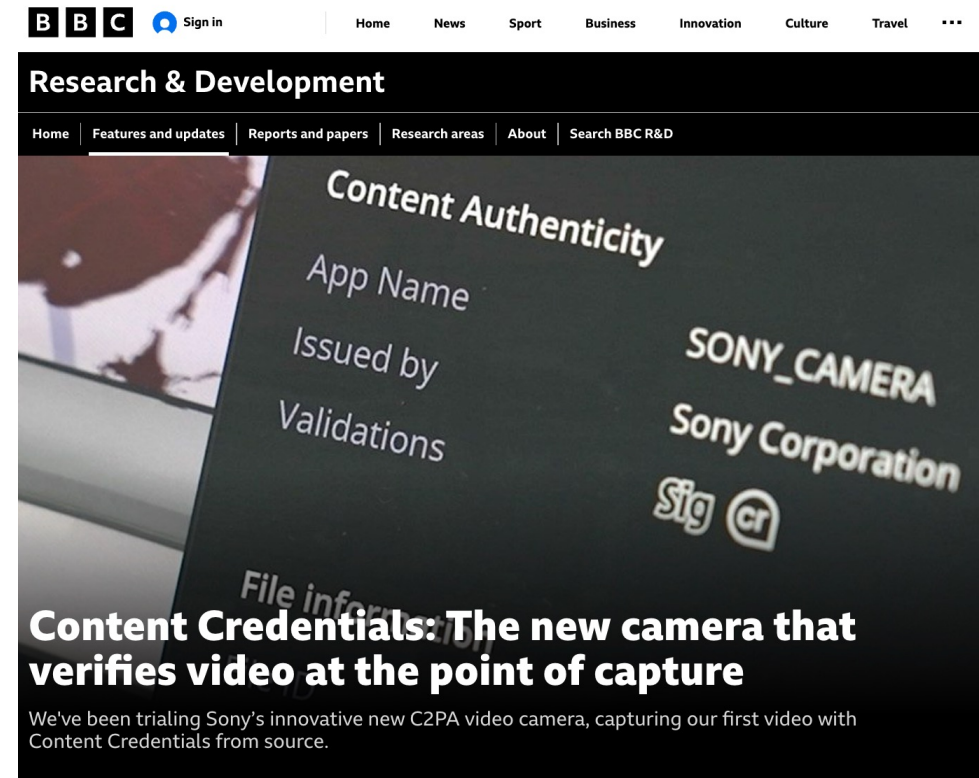


Participants



BBC R&D trial with Sony C2PA-enabled broadcast camera

- Part of the IBC Accelerator project
- “Using a pre-release version of Sony’s PXW-Z300 camera, which was announced in July 2025, we had one of the world’s first use cases of testing the C2PA workflow with video footage”



Published: 11 September 2025



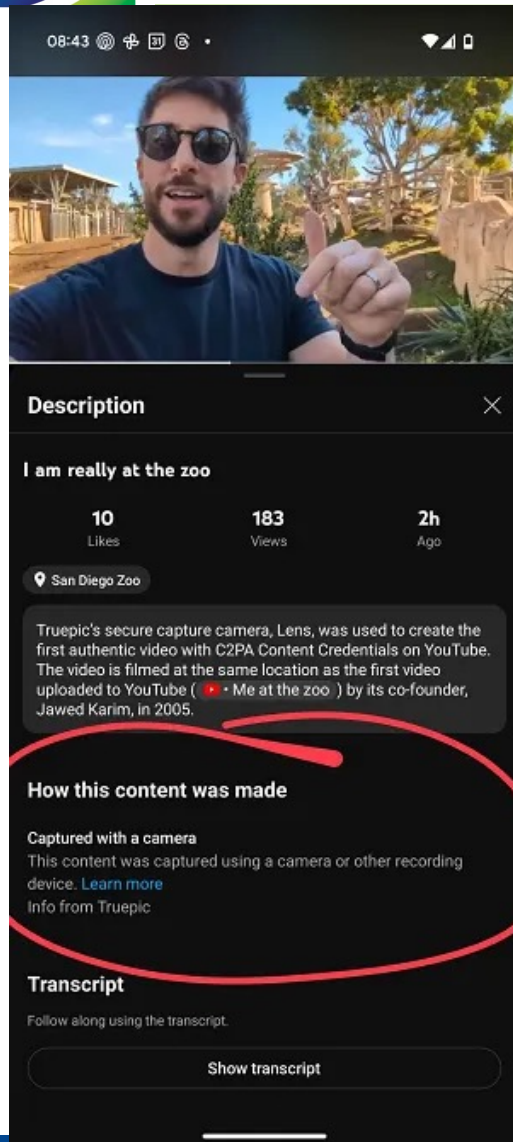
Judy Parnall
Head of Standards and Industry



Charlie Halford
Principal Research Engineer

As interest in authenticating digital content grows, broadcasters and news organisations need practical ways to assert source integrity and publisher credibility. This is particularly important as AI-generated media - video, still images and audio - is becoming more common and more convincing. That makes it **harder for journalists to distinguish between what is real and what is synthetic**.

YouTube “Captured with a camera” (Oct 2024)



How to get ‘Captured with a camera’ disclosure

For “captured with a camera” to appear in the expanded description, creators must use tools with built-in C2PA support (version 2.1 or higher) to capture their videos. This allows the tools to add special information, metadata, to the video file, confirming its authenticity. YouTube will relay the information that the content was “Captured with a camera,” and apply the disclosure when it detects this metadata. The content must also not have edits to sound or visuals. This disclosure indicates that the content was captured using a camera or other recording device with no edits to sounds or visuals.

What edits to avoid

To ensure the “Captured with a camera” can be applied, avoid these types of edits:

- Edits that break the chain of provenance, or make it impossible to trace the video back to its original source. For example, if you capture an image with C2PA metadata and then save it to your phone's photo album that doesn't support C2PA v2.1 or higher, that may break the chain of provenance.
- Significant alterations to the video's core nature or content, including its sounds or visuals.
- Edits that make the video incompatible with C2PA standards (version 2.1 and above).



C2PA 2.x and Identity

- From version 2.0 of the C2PA spec, released in January 2024, all references to individual or organisation identity were removed from the core C2PA spec
- A mechanism for asserting identity was created in the Creator Assertions Working Group (CAWG) which is a separate entity
- All metadata assertions that could identify people or organisations were also moved
- In the 2.x spec there remains an option for validator tools to support “additional trust anchors”, but this is currently up to each implementor



C2PA Conformance program

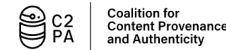
“The C2PA Conformance Program provides assurance that products *[i.e. hardware devices and software tools]* adhere to the Content Credentials specification, and fulfill a set of security requirements to ensure they are producing and validating C2PA data correctly.”

Introduces and manages the “C2PA Trust List” (specified in C2PA 2.0 spec) and sunsets the “Interim Trust List” currently being used.

Goals:

- Encourage ecosystem alignment with the 2.x specification
- Avoid unnecessary disruption for existing implementations
- Incentivize upgrades to C2PA 2.x
- Add Time Stamping Authorities to our Trust Lists

THE LINUX FOUNDATION PROJECTS



Conformance

The C2PA Conformance Program provides assurance that products adhere to the Content Credentials specification, and fulfill a set of security requirements to ensure they are producing and validating C2PA data correctly.

This Conformance Program is a risk-based, transparent and unbiased governance process intended to hold generator products, validator products and certification authorities accountable to the Content Credentials specification, the **Certificate Policy** and the **Security Requirements**. Conforming products are placed on a publicly accessible list. This conveys confidence in the implementation and its security to the public and guarantees interoperability across products in the Content Credentials ecosystem.

- Looking for more information? Read **Program Details** on GitHub.
- Interested in Participating? Fill out the **Expression of Interest form**.



C2PA Conformance program: Plan and Timeline

Through December 31, 2025:

The [Interim Trust List] will remain operational. During this time, new certificates will continue to be accepted and the Verify site will continue to display manifests as trusted, albeit with a disclaimer that these manifests were made with an older version of the trust model. The C2PA will strongly encourage adoption of the Conformance Program and the official C2PA Trust List.

January 1, 2026:

The [Interim Trust List] will be frozen. No new entries will be added, and no updates will be made.

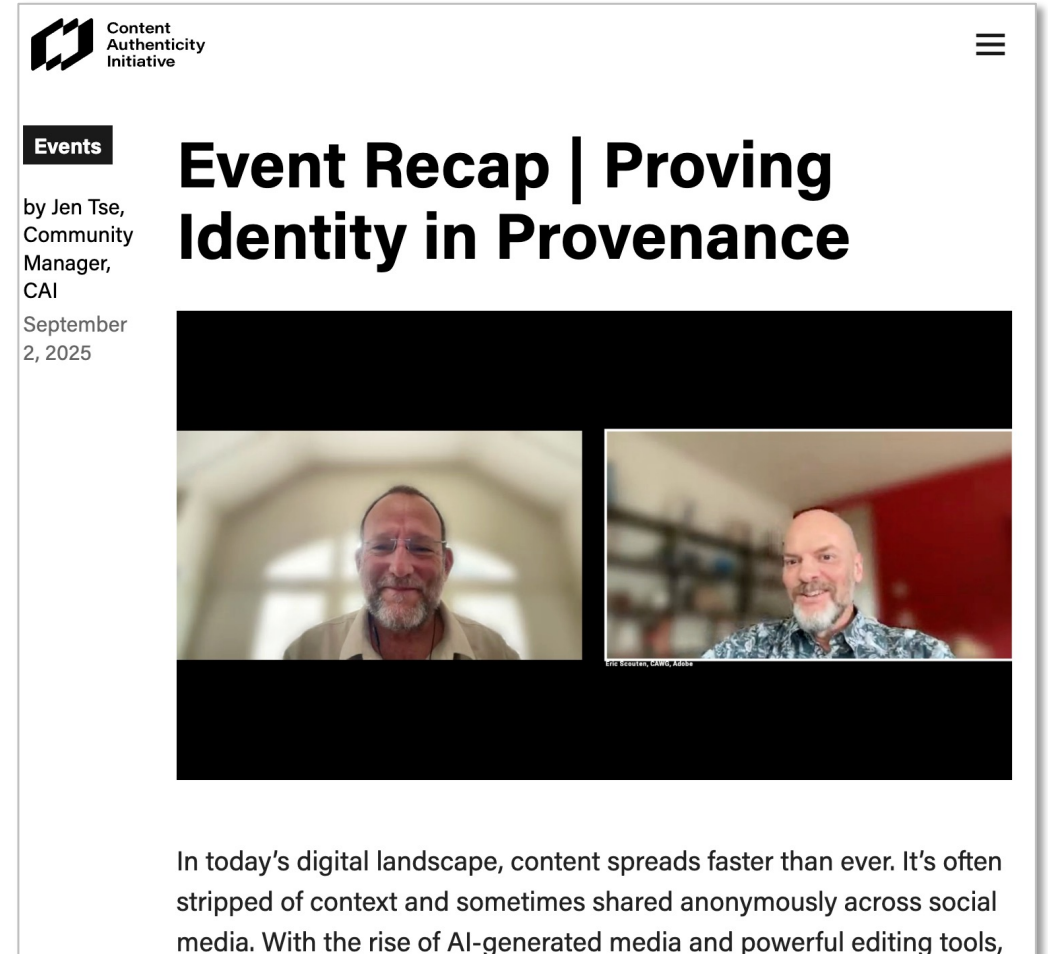
Existing certificates will remain valid for legacy support, but no future refreshes or additions will occur. Eventually, those certificates will expire and no longer be usable for signing. However, if content was signed during the ITL certificate's validity period, the content will always be considered valid against the legacy trust model.

Product Messaging

Just as the Verify site itself will do, Implementers are encouraged to begin distinguishing between Content Credentials using ITL-based certificates (typically tied to C2PA 1.4) and those from conforming products using the official C2PA TL.

CAWG and Identity Assertions

- Creator Assertions Working Group (CAWG.io) handles aspects that were removed from the main C2PA spec in version 2.0 in January 2024
- CAWG was initially a loose coalition but is now part of the Decentralised Identifier Foundation



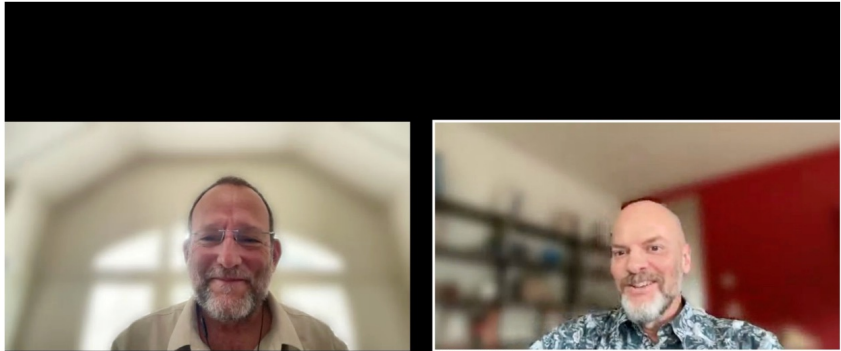
Content Authenticity Initiative

Events

by Jen Tse,
Community
Manager,
CAI

September
2, 2025

Event Recap | Proving Identity in Provenance




In today's digital landscape, content spreads faster than ever. It's often stripped of context and sometimes shared anonymously across social media. With the rise of AI-generated media and powerful editing tools,


[A recent CAI webinar describes CAWG's work in detail](#)





Mockups of how Identity Assertions might look in the Adobe Content Authenticity verifier tool




Contributor details ▾

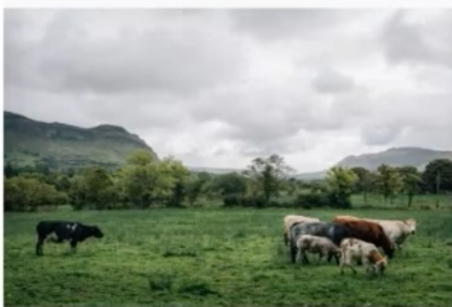
Name [Jane Smith](#) 

 Behance [Julie Smith](#)


 Instagram [juliesmith](#)

 I request that generative AI models not train on or use my content.



Content details >



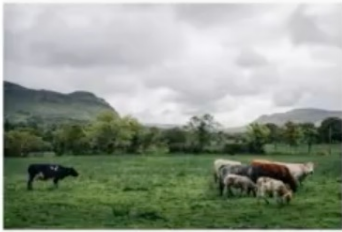
Publisher details ▾

 **BBC**
bbc.co.uk


Verified news media organization

 Origin Verified Publisher 

Content details >



Publisher details ▾

 **BBC**
bbc.co.uk



Title
Cattle Grazing Beneath Stormy Skies in County Sligo

Description
A group of cows graze in a green pasture surrounded by rolling hills and cloudy skies in a rural landscape, likely in a temperate region.

Credit
Photo by Jane McConnell / Reuters

Published on September 15, 2012

























Verified news media organization

 Origin Verified Publisher 

Content details >

Durable Content Credentials

- An obvious shortcoming is that all this signed metadata can simply be stripped out of the media file!
- So C2PA and CAI are looking at using watermarks and fingerprints to retrieve C2PA metadata
- CAI/Adobe has released [TrustMark](#), a simple open-source watermarking algorithm
- The identifier and the metadata still needs to be stored somewhere. Adobe has its own database.
- C2PA defines an algorithm for searching across multiple watermark systems

		Durable against metadata stripping	Durable against removal attacks	Strong cryptographic binding	Detectable on devices and apps	No network required
Metadata						
Fingerprint						
Watermark						
Combined						

Source: <https://contentauthenticity.org/blog/durable-content-credentials>



What are our next steps?

- Finalising best-practice guidelines for how metadata should be added to Verified News Publisher signed content
 - Workshops with publishers in Paris in April, Antibes in May, New York City in June, Bergen in September
- Work with C2PA on finalising organisational identity support
- 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](#)



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

[More details](#)



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



Thanks!

Brendan Quinn
mdirector@iptc.org