



Dutch Guild May 20th 2025

**From Source to Screen: Tracking
Truth with C2PA and Content
Credentials**

Fardau van Neerden



AGENDA



1. ABOUT ME



2. ABOUT ARBOR



3. WHY AI IS A RISK



4. WHAT IS C2PA



5. Q&A

SPEAKER

2005 – 2012 | Department of Justice - Technology Consultant
2012 – 2017 | RTL Nederland - Sr. System Engineer
2017 – 2025 | Microsoft - Cloud Solution Architect, Sr. Program Manager
2025 – present | Arbor - Product Owner



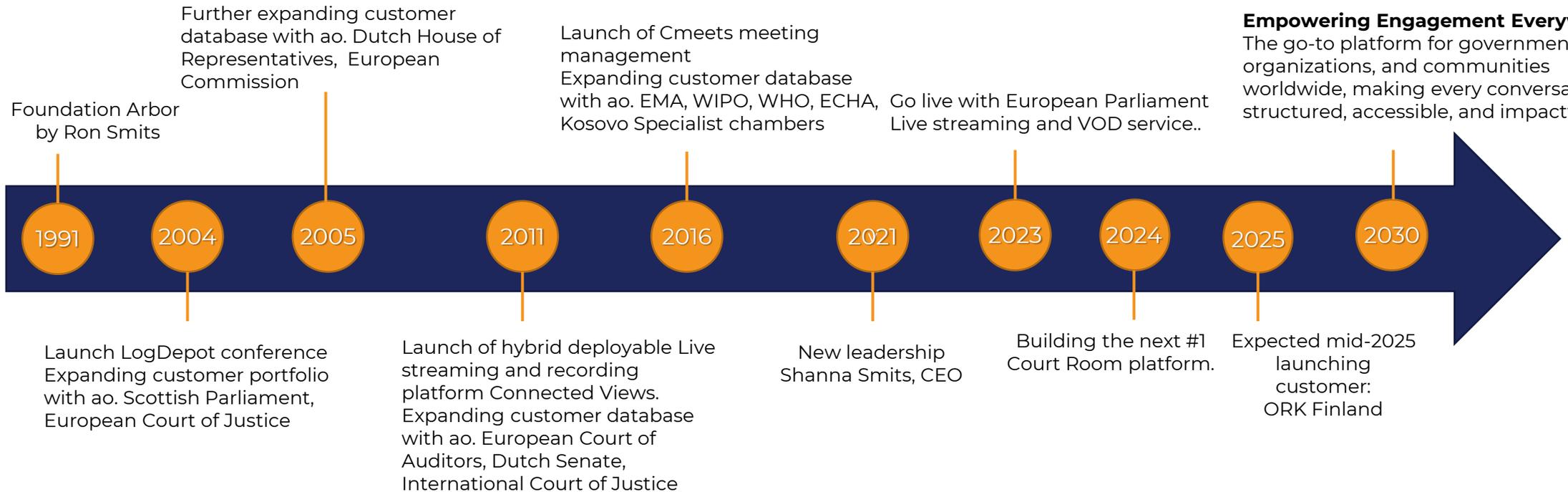
Fardau van Neerden
Product Owner



ABOUT ARBOR



OUR HISTORY, OUR TODAY AND OUR TOMORROW



STRUCTURED RECORDING/ARCHIVING AND WEBSTREAMING USER JOURNEY

- Simply create a new session to be recorded/streamed with a few clicks or connect with the meeting scheduling system.
- Prepare for the recording and webcast of the session your own way.

Prepare



- Full live control; correctly manage the parameters of a recording.
- Access restricted to certain people? No problem, a secure internal option is available.

Control and Manage



- Multitrack Audio available for multilingual audio requirements; participants and your audience can follow a listening meeting in the language of their choice.
- Integrated lossless recording and metadata capture

Capturing & record



- easy-to-access graphical interface for searching and reviewing archived records
- integrate content management for your video library of all past meetings.

Archive & playback



BRIDGING THE GAP: ENHANCING CITIZEN ENGAGEMENT IN GOVERNMENT OPERATIONS

Governments must uphold transparency, best achieved through seamless AV content sharing.



Live Streaming & Video on Demand (VOD):
Reliable distribution of official content.

Data Sovereignty & Security: Ensures content remains within managed infrastructure.

Regulatory Compliance: Meets accessibility and governmental IT requirements.

WHY AI IS A RISK



TRUST IN CONTENT SOURCE?

1. 2023 Slovak Election Deepfake

Example: Days before the Slovak parliamentary elections, a convincing deepfake audio clip circulated online, falsely portraying a prominent opposition politician discussing election rigging.

Relevance: No metadata, no traceable source—just viral misinformation.

Impact: Helped sway public opinion, highlighting how easily AI-generated content can destabilize democratic processes.

Slovakia's Election Deepfakes Show AI Is a Danger to Democracy

Fact-checkers scrambled to deal with faked audio recordings released days before a tight election, in a warning for other countries with looming votes.



PHOTOGRAPH: ZUZANA GOGDOVA/GETTY IMAGES



TRUST IN CONTENT SOURCE?

2. Fake Pentagon Explosion (2023)

Example: A deepfake image of an explosion near the Pentagon spread via verified Twitter accounts (now X), briefly causing panic and a dip in the stock market.

Relevance: The image looked like breaking news and was widely shared before it was debunked.

Impact: Showed how even a single AI-generated image, if not traceable, can manipulate markets and erode trust in real-time reporting.

Initial Reports of a Large Explosion near The Pentagon Complex in Washington D.C.



09:04 · 5/22/23 · 104K Views

TRUST IN CONTENT SOURCE?

3. Zelensky “Surrender” Deepfake (2022)

Example: A deepfake video showed Ukrainian President Volodymyr Zelensky urging troops to surrender to Russia. It was posted on hacked news platforms and spread on social media.

Relevance: The synthetic video exploited high-trust distribution channels.

Impact: Though quickly debunked, it illustrates how AV content pipelines can be weaponized if provenance isn't preserved.

TECHNOLOGY

Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn

MARCH 16, 2022 · 8:26 PM ET



Bobby Allyn



Ukrainian President Volodymyr Zelenskyy speaks to members of the U.S. Congress from Kyiv in this image from video provided by the Ukrainian Presidential Press Office and posted on Facebook.

AP

WHAT IS C2PA



C2PA

The **Coalition for Content Provenance and Authenticity** (C2PA) addresses the prevalence of misleading information online through the development of technical standards for **certifying the source and history** (or provenance) of media content. C2PA is a Joint Development Foundation project, formed through an alliance between Adobe, Arm, Intel, Microsoft and Truepic.

Founded in 2021

C2PA unifies the efforts of the Adobe-led [Content Authenticity Initiative \(CAI\)](#) which focuses on systems to provide context and history for digital media, and [Project Origin](#), a Microsoft- and BBC-led initiative that tackles disinformation in the digital news ecosystem.



C2PA - JOIN

Membership

Apply Now

Are you interested in joining C2PA to develop open standards that certify the source and provenance of online content? [Apply now](#) to join our incredible roster of members. [C2PA Introduction](#)

Apply Now

Steering Committee Members

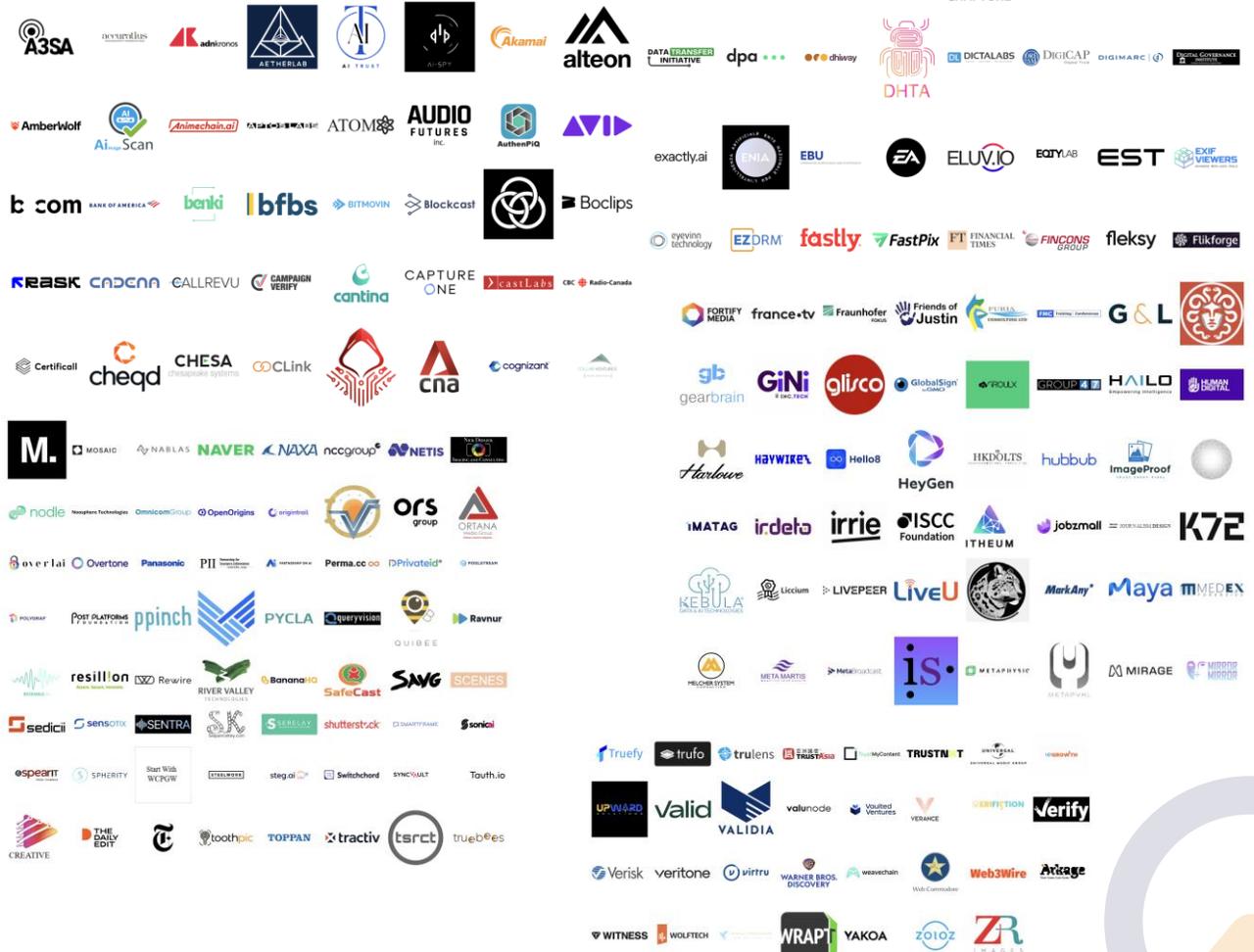


General Members



Contributor Members

Contributor Members



C2PA - PROVENANCE

- Provenance generally refers to the facts about the **history of a piece of digital content assets** (image, video, audio recording, document).
- Content Credentials enables the secure binding of statements of provenance data to instances of content. These provenance statements are called **assertions in a Content Credential**.
- Include assertions about **who** created the content and **how, when, and where** it was created.
- May also include assertions about **how it was edited** throughout its life.

What if provenance is not complete?

- For example, if an asset is cropped using a non-Content Credentials aware tool, the provenance data may not be updated to reflect that action.
- However, if the asset is then brought back into a Content Credentials aware tool for additional modification or preparation for publication, the Signer of the new Content Credential also implicitly attests to the crop action.
- So even though there is missing provenance information, the asset can still be trusted based on the Signer of the [active Content Credential](#).

It also allows to remove specific (PII) content due to local regulations



C2PA - PROVENANCE

Use-case Examples

- Helping consumers check the provenance of the media they are consuming
- Enhancing clarity around provenance and edits for journalistic work
- Offering publishers opportunities to improve their brand value
- Providing quality data for indexer / platform content decisions
- Assisting 'Intelligence' investigators to confirm provenance and integrity of media
- Enhance the evidentiary value of critical footage
- Enforcing disclaimer laws on retouched/edited images

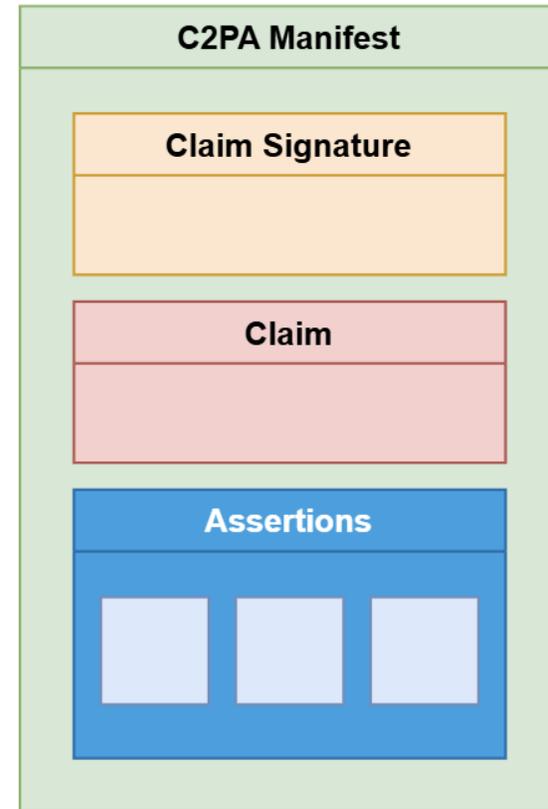


C2PA – TRUST IN CONTENT CREDENTIALS

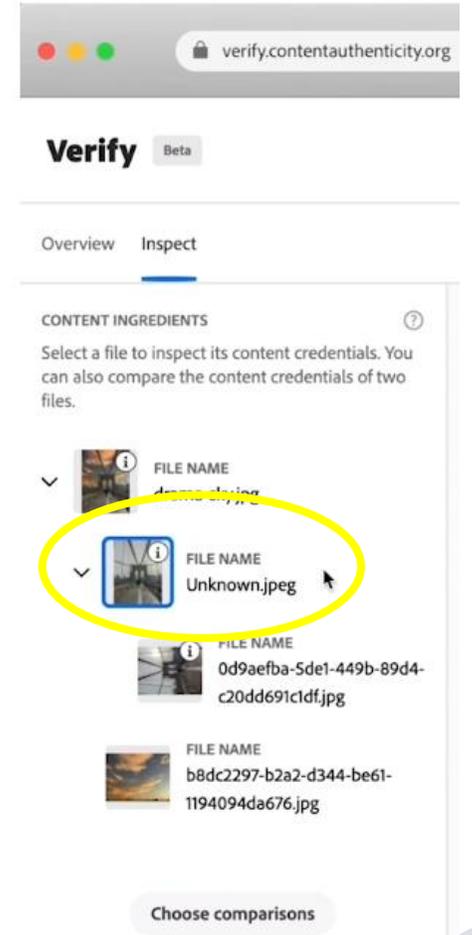
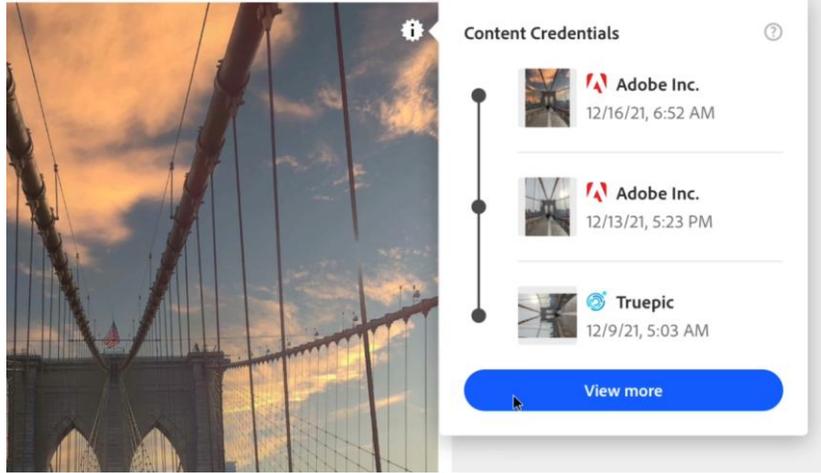
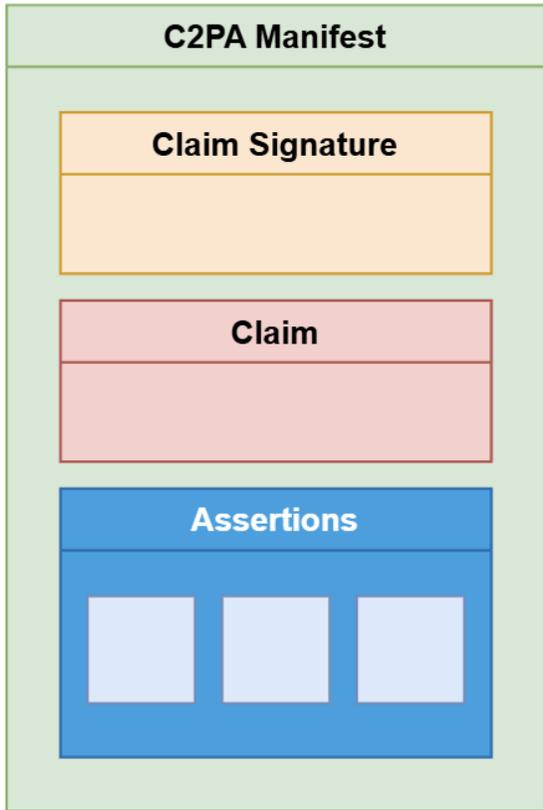
With Content Credentials, trust decisions are made by the consumer of the asset based on the Signer of the provenance data along with the information in the assertions contained in the provenance. **This signing takes place at each significant moment in an asset's life** (e.g., creation, editing, etc.) through the use of the Signer's unique credentials and ensures that the provenance data remains cryptographically bound to the newly created or updated asset.

Rely on Certificate Authorities

To enable consumers to make informed decisions about the provenance of an asset, and prevent unknown attackers from impersonating others, it is critical that each application and ecosystem reliably identify the owner of the signing credential (also known as a digital certificate) is issued. A certification authority (CA) performs this real-world due diligence to ensure signing credentials are only issued to verified entities. CAs that are recognized and trusted in a specific application or ecosystem are included in a trust list, which is a list of certification authorities that issue signing credentials for that application.



C2PA - TRUST



C2PA - TRUST

The screenshot displays the 'Verify' interface on the website `verify.contentauthenticity.org`. The page is split into three main sections: a left sidebar with metadata, a central image comparison, and a right sidebar with metadata.

Left Sidebar (Metadata for 'Unknown.jpeg'):

- CONTENT CREDENTIALS:** FILE NAME: Unknown.jpeg
- SIGNED BY:** Adobe Inc.
- SIGNED ON:** 12/13/21, 5:23 PM
- PRODUCED WITH:** Adobe Photoshop 23.0.2, Content Credentials (Beta)
- EDITS AND ACTIVITY:**
 - Color adjustments: Changed tone, saturation, etc.
 - Imported assets: Added images, videos, etc.
 - Size and position adjustments: Changed size, orientation, direction, or position
- ASSETS USED:**

Central Image Comparison:

The central image shows a side-by-side comparison of a suspension bridge. The left half is the original image, and the right half is the AI-edited version. A vertical white line separates the two, with a small icon in the center. The AI-edited version shows a significant color shift, with a warm, orange-gold glow over the sky and bridge, indicating the use of AI tools for color adjustment.

Right Sidebar (Metadata for 'drama-sky.jpg'):

- CONTENT CREDENTIALS:** FILE NAME: drama-sky.jpg
- SIGNED BY:** Adobe Inc.
- SIGNED ON:** 12/16/21, 6:52 AM
- PRODUCED WITH:** Adobe Photoshop 23.0.2, Content Credentials (Beta)
- EDITS AND ACTIVITY:**
 - AI tools: Edited with artificial intelligence or machine learning tools
 - Imported assets: Added images, videos, etc.
- ASSETS USED:**

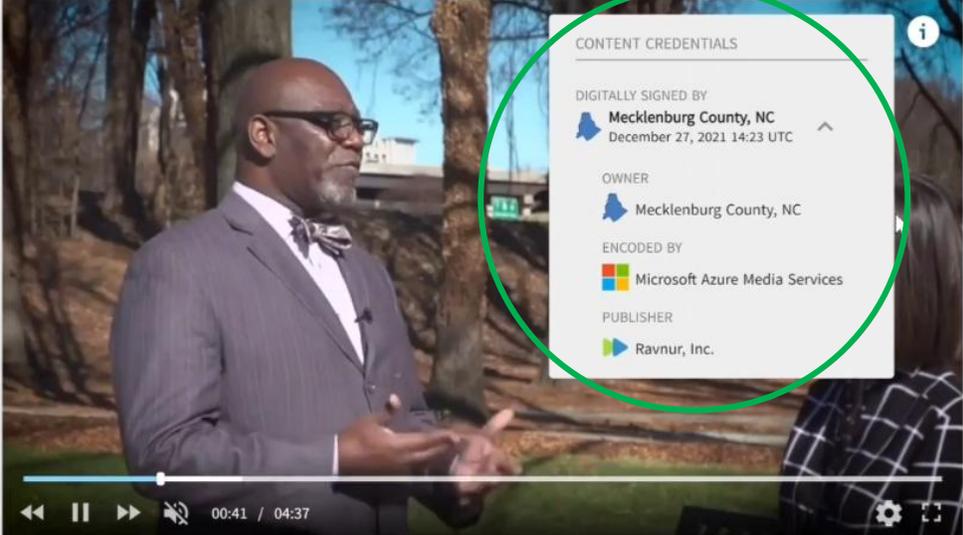


C2PA - TRUST



Mecklenburg County, North Carolina

Home > Video details



CONTENT CREDENTIALS

DIGITALLY SIGNED BY
Mecklenburg County, NC
December 27, 2021 14:23 UTC

OWNER
Mecklenburg County, NC

ENCODED BY
Microsoft Azure Media Services

PUBLISHER
Ravnur, Inc.

Board Of County Commissioners - 12 21 21

Home > Video details



CONTENT CREDENTIALS

Content credentials incomplete
January 11, 2022 18:20 UTC

DIGITALLY SIGNED BY
Mecklenburg County, NC
December 27, 2021 14:23 UTC

Board Of County Commissioners - 12 21 21



WHAT ABOUT AI AND C2PA? DO THEY BITE?



C2PA – TRUST IN AI

How does C2PA address the use of AI/ML in the creation and editing of assets?

Each action that is performed on an asset is recorded in the asset's Content Credentials. These actions can be performed by a human or by an AI/ML system. When an action was performed by an AI/ML system, it is clearly identified as such through its **digitalSourceType** field.

As an example, the `c2pa.created` action for an image created by a Generative AI model, might look like this, in CBOR Diagnostic Format (.cbordiag):

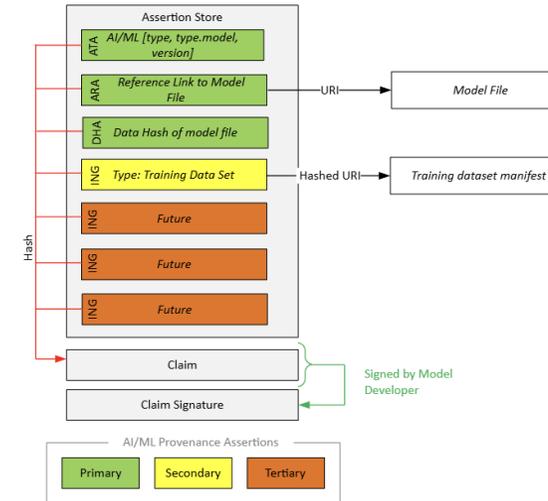
```
// an actions assertion used to describe output of Generative AI //
{
  "actions": [
    {
      "action": "c2pa.created",
      "when": 0("2023-02-11T09:00:00Z"),
      "softwareAgent" : {
        "name": "Joe's Photo Editor",
        "version": "2.0",
        "schema.org.SoftwareApplication.operatingSystem": "Windows 10"
      },
      "digitalSourceType": "http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia",
      "parameters" : {
        "ingredients" : [
          {
            "url": "self#jumbf=c2pa/joe-ed:urn:uuid:ABCD/c2pa.assertions/c2pa.ingredient__1",
            "alg": "sha256",
            "hash" : b64'...',
          },
          {
            "url": "self#jumbf=c2pa/joe-ed:urn:uuid:EFGH/c2pa.assertions/c2pa.ingredient__2",
            "alg": "sha256",
            "hash" : b64'...',
          }
        ]
      }
    }
  ]
}
```



C2PA – TRUST IN AI

How does C2PA address the use of AI/ML in the creation and editing of assets?

The Content Credential for an AI-ML model provides the consumer, e.g. a system operator designing an AI-ML system, with provenance and authenticity of the model. When the model is included as an ingredient in the Content Credential of the output of an AI-ML system, **the consumer of the output can check the validation state of the model and explore the model provenance to provide additional assurance that the output is trustworthy.**



```
JSON | 🗄️
/ Ingredient-1: Everything related to an OpenVINO Model TOPOLOGY FILE /
{
  "dc:title": "brain-tumor-segmentation-0001",
  "dc:format": "application/octet-stream",
  "relationship": "componentOf",
  "documentID": "uuid:87d51599-286e-43b2-9478-88c79f49c347",
  "instanceID": "uuid:7b57930e-2f23-47fc-affe-0400d70b738d",
  "data":
    { / hashed-ext-uri-map: Link to asset location (online) and asset hash /
      "url": "https://storage.openvino-toolkit.org/repositories/open_model_zoo/p",
      "alg": "sha256",
      "hash": "b64'Auxjtmx46cC2N3Y9aFmB09Jfay8LEwJWzBUTZ0sUM8gA='",
      "data_types": [ "c2pa.types.model.openvino.topology" ]
    }
}
```

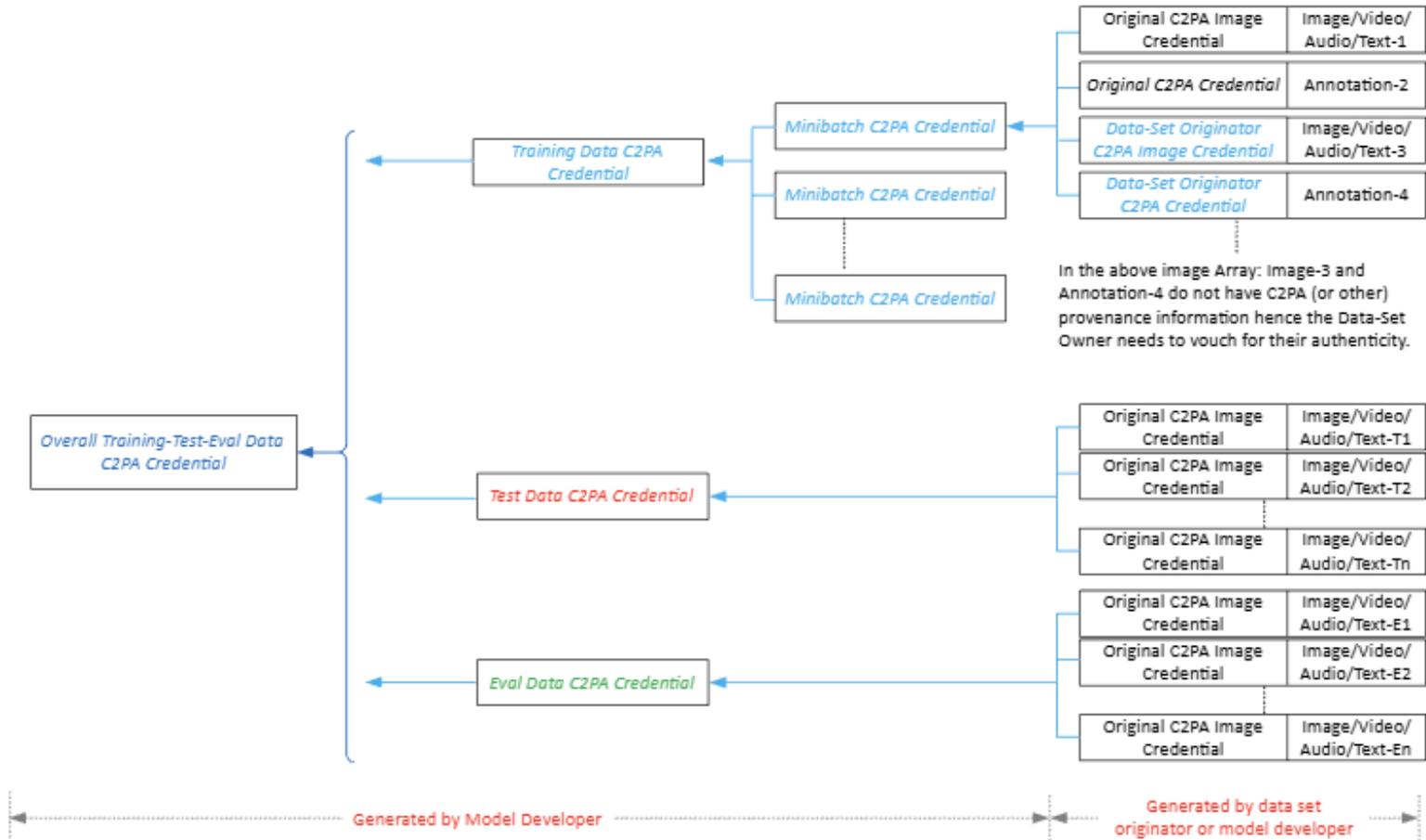
i.e. What model was used

```
/ Asset Type (OpenVINO Model) /
{
  "types": [
    {
      "type": "c2pa.types.model.openvino",
      "version": "2.11.0"
    }
  ]
}
```



C2PA – TRUST IN AI

The figure represents a possible credential for an AIML training data set that not only establishes the credentials of the overall training data set, but also it provides transparency for how the data set was used in the training process.



C2PA –WHERE ARE MANIFESTS STORED?

1. Embedded in the File (Bundled Storage)

- The C2PA manifest is **directly embedded** within the media file (e.g., JPEG, PNG, MP4).
- This is the preferred method for formats that **support metadata containers** (e.g., JPEG with EXIF/XMP, or MP4 atoms).
- This ensures the **manifest travels with the content**, making provenance information **tamper-evident and self-contained**.

2. Detached and Hosted Separately (Remote or Detached Storage)

- The manifest is **stored separately** and referenced via a **URI** or external link.
- Useful for formats or workflows where embedding is not feasible or desirable (e.g., streaming content, live feeds, proprietary formats).
- Enables **dynamic linking** and updates, but requires a trusted manifest store and access control.

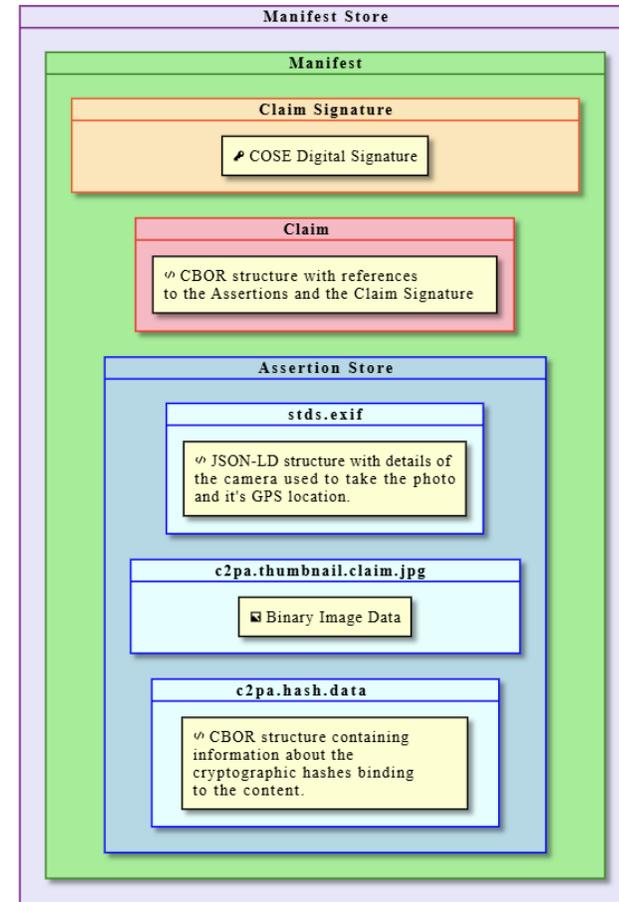


Figure 2. Example C2PA Manifest of a Photograph

CALL TO ACTION



CALL TO ACTION

- **Device Manufacturers and Software vendors (Apple/Google) to incorporate C2PA From Camera to Screen**
- **Content Creators and Distributors to unite and embrace C2PA initiatives during content lifecycle**
- **Media/News outlets to actively campaign Content Authenticity**
- **Create public wide awareness of content provenance and trust worthiness**
 - **Think about the “3x kloppen” campaign in The Netherlands. **Would we still trust non https?****

The image shows a website for the '3x Kloppen' campaign, which is a Dutch initiative for internet banking security. The website has a yellow background and features a navigation bar at the top with links for 'Home', 'Disclaimer', 'Veelgestelde vragen', and 'Nuttige links'. The main heading is 'VEILIG BLIJVEN INTERNETBANKIEREN' (Stay Safe Internet Banking). Below this is a large graphic with the text '3x KLOPPEN' and an icon of a hand pointing to three sun-like symbols. A video player shows a woman and a man, with a 'Bekijk volledige commercial' button. A central text block states: 'Banken zijn continu bezig de veiligheid van internetbankieren te waarborgen. Ook voor u is er een belangrijke rol weggelegd. Op deze website leert u in enkele eenvoudige stappen hoe ook u veilig kunt internetbankieren. Check of het klopt. Doe de test en druk op 'Start'.' Below this are three colored boxes, each with a sun icon and a question: 1. 'Klopt uw pc-beveiliging?' (Does your PC security check out?) with subtext: 'Voor veilig internetbankieren moet uw computersoftware helemaal up-to-date zijn. Dat geldt voor uw besturingssysteem, uw internetbrowser en uw beveiligingssoftware. Check deze software regelmatig.' 2. 'Klopt de website?' (Does the website check out?) with subtext: 'Als u de website van uw bank bezoekt, gaat dat automatisch via een beveiligde verbinding. Deze verbinding draagt bij aan veilig internetbankieren. Check altijd of de website echt van uw bank is.' 3. 'Klopt uw betaling?' (Does your payment check out?) with subtext: 'Bent u ingelogd op de website van uw bank. Voer dan de betaling uit volgens de instructies van uw bank. Als u de betaling correct uitvoert, weet u dat u veilig bankiert. Check daarom altijd uw bij- en afschriften.' A 'Start' button with a right arrow is located to the right of the central text.

CALL TO ACTION



Today the Coalition for Content Provenance and Authenticity (C2PA) is introducing the new and official Content Credentials “icon of transparency,” a mark that will provide creators, marketers and consumers around the world with the signal of trustworthy digital content.

c2pa.org



THANK YOU

Arbor Media B.V.
Gildenbroederslaan 2
7005 BM Doetinchem
The Netherlands

 31 314 399 055

 978 675 5437

 info@arbor.nl

 www.arbor.nl



ARBOR
WE EMPOWER ENGAGEMENT