

Christopher E. Hanba (*pro hac vice*)
 Email: chanba@dickinson-wright.com
 Joshua G. Jones (*pro hac vice*)
 Email: jjones@dickinson-wright.com
 DICKINSON WRIGHT PLLC
 607 W. 3rd Street, Suite 2500
 Austin, Texas 78701
 Telephone: (512) 770-4200
 Facsimile: (844) 670-6009

Eric M. Schiffer
 Email: eschiffer@schifferapc.com
 SCHIFFER, APC
 7545 Irvine Center Drive, Suite 200
 Irvine, CA 92618
 Telephone: (949) 533-0485

Attorneys for Plaintiff
Jonathan E. Jaffe

[Additional counsel listed on signature page]

**UNITED STATES DISTRICT COURT
 CENTRAL DISTRICT OF CALIFORNIA**

JONATHAN E. JAFFE, an individual

Plaintiff,

v.

ADOBE, INC.
 a Delaware corporation

Defendant.

Case No. 2:23-cv-06224-JWH-MAA

**PLAINTIFF JONATHAN E. JAFFE’S
 FIRST AMENDED COMPLAINT FOR
 PATENT INFRINGEMENT**

JURY TRIAL DEMANDED

Plaintiff Jonathan E. Jaffe (“Jaffe”) files this First Amended Complaint for Patent Infringement and Demand for Jury Trial against Adobe, Inc. (“Adobe”) for infringement of United States Patent No. 6,757,828 (the “’828 Patent”). A redline copy comparing Jaffe’s First Amended Complaint for Patent Infringement with Jaffe’s Original Complaint for Patent Infringement (Dkt. 1) is attached as Exhibit A.

THE PARTIES

1. Plaintiff Jonathan E. Jaffe is an individual who currently resides in Gallatin, TN.

2. Defendant is a Delaware corporation with its principal place of business located at 345 Park Avenue, San Jose, CA 95110. It has been served and has appeared in this case.

JURISDICTION AND VENUE

3. This is an action for patent infringement arising under the patent laws of the United States, Title 35, United States Code, including 35 U.S.C. §§ 154, 271, 281, and 283-285.

4. This Court has exclusive subject matter jurisdiction over this case for patent infringement under 28 U.S.C. §§ 1331 and 1338.

5. Adobe is subject to the general and specific personal jurisdiction of this Court, based upon its regularly conducted business in the State of California and in the Central District of California (“District”), including conduct giving rise to this action including at least by making, using, offering to sell, selling, or putting into service the accused products, systems, or services within the District, thus committing, acts of infringement within the District, and placed infringing products, systems, or services into the stream of commerce knowing or understanding that such products, systems, or services would be used in the Central District of California.

6. Venue is proper in this Court under 28 U.S.C. §§ 1400(b) because a substantial part of the events or omissions giving rise to these claims occurred in this district and because Adobe has a regular and established place of business in this District located at 3640 Holdrege Ave, Los Angeles, CA 90016.

THE ’828 PATENT

7. Mr. Jaffe is the co-inventor and owner of United States Patent No. 6,757,828 (the “’828 Patent”) titled “Indigenous authentication for sensor-recorders and other information capture devices” including the right to sue for all past infringement. A true and correct copy of the ’828 Patent is attached at Exhibit B.

8. The ’828 Patent issued from U.S. Patent Application No. 09/626,044 filed on July 27, 2000.

1 9. The Patent Office issued the '828 Patent on June 29, 2004, after a full and fair
2 examination.

3 10. The '828 Patent was valid until its expiration on July 3, 2022.

4 11. The '828 Patent relates to a method and apparatus for acquiring and recording a
5 sample of an environment in order to provide authentication for sensor-recorders and other
6 information capture devices.

7 12. The inventors of the '828 Patent recognized that, in digital environments, there is
8 great potential for alteration of images, data files, audio and video recordings, and other data
9 streams. Indeed this problem has become even more pronounced in recent years with the increase
10 in generative artificial intelligence.

11 13. The '828 Patent provides several advantages over the prior art because the
12 invention does not require that one know which device was used to create a digital file prior to
13 authenticating a given data file and, additionally, encryption is not required for authentication
14 which decreases manufacturing costs for information storage devices.

15 14. The '828 Patent describes and claims a specific way to authenticate digital files by
16 using aspects of the environment in which the digital file was created including, but not limited to,
17 date, time, latitude, longitude, altitude, roll, pitch, yaw, and compass heading.

18 15. Claim 1 of the '828 Patent reads:

19 1. A method for authenticating a data stream stored in a data file in memory,
20 said method comprising the steps of:
21 storing a data stream in a data file in a memory;
22 utilizing a sensor, which is tightly coupled to said memory, to generate at
23 least one internal and unique parameter;
24 monitoring the integrity of the tight coupling between said memory and said
25 sensor when said at least one internal and unique parameter is generated,
26 and, if said integrity is compromised, then also providing an indication of
27 said compromised integrity;
28 utilizing a signature protocol to generate a first signature based on said data
stream and said at least one parameter, said first signature being generated
without altering said data stream and being appended to said data file in said
memory;
utilizing said signature protocol to generate a second signature based on said
image;
comparing said first signature to said second signature,

1 if said first and second signatures are not the same, then generating an error
2 signal that is displayed to a user to indicate that said stored data stream is
not authentic, and

3 if said first and second signatures are the same, then generating an ok signal
4 that is displayed to a user to indicate that said stored data stream is authentic.

ADOBE

5 16. Upon information and belief, Adobe is a multinational software company founded
6 in 1982.

7 17. Upon information and belief, Adobe has more than 29,000 employees and earned
8 approximately \$17.6 billion in revenue in 2022.

9 18. Adobe sells ubiquitous software products throughout the world including Acrobat
10 and Photoshop.

COUNT I – INFRINGEMENT OF THE '828 PATENT

11 19. Mr. Jaffe repeats, realleges, and incorporates by reference, as if fully set forth
12 herein, the allegations of the preceding paragraphs, as set forth above.

13 20. Adobe makes, uses, offers to sell, and sells in the United States products, including
14 content attribution tools, also called “content credentials” within its Creative Cloud suite of
15 software products, launched the Content Authenticity Initiative which is a standard for digital
16 content provenance, and cofounded the Coalition for Content Provenance and Authenticity
17 (C2PA) technical standard for content provenance (the “Accused Products”).

18 21. The C2PA unifies the efforts of the Adobe-led Content Authenticity Initiative
19 (CAI) which focuses on systems to provide context and history for digital media.

20 The Coalition for Content Provenance and Authenticity (C2PA) is a [Joint Development Foundation](#) project that brings together the efforts
21 of the [Content Authenticity Initiative \(CAI\)](#) and [Project Origin](#).

22 Founded in late 2019 by Adobe in collaboration with the New York Times and Twitter, the CAI is building a system to provide to provide
23 provenance and history for digital media, providing a tool for creators to claim authorship while empowering consumers to make informed
24 decisions about what to trust. Project Origin, founded in 2019 by BBC, CBC Radio Canada, Microsoft and the New York Times, focuses on
25 tackling disinformation in digital news by defining an end-to-end process for publishing, distribution and attaching signals to a content to
26 demonstrate its integrity.

27 <https://c2pa.org/about/about/>

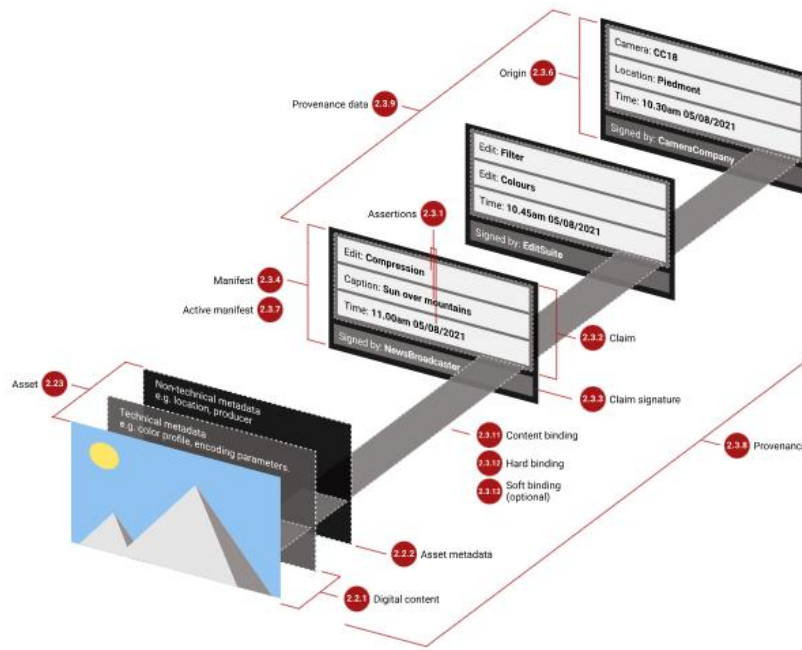


Figure 3. Elements of C2PA

https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_introduction

22. According to the C2PA, “[t]he C2PA binds the efforts of these two groups and focuses exclusively on the development of open, global technical standards to channel the content provenance efforts of the CAI and Project Origin. C2PA is tasked with: Documenting workflow requirements as informed by CAI, Project Origin and other partner organizations, Applying those requirements in development of content provenance specifications, Developing best practices and reference designs for applying those standards, Promoting selected specifications to become global standards, Promoting global adoption of digital provenance techniques, Promoting adoption of digital Coalition’s specifications and standards by social and media platforms, Ensuring content remains accessible even with digital provenance techniques applied.”

<https://c2pa.org/about/about/>

23. The C2PA specification “power[s] Content Credentials for digital content attribution in Adobe tools like Photoshop, which was announced as a public beta at Adobe MAX 2021.” <https://blog.adobe.com/en/publish/2022/01/26/cp2a-1spec-adobeblogv1>

24. Upon information and belief, the Accused Products implement the CAI through the C2PA. The Accused Products include Adobe products (standalone and/or mobile applications, i.e., “apps”) utilizing content authenticity, including but not limited to at least Adobe Behance, Adobe Capture, Adobe Creative Cloud, Adobe Darkroom, Adobe Lightroom, Adobe Lightroom Photo & Video Editor, Adobe Lightroom Classic, Adobe Premiere Pro, Adobe Photoshop, Adobe Photoshop Camera, Adobe Photoshop Express, Adobe Photoshop Camera, and Adobe Scan.

The Content Authenticity Initiative unveils content attribution tool within Photoshop and Behance

Today, we are unveiling a preview of our attribution tool in Adobe Creative Cloud. This feature will be available to select customers in pre-release within Photoshop and Behance in the coming weeks. The tool is built using an early version of the open standard that will provide a secure layer of tamper-evident attribution data to photos, including the author’s name, location and edit history. This will help consumers better understand the content they view online and give them greater confidence to evaluate its authenticity.

Content Attribution Tool, <https://blog.adobe.com/en/publish/2020/10/20/content-authenticity-initiative-unveils-content-attribution-tool-within-photoshop-behance.html#gs.x05anq>

25. The Accused Products employ a method for authenticating a data stream stored in a data file in memory. The Accused Products support authentication of media stored in a mobile device, camera, desktop computer, and in the cloud.

Why use Content Credentials?

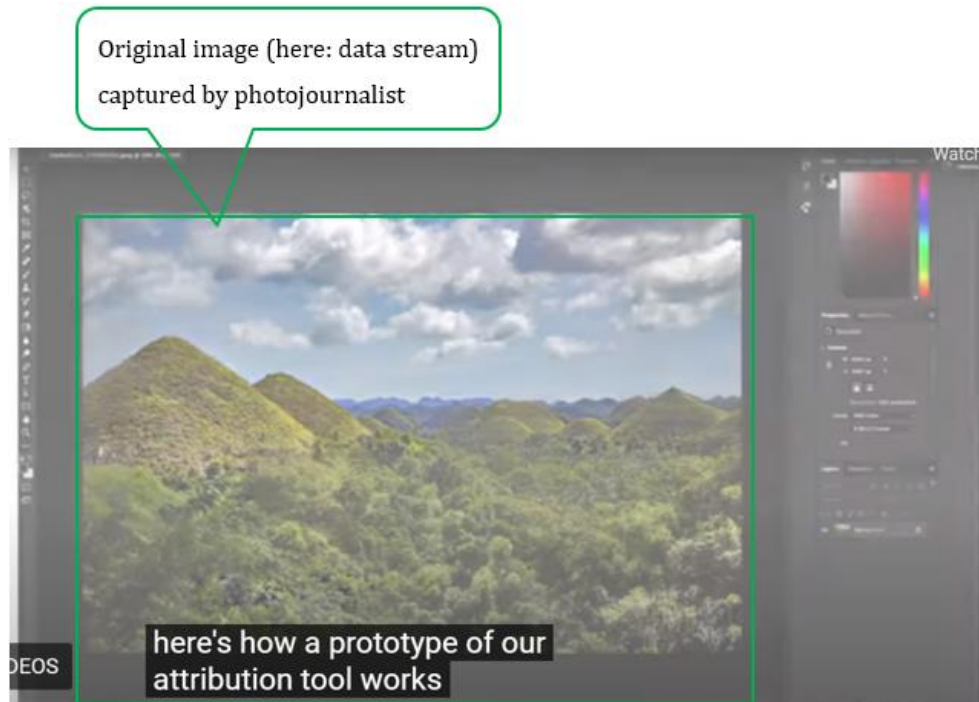
Using Content Credentials is an easy way to share content transparently. It can help build credibility and trust with viewers by sharing more information about yourself and your creative process. It can also help prevent the spread of misinformation and disinformation online.

Content Credentials allow you to attach your identity and contact information to your work, giving people more ways to find and connect with you when they encounter your content online. You can also attach important usage details to your content, including whether or not you want Content Credentials-supported AI models to use your content for training purposes.

<https://helpx.adobe.com/creative-cloud/help/content-credentials.html>

26. The Accused Products store a data stream in a data file memory. For example, Adobe Photoshop captures/retrieves images on a mobile device, camera, desktop computer, and

the cloud. The captured photos are backed up to the memory and must be stored in the device's memory or on the cloud server's memory.



Content Attribution Tool, <https://blog.adobe.com/en/publish/2020/10/20/content-authenticity-initiative-unveils-content-attribution-tool-within-photoshop-behance>

How are Content Credentials stored and recovered?

Content Credentials can be stored and recovered in three ways:

Attached directly to their respective files This increases file sizes but can keep your Content Credentials more private. Attached Content Credentials are less resilient and can be stripped from your content when published or shared online.

Published to the Content Credentials cloud This method reduces file sizes and improves their resiliency. If they're ever stripped from your content, they can be recovered with [Verify](#). In Verify, your published Content Credentials may appear as possible matches for content that is visually similar to your own.

- Adobe's Content Credentials cloud is a public, persistent storage solution for your Content Credentials, separate from the cloud file storage included in your Adobe plan.
- If Content Credentials are missing after your content is published online, the platform you're using likely doesn't yet support Content Credentials. If you post your Content Credentials to the Content Credentials cloud, they can be recovered on [Verify](#).

<https://helpx.adobe.com/creative-cloud/help/content-credentials.html>

1 27. The C2PA standard specifies that assertion data (e.g. data about when, where and
2 how an asset or digital file was created), may be embedded with the assertion data itself on the
3 device or stored externally in the cloud. A device, such as a mobile device, camera, or desktop
4 computer has memory in which data files, such as images, are stored, as well as assertion data. In
5 addition, cloud servers also have memory to store data files such as images and assertion data.

6 **19.10. Cloud Data**

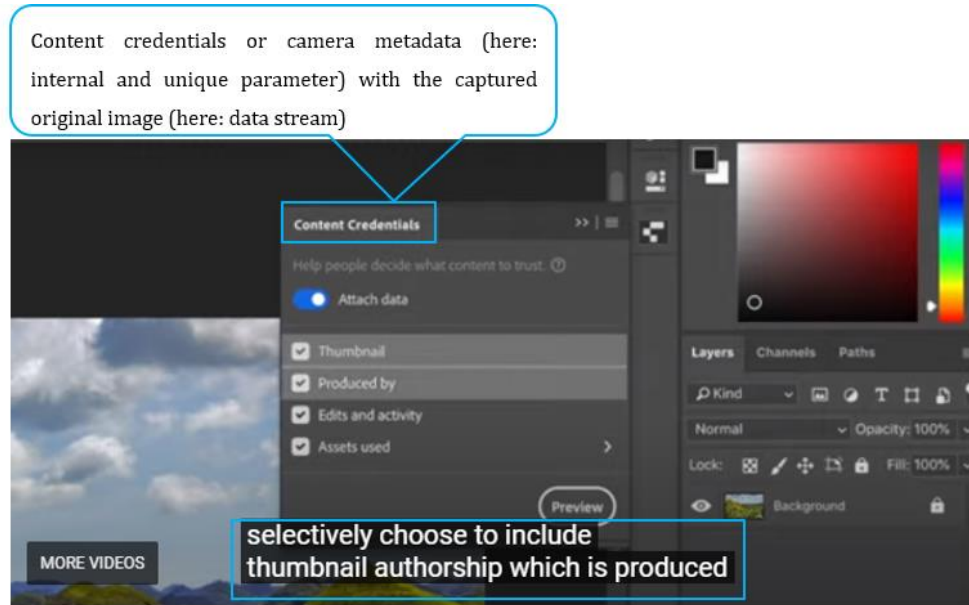
7 There are use cases where storing the data for the assertion remotely, such as in the cloud, is better than em-
8 bedded inside the asset, especially when the data is large. For any such cases, it is possible to use a special type
9 of assertion that serves as a reference to that information. For privacy and reliability reasons, data referenced
10 through a Cloud Data assertion shall be considered optional: their contents should not be retrieved as part of
11 manifest validation. A validator may retrieve the contents later to serve an application-dependent need, such as
further exploration of the provenance history.

12 https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_cloud_data

13 28. The Accused Products utilize a sensor, which is tightly coupled to said memory, to
14 generate at least one internal and unique parameter. Such a sensor could include, but is not limited
15 to a GPS receiver in a camera or mobile device, a digital image sensor which captures a photo in
16 a camera or mobile device, or a processor that captures camera or mobile device metadata. Upon
17 information and belief, a sensor could also include temperature sensors such as ring oscillators,
18 which use a random salt for cryptographic hashing, and thermal energy sensors. The Accused
19 Products define an “actor” as “a human or hardware or software product” which includes hardware
20 such as a camera, “image editing software, cloud service, or the person using such tools.” These
21 actors all utilize a sensor according to the patented method. In one example, the Accused Products
22 capture/retrieve an image by utilizing a sensor on a mobile device, camera, desktop computer, and
23 the cloud. In another example, hardware devices such as a camera or mobile phone contain sensors
24 which store image files in memory. The Accused Products, which include image editing software,
25 utilize a sensor when the image is loaded into the program and tamper evident edits are made to
26 the image. The Accused Products must utilize the hardware camera sensor that is tightly coupled
27 to the memory of the mobile device, camera, desktop computer, and the cloud computing device

28

where the hardware camera sensor captures the image which is stored in the mobile device, camera, desktop computer, and cloud computing device memory.



Source: Content Attribution Tool, <https://blog.adobe.com/en/publish/2020/10/20/content-authenticity-initiative-unveils-content-attribution-tool-within-photoshop-behance>

Where does CAI data live?

A piece of content's CAI data can either be embedded into the file itself, or stored in Adobe's Content Credentials cloud. Adobe's Content Credentials cloud is a public, persistent storage option for your attribution and history data. Publishing to this cloud will help keep your files smaller and make their Content Credentials more resilient and recoverable.

<https://contentauthenticity.org/faq>

Example uses

Numerous Adobe tools and products implement Content Credentials. You can optionally attach credentials to images you create or modify using Photoshop and Lightroom. Additionally, all images created using the Firefly generative AI tool automatically have attached Content Credentials. Behance displays Content Credentials if they are attached to media shared on the site, and still images provided through Adobe Stock automatically have Content Credentials attached.

<https://opensource.contentauthenticity.org/docs/getting-started/>

Actor: A human or hardware or software product. For example, a camera, image editing software, cloud service, or the person using such tools.

<https://opensource.contentauthenticity.org/docs/getting-started/>

29. Adobe's mobile applications also utilize the camera sensor of a mobile device by allowing a user to capture digital photos directly from the mobile application to be selected and edited by the mobile application.

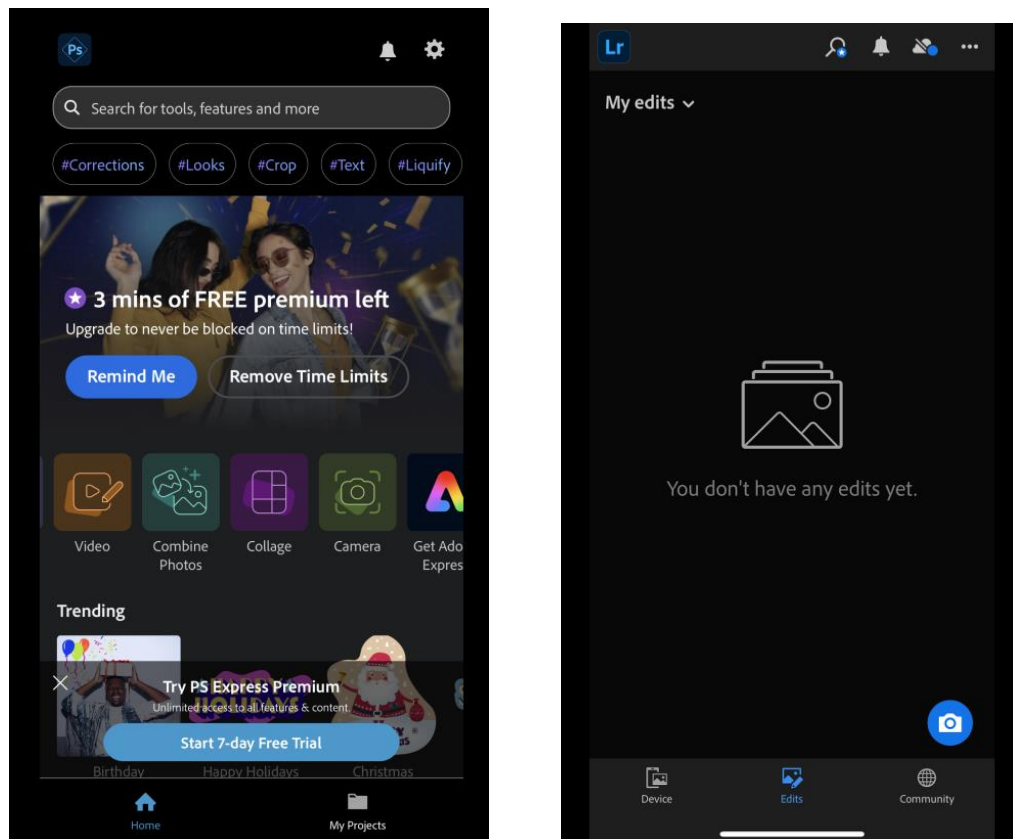
View and select photos

Launch the app and select the photo that you want to work with. The first screen displays photos from your device's memory.

Alternatively, you can click a photograph using the app and work with it right away. To do this choose **Capture** from the **Home** screen.

<https://helpx.adobe.com/photoshop-express/get-started-ios.html>

30. The following represents screen captures of two such Adobe mobile applications, showing the ability to capture images through the mobile camera:



31. The Accused Products also utilize a sensor when Content Credentials are used on compatible cameras that implement the C2PA standard such as Leica and Nikon.

1 [https://news.adobe.com/news/news-details/2022/Adobe-Partners-With-Leica-and-Nikon-To-](https://news.adobe.com/news/news-details/2022/Adobe-Partners-With-Leica-and-Nikon-To-Implement-Content-Authenticity-Technology-Into-Cameras/default.aspx)
 2 [Implement-Content-Authenticity-Technology-Into-Cameras/default.aspx](https://news.adobe.com/news/news-details/2022/Adobe-Partners-With-Leica-and-Nikon-To-Implement-Content-Authenticity-Technology-Into-Cameras/default.aspx)

3 32. The C2PA standard specifies that actors (e.g. hardware or software that participates
 4 in the C2PA standard such as a camera, image editing software, or cloud service) utilize sensors
 5 to create assertion data about an asset such as a digital image. Assertions can include information
 6 such as camera information such as maker and lens of the camera, as well as location information
 7 and pixel data such as an image thumbnail.

8 https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_glossary;
 9 https://c2pa.org/specifications/specifications/1.2/guidance/Guidance.html#_assertions;
 10 https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_assertions

11 33. The technical metadata in image files captured by the digital camera and/or
 12 smartphone sensor are stored in Exchangeable image file (Exif) format. Such technical metadata
 13 captured by the sensor and stored in Exif format include, but are not limited to device make and
 14 model, shutter speed, ISO number, date and time of capture, location.

15 **Exif assertion**

16 Exchangeable image file (Exif) format is a standard for storing technical metadata in image files of JPEG, TIFF, PNG, and
 17 other formats. Most digital cameras (including smartphones), scanners and other digital capture devices use Exif to store
 18 information such as device make and model, shutter speed, ISO number, date and time of capture, location, and so on.
 19 For more information on Exif, see the [Exif specification](#).

20 <https://opensource.contentauthenticity.org/docs/manifest/assertions-actions#exif-assertion>

21 34. The Accused Products specify that Exif information can be added to an asset (a
 22 digital media file or stream of data) in a way to validate the asset cryptographically.

1 Use an Exif assertion to add Exif information to the asset in a way that can be validated cryptographically. An Exif
 2 assertion has the label `stds.exif`.

3 Here is a simple example:

```

4  "assertions": [
5    ...
6    {
7      "label": "stds.exif",
8      "data": {
9        "@context" : {
10         "exif": "http://ns.adobe.com/exif/1.0/"
11       },
12       "exif:GPSVersionID": "2.2.0.0",
13       "exif:GPSLatitude": "39,21.102N",
14       "exif:GPSLongitude": "74,26.5737W",
15       "exif:GPSAltitudeRef": 0,
16       "exif:GPSAltitude": "100963/29890",
17       "exif:GPSTimeStamp": "2019-09-22T18:22:57Z"
18     }
19    ...
20  ]
  
```

21 <https://opensource.contentauthenticity.org/docs/manifest/assertions-actions>

22 35. The sensor is tightly coupled to said memory given that the metadata created by the
 23 sensor, such as a hardware camera sensor, whether on a mobile phone or another camera device,
 24 is “tamper evident” according to the Content Authenticity Initiative and the C2PA standard. Each
 25 manifest that is assigned to an asset, such as a digital image, is digitally signed and stored in
 26 memory and cannot be altered without also changing the unique “fingerprint” of the metadata
 27 stored.

28 The CAI uses *cryptographic asset hashing* to provide verifiable, tamper-evident signatures that the asset and metadata
 haven't been altered since the asset was published with the attached manifest. This means that a hash function converts
 the digital asset data to a unique “fingerprint,” which is signed using a certificate. Once the credentials are signed, if the
 asset is changed then its fingerprint also changes. That's why it's called “tamper evident.” You're not prevented from
 changing an image that has Content Credentials, but if you do, the credentials are no longer valid unless you change it
 using a tool that updates and re-hashes the credentials, along with a timestamp and optionally a description of what
 changed. The C2PA specification refers to this as *hard binding*.

<https://opensource.contentauthenticity.org/docs/getting-started/>

28

36. The Accused Products add the tamper evident metadata to imported digital photos and also create tamper evident digital photos that include the metadata automatically when the photo is created by Adobe's mobile applications' utilization of a mobile device camera or when an Adobe partnered camera that implements Content Credentials and the C2PA standard is used.

What information is included?

The following non-personal identifiable information is always included in Content Credentials automatically applied to assets generated with Adobe Firefly features:

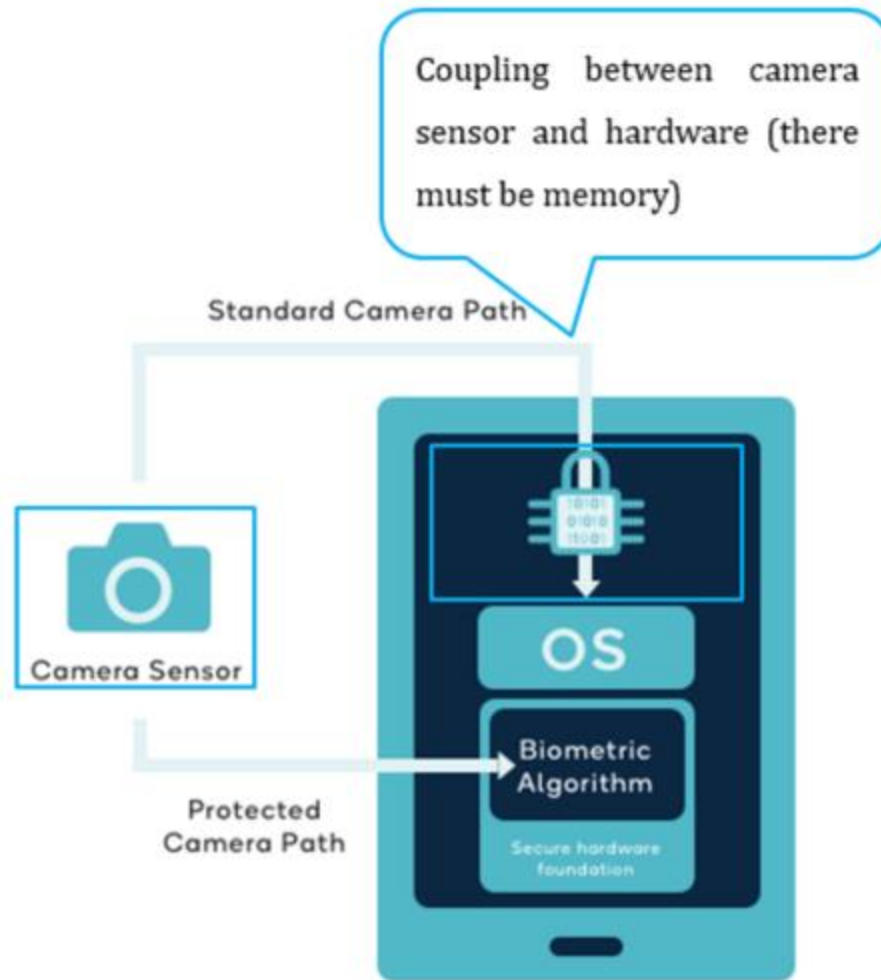
- **Output thumbnail:** visual thumbnail of the output; displays only for outputs generated using the Text to Image feature in the Firefly web app
- **Issuer:** Adobe Inc., the organization responsible for issuing the Content Credential
- **Content summary:** a notice that Adobe generative AI was used in the creation of the asset
- **App or device used:** the Adobe software application or hardware device used to produce the asset
- **AI tool used:** the Adobe generative AI tool used
- **Actions:** the general editing and processing actions taken to produce the asset. Only "Created" or "Other edits" actions will be listed for assets generated with Adobe Firefly features.

<https://helpx.adobe.com/firefly/using/content-credentials.html>

<https://news.adobe.com/news/news-details/2022/Adobe-Partners-With-Leica-and-Nikon-To-Implement-Content-Authenticity-Technology-Into-Cameras/default.aspx>

37. In addition, the camera sensor of, for example, a mobile device, is tightly coupled to the hardware and, therefore, the memory of the device.

28



<https://www.qualcomm.com/products/features/mobile-security>

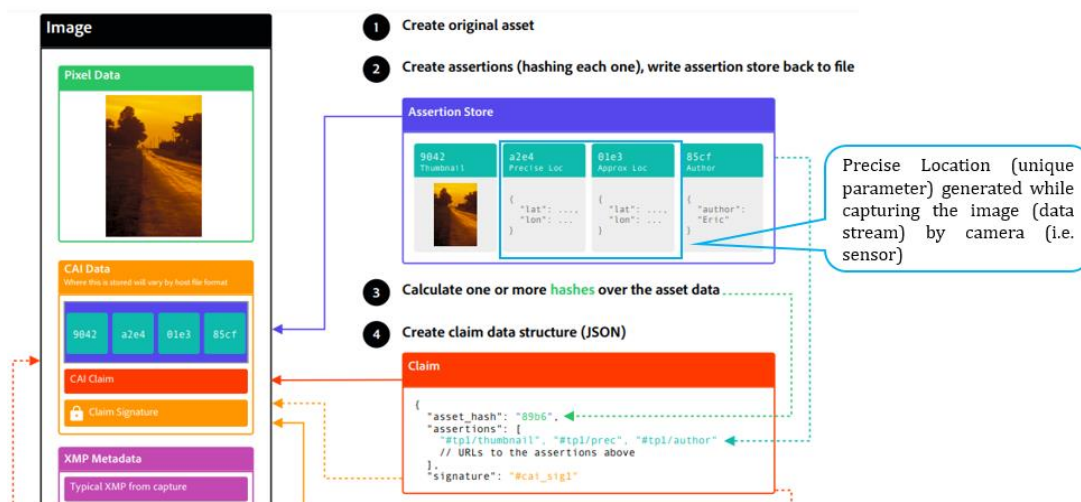
38. The Accused Products utilize Exif technical metadata which is stored in the memory of a digital camera, smartphone, and other digital capture devices which further demonstrates the sensor capturing such Exif information is tightly coupled to the memory of the hardware device. Cameras compatible with the C2PA standard, such as made by Leica and Nikon in partnership with Adobe, have a tight coupling between the camera sensor and the memory of the camera and Exif information stored in the memory of the camera.

<https://news.adobe.com/news/news-details/2022/Adobe-Partners-With-Leica-and-Nikon-To-Implement-Content-Authenticity-Technology-Into-Cameras/default.aspx>

39. The internal and unique parameters include elements such as GPS (latitude and longitude), information about the camera or device such as the maker of the camera or lens, and/or the date and time of the image and assertion data as specified in the C2PA standard.

1. A capture device captures an image and concurrently creates a set of assertions about the image such as capture location, equipment details, identity of the user, and perhaps a representative thumbnail. These assertions are embedded in the asset.

Not all information in CAI claims is the same. Each has different dependencies and potential vulnerabilities. For instance, on-device camera information (such as lens used) is different from creation date or location information which is dependent on an external signal (e.g. clock or GPS). An optimal UX for viewers will indicate this, through progressive disclosure, without overly complicating the experience.



CAI,

Whitepaper,

<https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascde%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19;>

https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_assertions

40. The Accused Products monitor the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity. For example, the Accused Products must capture an image through a camera sensor in the hardware

1 and the captured image is stored in the hardware memory. The Accused Products detect the un-
 2 authentic data and prevent security tampering. The integrity of the tight coupling between the
 3 memory and the sensor must be monitored and provides an indication the integrity of the image is
 4 compromised, for example, by indicating whether the original data of the image and the subsequent
 5 data do not match.

6 Content consumers will be best served by a different set of UX principles to help them make
 7 decisions about what to trust through the presentation of claim evidence. For that reason, it
 8 is important that if a visual indication is associated with a valid asset, it should indicate only
 9 that CAI data is present and verified, and should *not* appear to indicate whether the content
 10 is authentic. In cases where the asset and its CAI data do not match, this should be clearly
 11 indicated as well.

12 CAI Whitepaper,

13 <https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Aascds%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19>

14 15 **1. Creation**

16 We use cryptographic asset hashing to provide verifiable, tamper-
 17 evident signatures that the image and metadata hasn't been
 18 unknowingly altered. At creation, choose what information to attach
 19 to the content being created. Throughout this process, the creator of
 20 content can choose to preserve attribution or to remain anonymous.
 21 Privacy and security of photojournalists and other creators are of the
 22 utmost consideration in our work.

23 <https://contentauthenticity.org/how-it-works>

24 41. The C2PA standard describes that assertions, such as camera information such as
 25 maker and lens of the camera, as well as location information and pixel data such as an image
 26 thumbnail, are bound together into units called a C2PA Manifest. Such manifests must include
 27 one or more binding assertions to ensure that the asset (or digital image) is tamper-evident.
 28

https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html

42. The C2PA standard also describes “indicators of C2PA data” which demonstrate an indication of compromised integrity to the asset or digital image.

4.3. Validation states (E)

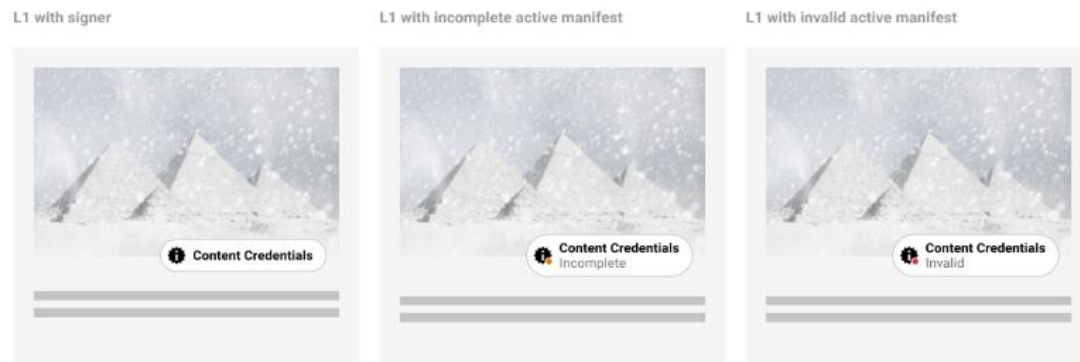


Figure 3. L1 validation states {need to update this image}

In the event that the active manifest is invalid, a stateful indicator of data validation can be displayed. There are several scenarios when displaying a data validation state may be necessary. See Chapter 14, Validation in the [C2PA Technical Specifications](#) for further information.

https://c2pa.org/specifications/specifications/1.0/ux/UX_Recommendations.html#_l1_indicator_of_c2pa_data

43. Cameras compatible with the C2PA standard, such as made by Leica and Nikon, also monitor the integrity of the tight coupling between the camera sensor and the memory of the camera and Exif information stored in the memory of the camera.

44. The Accused Products utilize a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory. For example, the Accused Products utilize cryptographic asset hashing to provide assurances that a digital image file has not been altered since publication.

The CAI uses *cryptographic asset hashing* to provide verifiable, tamper-evident signatures that the asset and metadata haven't been altered since the asset was published with the attached manifest. This means that a hash function converts the digital asset data to a unique "fingerprint," which is signed using a certificate. Once the credentials are signed, if the asset is changed then its fingerprint also changes. That's why it's called "tamper evident." You're not prevented from changing an image that has Content Credentials, but if you do, the credentials are no longer valid unless you change it using a tool that updates and re-hashes the credentials, along with a timestamp and optionally a description of what changed. The C2PA specification refers to this as hard binding.

<https://opensource.contentauthenticity.org/docs/getting-started/>

5.4 Digital Signatures

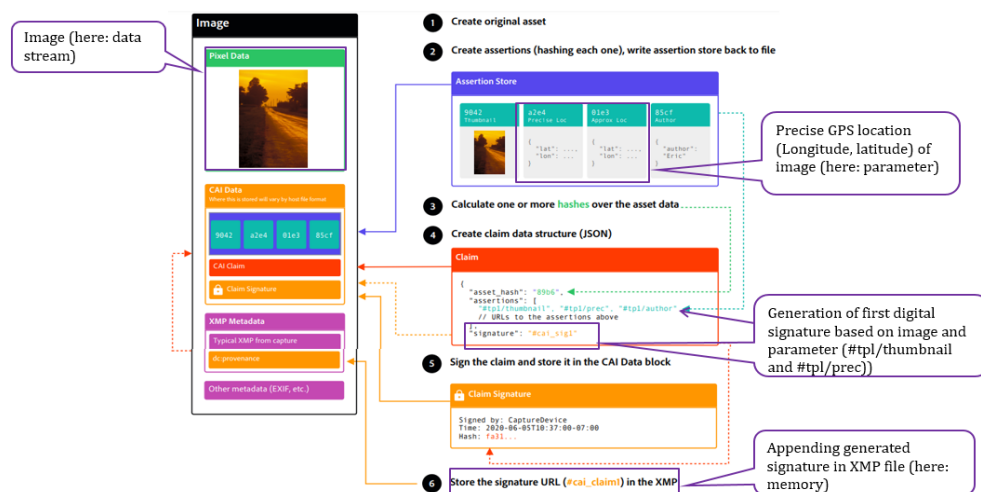
In order to ensure the integrity of the CAI information that is embedded into an asset, including the asset's data itself, *digital signature* technology is employed. That same technology also provides an authentication mechanism connected to the signer, that provides a way to establish trust in the actors involved in the CAI-enabled workflow.

Because the data being signed is, in signature terms, "arbitrary message content," a standard *Cryptographic Message Syntax* (CMS) signature is used to sign the asset. While a simple CMS signature is sufficient, CAI recommends using a CMS Advanced Electronic Signature (CAvES) instead. Use of a CAvES-compliant signature will ensure that the CAI data complies with the *European eIDAS legislation*.

It is also recommended that the signer should use a trusted timestamp authority to generate a trusted time-mark or time-stamp token. This is for proving that the signature itself actually existed at a certain date and time and can be incorporated into the CAvES content-time-stamp attribute to create a CAvES-T compliant signature.

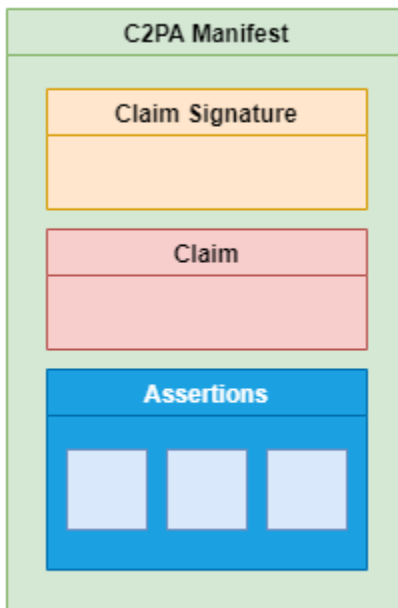
Content Attribution Initiative Whitepaper,

<https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascde%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19&viewer%21megaVerb=group-discover>



1 *Id.*

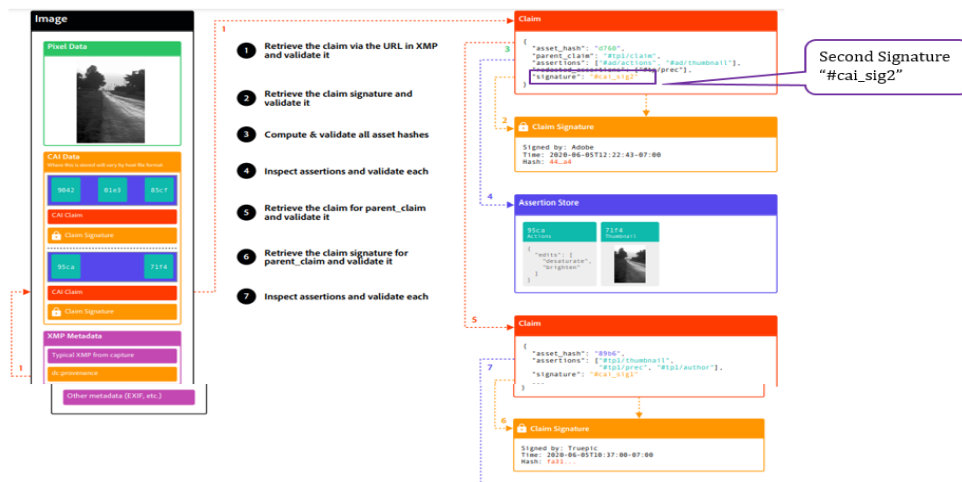
2 45. The C2PA standard specifies that manifests, which include bundles of asset
3 assertions, include digital signatures. The C2PA manifest includes bundles of assets assertions
4 called claims which are digitally signed.



6
7
8
9
10
11
12
13
14
15
16 *Figure 1. A C2PA Manifest and its constituent parts*

17 https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html

18 46. The Accused Products utilize the signature protocol to generate a second signature
19 based on the said data stream.



Content Authentication Initiative Whitepaper,

<https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Aascds%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19&viewer%21megaVerb=group-discover>

47. The C2PA standard describes an image having multiple claims, which are bundles of asset assertions about the image, that are both digitally signed indicating a second signature based on the data stream.

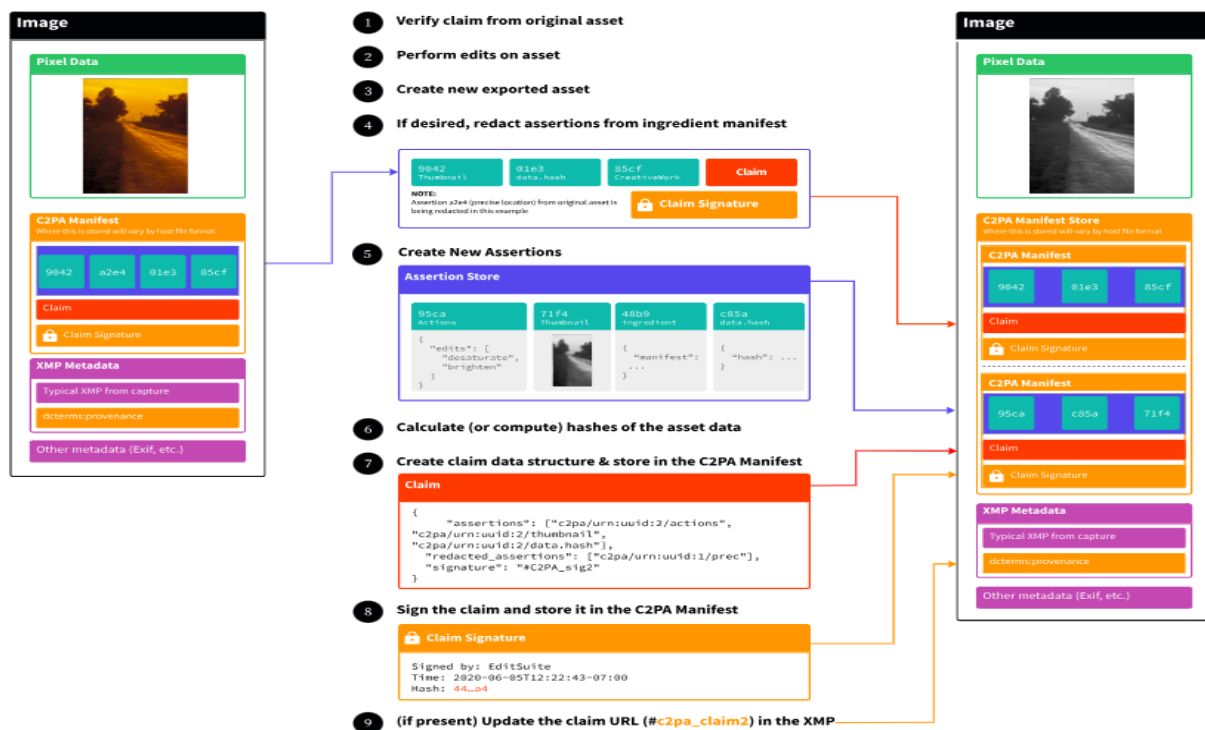


Figure 8. Redacting assertions in a secondary claim

https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_signing_a_claim

48. The Accused Products compare the first and the second signature.

1. A capture device captures an image and concurrently creates a set of assertions about the image such as capture location, equipment details, identity of the user, and perhaps a representative thumbnail. These assertions are embedded in the asset.
2. A claim, referring to the set of assertions and including a hash of the image, is created and cryptographically signed by a trusted signing authority on behalf of the user. The claim is then embedded into the image and a reference to it stored in the asset's metadata (see "Figure 1: Creating a Claim").
3. The image, with its attached claim, is imported into an editing tool. The prior claim is verified (see "Figure 2: Validating Claims"), such that upon successful verification its assertions and claims can be carried forward as the image's history is accumulated.
4. As edits are made, additional assertions are captured and stored in a cloud service. Upon image export, these are gathered together as part of a second claim along with the hash of the updated image. A URL to the claim is stored in the asset's metadata. This new claim (which is also stored in the cloud) refers to the prior claim, therefore ensuring that all assertions from both claims are accessible via the exported image without any link to the prior version of the image.
5. The edited image, with its CAI metadata attached, is shared on a platform.
6. A content consumer encounters the image on the Web via a CAI-enabled viewing experience and sees a visual indication that CAI claims are present.
7. Finally, the content consumer interacts with the visual indicator to learn about the image's history. The most recent claim is retrieved and verified along with the entire chain of claims and their component assertions (see "Figure 2: Validating Claims"). The assertions are displayed to the viewer in a clear, time-ordered user experience depicting the image's claim history from inception to display.

Content Authentication Initiative White Paper,
<https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascde%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19&viewer%21megaVerb=group-discover>

49. The C2PA standard describes that, in the Accused Products, each of multiple claims, that are each associated with a given asset, such as a digital image, are all digitally signed. These signatures are then compared by retrieving the signature value from the manifest. If the signature field is not present then the claim is rejected by the Accused Products.

16.4. Validate the Signature

Retrieve the URI reference for the signature from the value of the claim's `signature` field and resolve the URI reference to obtain the COSE signature. The signature must be embedded in the same manifest as described in Section 12.1.1, "C2PA Box details". If the signature URI does not refer to a location within the same C2PA Manifest box (a `self#jumbf` location), the claim must be rejected. If no such field is present or the URI cannot be resolved, then the claim must be rejected with a failure code of `claimSignature.missing`.

NOTE

The signature and the claim need to be in the same manifest to be valid.

https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#validation

50. When the Accused Products compare the first and second signatures, if the signatures are not the same, an error is signaled to the user to show the stream is not authentic, if the signatures are the same, then an OK signal is generated to indicate to the user the stream is authentic.

1. A capture device captures an image and concurrently creates a set of assertions about the image such as capture location, equipment details, identity of the user, and perhaps a representative thumbnail. These assertions are embedded in the asset.
2. A claim, referring to the set of assertions and including a hash of the image, is created and cryptographically signed by a trusted signing authority on behalf of the user. The claim is then embedded into the image and a reference to it stored in the asset's metadata (see "Figure 1: Creating a Claim").
3. The image, with its attached claim, is imported into an editing tool. The prior claim is verified (see "Figure 2: Validating Claims"), such that upon successful verification its assertions and claims can be carried forward as the image's history is accumulated.
4. As edits are made, additional assertions are captured and stored in a cloud service. Upon image export, these are gathered together as part of a second claim along with the hash of the updated image. A URL to the claim is stored in the asset's metadata. This new claim (which is also stored in the cloud) refers to the prior claim, therefore ensuring that all assertions from both claims are accessible via the exported image without any link to the prior version of the image.
5. The edited image, with its CAI metadata attached, is shared on a platform.
6. A content consumer encounters the image on the Web via a CAI-enabled viewing experience and sees a visual indication that CAI claims are present.
7. Finally, the content consumer interacts with the visual indicator to learn about the image's history. The most recent claim is retrieved and verified along with the entire chain of claims and their component assertions (see "Figure 2: Validating Claims"). The assertions are displayed to the viewer in a clear, time-ordered user experience depicting the image's claim history from inception to display.

Content Authentication Initiative Whitepaper,
<https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascde%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19&viewer%21megaVerb=group-discover>

51. The C2PA standard specifies “status codes” which are generated after comparison of the first and second digital signatures. The standard specifies “success codes” which are generated to indicate to the user that the stream is authentic, and “failure codes” to indicate to the user that the user stream is not authentic.

16.1.1. Success codes

Value	Meaning	url Usage
<code>claimSignature.validated</code>	The claim signature referenced in the ingredient's claim validated.	C2PA Claim Signature Box
<code>signingCredential.trusted</code>	The signing credential is listed on the validator's trust list.	C2PA Claim Signature Box

16.1.2. Failure codes

Value	Meaning	url Usage
<code>claim.missing</code>	The referenced claim in the ingredient's manifest cannot be found.	C2PA Claim Box
<code>claim.multiple</code>	More than one claim box is present in the manifest.	C2PA Claim Box
<code>claim.hardBindings.missing</code>	No hard bindings are present in the claim.	C2PA Claim Box
<code>claim.required.missing</code>	A required field is not present in the claim.	C2PA Claim Box
<code>claim.cbor.invalid</code>	The cbor of the claim is not valid	C2PA Claim Box
<code>ingredient.hashURI.mismatch</code>	The hash of the the referenced ingredient claim in the manifest does not match the corresponding hash in the ingredient's hashed URI in the claim.	C2PA Assertion
<code>claimSignature.missing</code>	The claim signature referenced in the ingredient's claim cannot be found in its manifest.	C2PA Claim Signature Box
<code>claimSignature.mismatch</code>	The claim signature referenced in the ingredient's claim failed to validate.	C2PA Claim Signature Box

1 [https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_signature_val](https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_signature_validation)
2 [idation](https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html#_signature_validation)

3 52. Adobe has directly infringed the '828 Patent in violation of 35 U.S.C. § 271(a) by
4 making, using, offering for sale, and selling the Accused Products that embody the patented
5 inventions of at least claim 1 of the '828 Patent.

6 53. Adobe's infringing products include at least the content attribution tools, also called
7 "content credentials" within its Creative Cloud suite of software products and its products that
8 adhere to the Content Authenticity Initiative and other products with the same or similar
9 functionality that satisfy each element of one or more asserted claims.

10 54. The Accused Products satisfy each and every element of each asserted claim of the
11 '828 Patent either literally or under the doctrine of equivalents.

12 55. Adobe's infringing activities are and have been without authority or license under
13 the '828 Patent.

14 56. Adobe has willfully infringed the '828 Patent. Adobe has had knowledge of the
15 '828 Patent since at least 2007. At that time, Goldhar/Jaffe Technology Development Corporation
16 ("GJTDC"), the original assignee of the '828 Patent, had communications with Adobe about '828
17 Patent and the integration of concepts embodied in the '828 Patent. At Adobe's request,
18 presentations were prepared for Adobe about the '828 Patent and the integration of the concepts
19 embodied in the '828 Patent for use by Adobe. GJTDC provided several drafts of the presentations
20 to Adobe for comment, GJTDC received comments from Adobe, and GJTDC modified the
21 presentations to address Adobe's comments. GJTDC sent at least four versions of the presentation
22 to Adobe beginning in January 2007. These presentations included an "Intellectual Property" page
23 which stated that the concepts described in the presentations were protected by the '828 Patent.
24 The full patent number as well as the issue date of the '828 Patent were included. In February
25 2007, Cheryl Shimamoto of Adobe informed GJTDC that Adobe found "[t]he technology is very
26 interesting, but relevance to our program is marginal. So, rather than have you fly out here, we'd
27 rather stop now." Adobe abruptly terminated all discussions shortly thereafter. These prepared
28 presentations from 2007 still exist.

1 57. Mr. Jaffe is informed and believes that despite Adobe's knowledge of the '828
2 Patent and Mr. Jaffe's patented technology, Adobe made the deliberate decision(s) to make, use,
3 sell, or offer to sell products that it knew infringed the '828 Patent.

4 58. Mr. Jaffe is informed and believes that Adobe knew or was willfully blind to Mr.
5 Jaffe's technology and the '828 Patent. Despite this knowledge and/or willful blindness, Adobe
6 has acted with blatant and egregious disregard for Mr. Jaffe's patent rights with an objectively
7 high likelihood of infringement.

8 59. Mr. Jaffe is informed and believes that Adobe has undertaken no efforts to avoid
9 infringement of the '828 Patent, despite Adobe's knowledge and understanding that Adobe's
10 products infringe the '828 Patent. Thus Adobe's infringement of the '828 Patent is willful and
11 egregious, warranting enhancement of damages.

12 60. As such, Adobe has acted and continues to act recklessly, willfully, wantonly,
13 deliberately, and to egregiously engage in acts of infringement of the '828 Patent, justifying an
14 award to Mr. Jaffe of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs
15 incurred under 35 U.S.C. § 285.

16 **COUNT II – INDUCED INFRINGEMENT OF**
17 **THE '828 PATENT**

18 61. Mr. Jaffe repeats, realleges, and incorporates by reference, as if fully set forth
19 herein, the allegations of the preceding paragraphs, as set forth above.

20 62. Adobe is liable for indirect infringement under 35 U.S.C. § 271(b) of at least one
21 claim of the '828 Patent, at least as early as 2007, because it knowingly encouraged, aided, and
22 directed others to make, use, sell, or offer for sale the Accused Products.

23 63. As detailed above, Adobe was informed by GJTC of the '828 Patent in 2007.

24 64. Adobe specifically intended the Accused Products to be used and operated to
25 infringe one or more claims of the '828 Patent.

26 65. Adobe encourages, directs, aids, and abets the use, configuration, and installation
27 of the Accused Products.

28

- 1 (F) A finding that this case against Adobe is “exceptional” and an award to Mr. Jaffe
2 of its costs and reasonable attorneys’ fees, as provided by 35 U.S.C. § 285;
3 (G) An accounting of all infringing sales and revenues of Adobe, together with post
4 judgment interest and prejudgment interest from the first date of infringement of
5 the ’828 Patent;
6 (H) Such further and other relief as the Court may deem proper and just.
7

8 Dated: December 15, 2023

Respectfully submitted,

9 DICKINSON WRIGHT, PLLC

10 By: /s/ Christopher E. Hanba

11 Christopher E. Hanba

12 Christopher E. Hanba (*pro hac vice*)

13 Email: chanba@dickinson-wright.com

14 Joshua G. Jones (*pro hac vice*)

Email: jjones@dickinson-wright.com

DICKINSON WRIGHT PLLC

607 W. 3rd Street, Suite 2500

Austin, Texas 78701

16 Telephone: (512) 770-4200

17 Facsimile: (844) 670-6009

18 Ariana D. Pellegrino (*pro hac vice pending*)

Email: apellegrino@dickinson-wright.com

DICKINSON WRIGHT PLLC

500 Woodward Avenue, Suite 4000

20 Detroit, MI 48226

21 Telephone: 313-223-3500

22 Eric M. Schiffer

Email: eschiffer@schifferapc.com

SCHIFFER, APC

7545 Irvine Center Drive, Suite 200

24 Irvine, CA 92618

25 Telephone: (949) 533-0485

26 Attorneys for Plaintiff

27 Jonathan E. Jaffe
28

CERTIFICATE OF SERVICE

I hereby certify on December 15, 2023, that a copy of the foregoing was filed electronically through the Court's CM/ECF system, with notice of case activity automatically generated and sent electronically to all counsel of record, constituting service per Civil L.R. 5-1(h)(1).

/s/ Christopher E. Hanba

Christopher E. Hanba