



Apple Reference Image

A New Approach for Verified Photography

September 2026

Contents

Introduction	3
The Core Requirements of Apple Reference Image.....	5
Technical Details.....	7
Conclusion	12

Introduction

Today, powerful, widely available AI tools allow users to easily generate or alter photorealistic images to a degree that was difficult to imagine just a few years ago. These tools enable helpful features, like one-touch removal of background distractions, but they also make it difficult to distinguish between photographs that depict real events and synthetic images that are heavily altered or entirely generated. So, in the case where the essential role of a photograph is to prove that something actually happened, an image appearing photorealistic is no longer sufficient to establish its veracity.

This is not a simple problem to address. Modern cameras rely on sophisticated image-processing algorithms to produce the final viewable image, so certifying that an image accurately reflects what a real camera sensor captured requires a chain of trust covering the sensor as well as the computational photography software that interpreted the capture. Industry approaches to this problem, based on the C2PA standard, attach provenance metadata after capture and certify the history of image edits from that point forward. This approach, however, is vulnerable to compromise at any point in the editing chain, and a viewer has no way to detect such a failure. It can also create privacy risks for photographers working in dangerous conditions by tying the image to a public identity, either to a particular device or to an individual.

iPhone is the world's most popular camera and the most secure consumer mobile device, and as such, Apple is uniquely positioned to take on this challenge. The iPhone camera is integrated into a platform that sets the industry's highest standards of security from the silicon up. We also operate Private Cloud Compute (PCC), an industry-leading privacy-preserving cloud infrastructure that is secure, auditable, and can perform verifiable algorithmic operations without allowing anyone — even Apple — the ability to see the data being processed.

Leveraging these state-of-the-art capabilities, we have created Apple Reference Image, a novel solution for verifiable photography on iPhone, and debuting on the main camera sensor of iPhone 18 Pro and iPhone 18 Pro Max. This new, opt-in camera mode lets a photographer create a securely timestamped reference image that accurately reflects what was captured by the iPhone's camera sensor. Dedicated secure hardware on the device protects the integrity of this reference image, and Private Cloud Compute protects the privacy of the image data during processing. The system is built to be resilient to compromise, no matter how unlikely: any fraudulent images can be revoked without exposing the photographer's identity.

Apple Reference Image offers a trustworthy, scalable guarantee that a reference image is what it claims to be: a real photograph, captured by a real sensor in an iPhone camera, at a specific time. It sets a new standard for verifiable digital photography.

The Core Requirements of Apple Reference Image

A high-assurance photographic provenance system must meet three core requirements:

- **Semantic authenticity:** a reference image must faithfully show what the sensor captured. Transformations of image data from the raw captured pixels to the final viewable image must be publicly verifiable.
- **Resilience to compromise:** image authenticity cannot be undermined by tampering with the camera sensor, through common cryptographic attacks, or via software-level jailbreak of the device. If, despite these protections, any fraudulent reference images are created, they can be revoked.
- **Privacy preservation:** an outside observer cannot determine whether any pair of reference images were taken by the same device. Image contents are not exposed to Apple or anyone else.

Apple Reference Image leverages custom-designed image sensors in iPhone 18 Pro and iPhone 18 Pro Max to ensure reliable capture of image data, and relies on Private Cloud Compute, which provides a computational environment for secure photographic processing that cannot be subverted even in the case of device compromise. We believe no other commercially available photographic provenance system meets these strict requirements.

Semantic Authenticity

For any photographic authenticity system, the defining goal is that a user can trust that what is shown as the authenticated image corresponds to the scene that was actually photographed. A central challenge these systems face is how to secure the extensive photographic processing pipeline of a modern computational camera. Simply signing the raw values emitted by a sensor does not yield a viewable image: these pixels still need significant processing, like [demosaicing](#) and lens-shading correction, to be usable. To solve this, prior industry systems have delayed signing images until they reach the end of their software processing pipeline. But this approach is vulnerable to attacks that inject spoofed pixel data onto the data transport from the sensor, or to compromises of the device operating system that can completely alter the image before signing. Neither signing raw sensor values, nor delaying signing until the photograph is processed, meets our bar for semantic authenticity. Our solution hinges on splitting the Apple Reference Image process into two phases: creating a secure digital negative, and developing that negative into a reference image. Each phase receives our strongest protections.

The creation of a secure digital negative begins with a secure boot of the camera sensor into a specialized reference capture mode. The mode instructs the sensor to cryptographically sign pixel data immediately after capture, and prevents the sensor firmware from modifying the data. This creates a hardware-enforced assurance that the operating system receives pixel data exactly as the hardware sensor captured it, preventing injection or tampering attacks.

We treat image metadata with the same level of protection. Sensor-produced metadata is signed at capture time together with the pixel data. For the few metadata values that originate beyond the camera sensor, such as digital zoom boundaries and focal length, we use the Secure Enclave Processor (SEP) to sign the values. This off-sensor metadata cannot alter the pixel values themselves.

Knowing when a photograph was captured is often a critical element in establishing its veracity. While prior industry systems have included a timestamp provided by the general device operating system, we believe this plainly falls short of the real-world assurance need. Instead, Apple Reference Image provides both a lower bound and an upper bound on capture time from Apple's cryptographic timestamp service, and we guarantee the photo was taken between the two bounds. On a regular heartbeat, the device requests a cryptographic timestamp token, and retains the most recent one it has received. Globally this happens on average every 15 minutes, though the interval depends on local network conditions. This provides a proven lower bound timestamp for the photographic capture. After capture, the device requests a second timestamp to use as an upper bound, and both timestamps are embedded and signed with the sensor data.

As a result, the secure digital negative contains all the essential information for rendering a reference image — the pixel data, essential sensor metadata, and the secure timestamp bounds — all protected from device software compromise.

To develop this secure digital negative into a user-visible reference image, we take advantage of the privacy-preserving computing environment provided by Private Cloud Compute. When the user chooses to create a reference image, the device uploads the digital negative to PCC, which runs the processing steps needed to render the image — including demosaicing, tone mapping, and compression — in a highly secure, private, and verifiable environment. Experts can verify that PCC doesn't alter a digital negative during development: they can examine the software that does the work. Every production build of PCC is recorded in an append-only, cryptographically tamper-proof transparency log, the binaries are available for public inspection, and a device will only send data to a node that can attest to running a build from that log. These are the same extraordinary guarantees we make for how PCC protects the privacy of Apple Intelligence requests.

Apple Reference Image combines the strong guarantees of these two stages — the hardware-level assurance over the secure digital negative, and PCC's verifiable transparency over the processing algorithms — to provide industry-leading semantic authenticity for the resulting images.

Resilience to Compromise

In designing Apple Reference Image, we considered a broad range of attacks, and constructed the system so as to resist compromise from multiple vectors.

As described above, we designed the core reference image pipeline to withstand a compromise of the operating system, or a data injection attack on the sensor bus. But we needed additional safeguards against a broader class of hardware attacks that could involve removing the sensor from the device.

These defenses begin before a single picture is taken, at manufacturing time. When the image sensor is first initialized in the factory, it creates a cryptographic signing identity, sharing only the public key with the factory. The SEP similarly creates a separately attested signing identity. These identities are bound together into the device manifest, allowing us to later check whether a particular sensor and SEP are from the same device. At capture time, the device incorporates this platform information into the digital negative it produces. When the reference image is then developed in PCC, PCC can validate that the photograph has come from a valid sensor-device pairing.

We also considered cryptographic attacks. Existing photo signing schemes, to our knowledge, all sign with classically secure algorithms, but quantum-secure algorithms are increasingly critical to the long-term integrity of cryptographic signatures. Because reference images are published assets whose integrity must survive for as long as anyone might want to check them, a signature secure only against classical adversaries isn't sufficient: an image asserted to be authentic in 2026 should be securely verifiable in perpetuity. So we designed the system to resist quantum attacks on any algorithm used to protect the integrity of publicly distributed reference images. The final signature on a reference image is a composite post-quantum signature combining RSA-3072 and ML-DSA-87. To our knowledge, Apple Reference Image is the only image provenance system that provides quantum-secure defenses.

Finally, as no security system is perfect, we created a revocation system that can revoke individual photos, as well as all photos from a specific sensor. As part of developing the secure digital negative, PCC computes a confidence score that assesses whether the image has the physical characteristics expected of raw output from our camera sensors. Before the developed reference image is signed, PCC sends the photo GUID, sensor ID, and this confidence score to a companion service, which records them and updates the running score associated with that sensor. If a low-scoring sensor is revoked, PCC will no longer sign its images. Apple devices fetch updated revocation lists on a regular cadence; any time a reference image is viewed, the viewer can have confidence that the image isn't known to be fraudulent.

Privacy Preservation

Other industry solutions require a photographer or institution to vouch for an image using their own credentials. We are concerned this puts some photographers, such as those operating in conflict zones, in a difficult position; it should not be necessary to forgo anonymity in order to prove image authenticity. We built Apple Reference Image to avoid using an explicit, public credential for photographers, and to avoid even implicit public association between different photos taken by the same sensor. The final reference image is instead signed by Apple's signing service, after validation by PCC. That signature is backed by Apple's strongest technical guarantees.

Our implementation also protects the confidentiality of the image itself, including from Apple. Merely capturing a reference image should never expose the actual pixels to Apple or anyone else. We achieve this through the exceptional privacy properties of PCC — the nodes themselves are architected so that not even Apple can access image data, just as Apple cannot see the information processed for Apple Intelligence in PCC. While the revocation service must maintain a private record of photo GUIDs and associated sensors to allow for revocation, it never has access to the image data, and does not allow for public access to this record. And as final revocation checks occur using on-device lists, a device never reveals to anyone which photo it's looking at in order to find out whether it's still valid.

Last, we have taken care to limit network visibility wherever possible. Timestamping requests travel over Oblivious HTTP, so the timestamp service never learns the IP address of the requesting device. Similarly, calls to the revocation and signing services occur from within PCC itself, which provides only the minimum information required for those services to function. Altogether, we believe these privacy protections are far stronger than in any existing image provenance system, allowing both photographers and viewers access to authentic images without inadvertently revealing their personal information.

Across all three requirements — semantic authenticity, resilience to compromise, and privacy preservation — we believe that Apple Reference Image sets a new standard for security in the industry. For readers who are additionally interested in the technical details of our implementation, the next section will describe the precise manufacturing, signing, and verification sequences that underpin the security guarantees of Apple Reference Image.

Technical Details

Reference Image Set-Up

The foundation for Apple Reference Image is created during device manufacturing. When an Apple photo sensor is first initialized, it generates its own ECDSA P-256 signing key pair and never releases the private half. The factory recording station retrieves only the corresponding public verification key, signs it with a factory certificate authority (CA), and records the key and certificate in the device's hardware manifest.

The Secure Enclave Processor (SEP) goes through a similar process: it generates a key certified by our Basic Attestation Authority (BAA) under a separate CA, which lets the device later produce signatures that Apple can attribute to that specific phone. A third CA then signs the device manifest itself, binding the sensor key and the BAA-attested SEP key together as belonging to the same iPhone. This binding is what later lets us state that a particular sensor and a particular Secure Enclave were, and are, part of the same device.

Once the device is in use, it begins timestamp collection. Apple Push Notification Service (APNs) runs an existing heartbeat protocol to ensure the health of the connection for push notifications. Coinciding with this heartbeat, APNs now delivers an up-to-date RFC 3161 timestamp token from Apple's timestamp service, signed with ECDSA P-256 over SHA-256, and the device keeps the most recent one it receives.

Image Capture

To begin the capture process, the user switches to Reference mode. This reboots the sensor into the specialized, secure reference mode. This capture mode accepts one input from the device operating system: a SHA-256 digest to be embedded at a fixed location in the captured frame's metadata. The digest is computed from the most recent secure timestamp, the device manifest, and the device's secure boot manifest.

At capture, the sensor measures light as an analog signal, which is digitized. The digitized frame and the embedded metadata digest are signed together, inside the sensor, with the sensor's private key. OS-derived metadata (digital zoom factor, exposure, and lens parameters) is collected from the camera system. We take a commitment to the sensor's signature together with this metadata and sign it with the SEP, using the BAA-attested key.

We compute a SHA-256 commitment to the SEP signature and send it to the timestamp service, which returns a signed token establishing that the photo existed no later than that moment, an upper bound to complement the lower bound already embedded in the frame. If the device is offline, no upper bound is available yet; a background process keeps attempting the request and inserts the token once it succeeds, producing the tightest interval the circumstances allow.

Everything produced so far — the pixels, both signatures, the timestamps, the metadata, the device manifest, and the secure boot manifest — is stored in the secure digital negative on the device, in DNG format, linked to the conventionally processed photo from the standard pipeline. The negative can sit there indefinitely, and it can also be shared in this undeveloped state, a workflow professional photographers may need.

Reference Image Development

When the user initiates developing a reference image, the device uploads the secure digital negative to Private Cloud Compute. PCC recomputes the digest embedded in the frame and verifies the sensor's signature over the pixels and that digest, verifying the certificate chain back to the sensor CA. PCC also verifies the SEP signature and chains it to the BAA CA, and it verifies the signature on the device manifest and chains it to the CA that signs device manifests at the factory. It then confirms that the sensor and SEP named in those chains belong to the same device. Only if all these checks pass does processing continue.

PCC next checks the timestamps. If the lower-bound timestamp fails verification, PCC substitutes March 31, 2026, since the feature didn't exist before that date and no photo can predate it. If the upper-bound timestamp is missing or doesn't verify, PCC substitutes the current development time in PCC.

Using a neural network with hidden weights, PCC computes a confidence score for the photograph. This additional step confirms that the image has the physical characteristics expected of raw output from our sensors, increasing confidence in its authenticity. PCC then develops the negative with demosaicing, tone mapping, and related corrections. The result is compressed as a JPEG and hashed, creating a commitment to the developed image. This hash serves two purposes: it's the value that will be signed, assuming it passes our remaining checks, and it supplies the bits used for the photo GUID.

PCC sends the photo GUID, the raw hash, the confidence score, and the sensor ID to a companion service, which records them, updates the running confidence score associated with that sensor, and confirms the sensor doesn't appear on a revocation list. If these checks pass, PCC then submits the commitment to our signing service, which signs it with a composite post-quantum signature using a hybrid MLDSA87-RSA-3072-PSS-SHA512 scheme. The signature is

embedded in the JPEG, and the reference image is returned to the device, which associates it with the main photo from the original capture.

After the secure digital negative is successfully developed, it's automatically moved to the deleted photos folder. As with any deleted photo, the user can recover the negative for preservation if desired, or delete it immediately; otherwise, it's automatically purged after 30 days.

On the client side, whenever the reference image is displayed, the client verifies the final signature on the JPEG and confirms its photo GUID doesn't appear on the current revocation list before showing the image.

Conclusion

Apple Reference Image builds on Apple's unique foundation of capabilities in hardware and software, including sensor identity certification at the factory, silicon security, and Private Cloud Compute, giving photographers a new way to provide a verifiable photograph. This allows them to attest to what their iPhone actually captured, without requiring them to expose a public identity or place trust in a third party. At its core, Apple Reference Image binds a signature from an iPhone camera sensor to a securely timestamped, tamper-evident record, developing it inside PCC while running publicly verifiable code, and signing it with a composite post-quantum signature designed to remain secure for decades. If a device is later found to be compromised, its images can be revoked and flagged retroactively, without revealing which images came from the same sensor. The result is a verification model that offers photographers, newsrooms, and everyday users renewed confidence that an image they're viewing is a photograph actually captured by a camera.

© 2026 Apple Inc. All rights reserved. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries and regions. Apple Intelligence is a trademark of Apple Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. September 2026