Archiving Adobe Sign documents through eOriginal vaulting services

Digitally manage and protect documents.

Adobe Sign partners with eOriginal to help organizations meet compliance and regulatory requirements by archiving important signed documents in a secure digital vault. Once a document is signed, eOriginal can securely vault it with the highest levels of protection and compliance in a fully digital environment. Organizations can choose to archive all documents in a particular account, all documents initiated by a specific group (or subset of users), or individual documents.

When a document is created, the original document that is uploaded to Adobe Sign is considered the authoritative copy of the contract. The authoritative copy remains on the Adobe servers throughout the entire signature cycle. Once the signature cycle is complete, the authoritative copy is archived in the eOriginal vault, and the document becomes a legal instrument. A PDF copy of the document remains in Adobe Sign, but it is watermarked with "Copy of Original" to indicate that the document vaulted by eOriginal is the only authentic version:

How it works

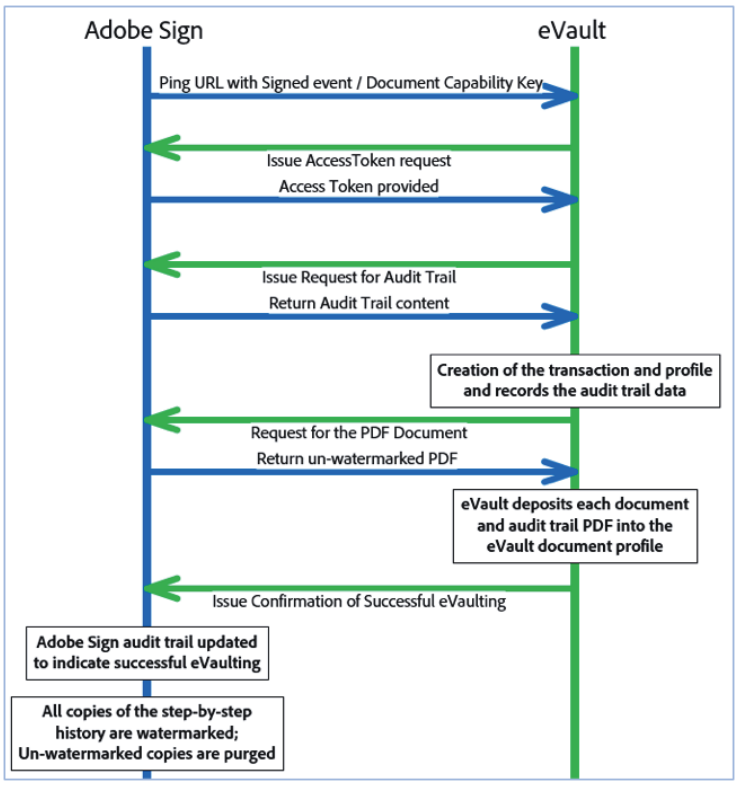
Upon completion of the signature cycle, any transaction enabled for vaulting will trigger the eOriginal vaulting service to initiate the transfer of the authoritative copy. This is an asynchronous call-and-response process in which the vaulting service requests information from Adobe Sign after receiving a notification, and Adobe Sign provides the content requested.

These sequential requests happen in near real time to ensure that the authoritative copy is stored with the vaulting service the moment the signature process is complete.

After the final signature is applied:

1. The eOriginal vaulting service is notified via ping that the signature process for a document with vaulting enabled has been completed. Adobe Sign sends a unique identifier for the document, called the Document Capability Key, to the vaulting service.
2. The vaulting service requests an access token for the final signed document.
3. Adobe Sign validates that the vaulting application is authorized to request an access token for the document. This ensures that only the vaulting application receives the authoritative copy of the document. Adobe Sign provides the unique one-time-use access token.
4. The vaulting service next requests the document audit trail to create a profile for the document.
5. Adobe Sign provides the audit trail; the audit trail includes the complete record of what happened during the signature process, including the identity of the signers, the date and time of each event, the IP address, and location information (if available).
6. The vaulting service then requests the non-watermarked version of the signed document using the one-time access token.
7. Adobe Sign validates the one-time access token and provides a non-watermarked document to the vaulting service.
8. The vaulting service confirms receipt of the document and notifies Adobe Sign that the vaulting process is complete.

9. Adobe Sign updates the audit trail to reflect the document's status as vaulted.
10. All versions of the document created during the signature process are watermarked, and non-watermarked copies of those documents are purged.



At this point, Adobe Sign only stores a watermarked copy of the document, including the step-by-step PDF copies obtainable in the history of the signing cycle. Thumbnail images are not watermarked because they are purely images, and not legal documents.

Non-watermarked documents can only be obtained from the vaulting service once the document is vaulted.

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

8/16