



Technology Comparison

AbsoluteProof Trusted Timestamping Compared to Digital Signatures: *Separate but Complementary Technologies*

PKI-based digital signatures provide a mechanism to reliably associate an identity with an electronic document or a portion of an electronic document.

As in a signature on a paper document, the actual meaning of the signature can vary. For example, the signature might signify the signer's agreement with contractual terms detailed in the signed document. An important characteristic of a digital signature is that it can be verified. When you verify a digital signature, you verify that the document has not changed since it was signed and that the identified party actually signed the document. Stated simply, signatures can reliably provide the "who" component of document authentication.

Digital signatures do nothing to reliably provide the "when" component of document authentication. For example, if an organization is asked to provide evidence that a particular record has not changed since a certain date, the fact that the record was digitally signed does not help. This is because a signed document can be altered, and then re-signed, and the result will be a perfectly valid signature. Digital time stamps are designed to solve this problem. Digital time stamps associate a reliable time-value with a document and thereby provide the "when" component of document authentication. If the document is altered, or the time-value associated with the time stamp is altered, then the time stamp is invalidated. One can always alter the document and re-time stamp it, but the new time stamp will carry a time-value that indicates the current time.

Digital signatures and trusted digital time stamps are separate but complementary technologies. If you only need the "who" then digital signatures are appropriate. If you only need the "when", then trusted time stamps are appropriate. If you need the "who" and the "when", then both are appropriate.

Trusted digital time stamps solve two key problems that can arise with digital signatures: repudiation and long-term signatures. The problem of repudiation occurs when the signer claims that they didn't actually sign the document. For example, because their signing key was compromised and someone else must have signed the document using their key. This problem can be solved by applying a timestamp to the document, signature, and evidence of key validity. For example, a Certificate Revocation List or CRL. Since the time stamp reliably associates a time-value with these objects, it can be used to prove that the key was in fact valid when the document was signed, and hence, eliminate the opportunity for repudiation.

Verifying digital signatures over the long term can be problematic because the revocation information used to validate the signature may no longer be available (technically, this is because certification authorities typically do not provide revocation information for certificates once they have expired). Furthermore, the fact that the cryptographic primitives used to create the signatures and revocation information can become weak over time, calls the long-term reliability of the signature into question. Digital time stamps can solve these problems. A time stamp can be applied to the document, signature, and revocation information that proves that the signature was created at a point in time when the key was valid (not compromised or expired) and that the underlying cryptographic primitives were still strong.

Because Surety's time stamps do not rely on cryptographic keys or certificates, they do not have the same expiration problems. Furthermore, Surety's patented time-stamp renewal technology enables Surety time stamps to be refreshed with new hashing algorithms when existing algorithms become weak.



TM

12020 Sunrise Valley Dr.
Suite 250
Reston, VA 20191
800-298-3115