Digital Signature

Return to Glossary

Definition 1:

A **Digital Signature** according to NIST[1] is the result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of:

1. Source/identity authentication,
2. Data integrity authentication, and/or
3. Support for signer non-repudiation.

Definition 2

A **Digital Signature** is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

Source: https://searchsecurity.techtarget.com/definition/digital-signature

1)

Elaine Barker, NIST, Recommendation for Key Management: Part 1 - General, NIST Special Publication 800-57 Part 1, Revision 5, May 2020, Accessed 18 January 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf