WISE

Introduction to Digital Signature Algorithms(DSA)

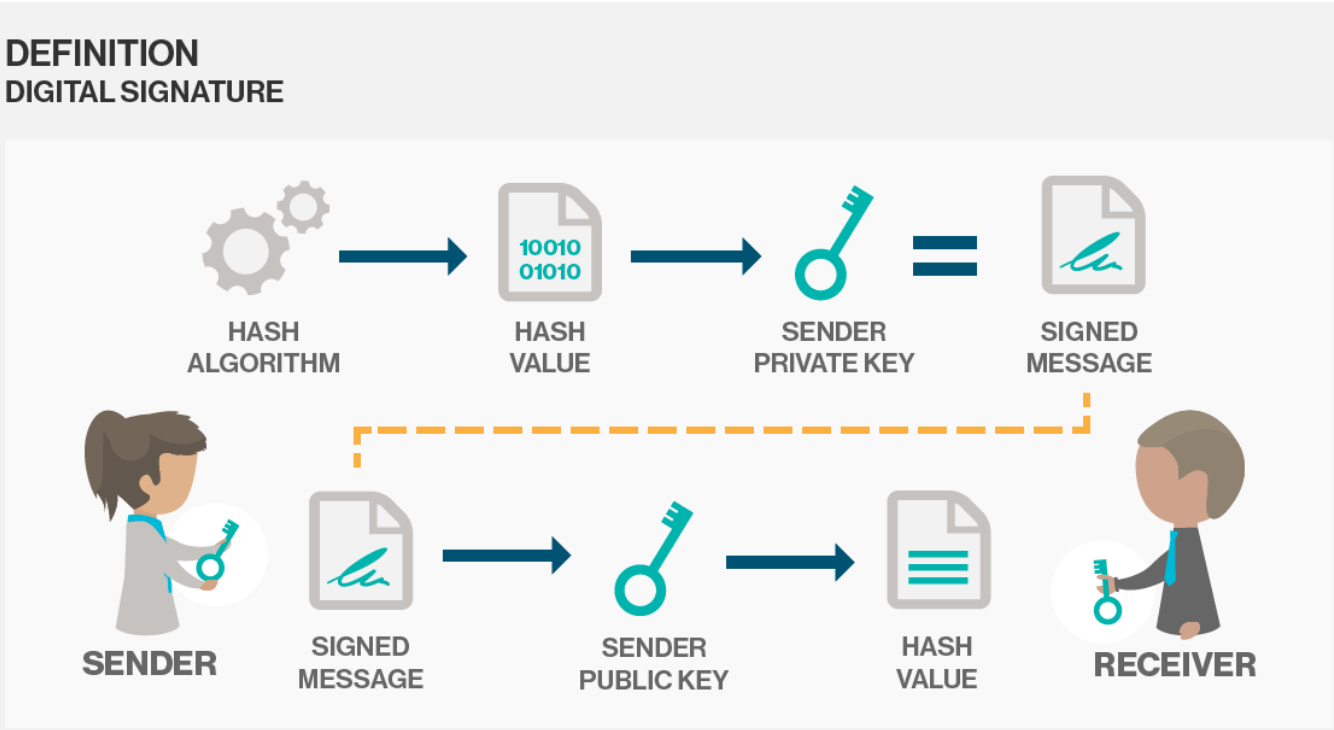
Tang Dexuan

2017.10.19

What is DSA?

- The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.
- The **Digital Signature Algorithm** (**DSA**) is a Federal Information Processing Standard for digital signatures. In August 1991 the National Institute of Standards and Technology (NIST) proposed DSA for use in their **Digital Signature Standard** (**DSS**) and adopted it as FIPS 186 in 1993.Four revisions to the initial specification have been released: FIPS 186-1 in 1996,FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013.

How DSA works?



- Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.
- The value of the hash is unique to the hashed data. Any change in the data, even changing or deleting a single character, results in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash.

Reference

01 https://en.wikipedia.org/wiki/Digital_Signature_Algorithm

02 http://searchsecurity.techtarget.com/definition/digital-signature

Thank you

Tang Dexuan

2017.10.19