Table of Contents

1. This Standard specifies algorithms for applications requiring a digital signature, rather than a written signature.
2. A digital signature is represented in a computer as a string of bits.
3. A digital signature is computed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified. Digital signatures may be generated on both stored and transmitted data.
4. Signature generation uses a private key to generate a digital signature, signature verification uses a public key that corresponds to, but is not the same as, the private key. Each signatory possesses a private and public key pair.
5. Public keys may be known by the public, private keys are kept secret. Anyone can verify the signature by employing the signatory's public key.
6. Only the user that possesses the private key can perform signature generation.
7. A hash function is used in the signature generation process to obtain a condensed version of the data to be signed; the condensed version of the data is often called a message digest.

General Discussion

A digital signature is an electronic analogue of a written signature.

The digital signature can be used to provide assurance that the claimed signatory signed the information.

In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data).

These assurances may be obtained whether the data was received in a transmission or retrieved from storage.

A properly implemented digital signature algorithm that meets the requirements of this Standard can provide these services.

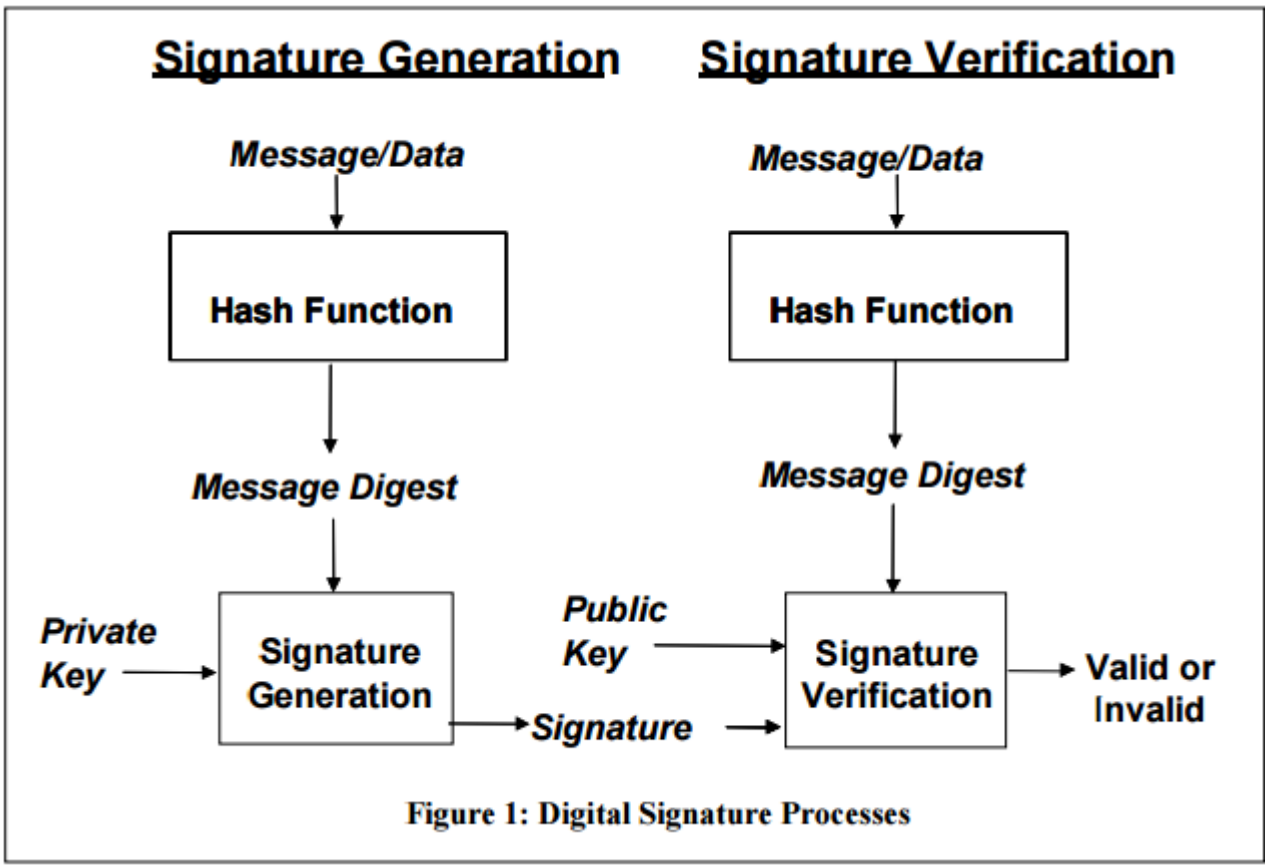
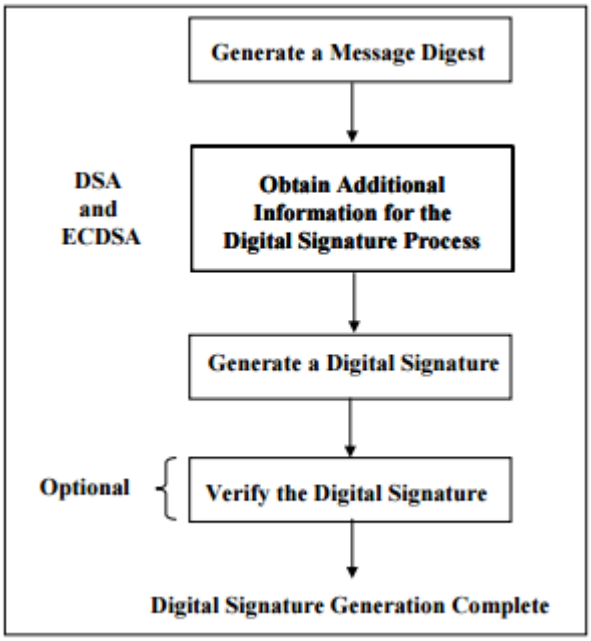


Figure 1: Digital Signature Processes

Digital Signature Generation

Figure 2 depicts the steps that are performed by an intended signatory (i.e., the entity that generates a digital signature).



Digital Signature Verification and Validation

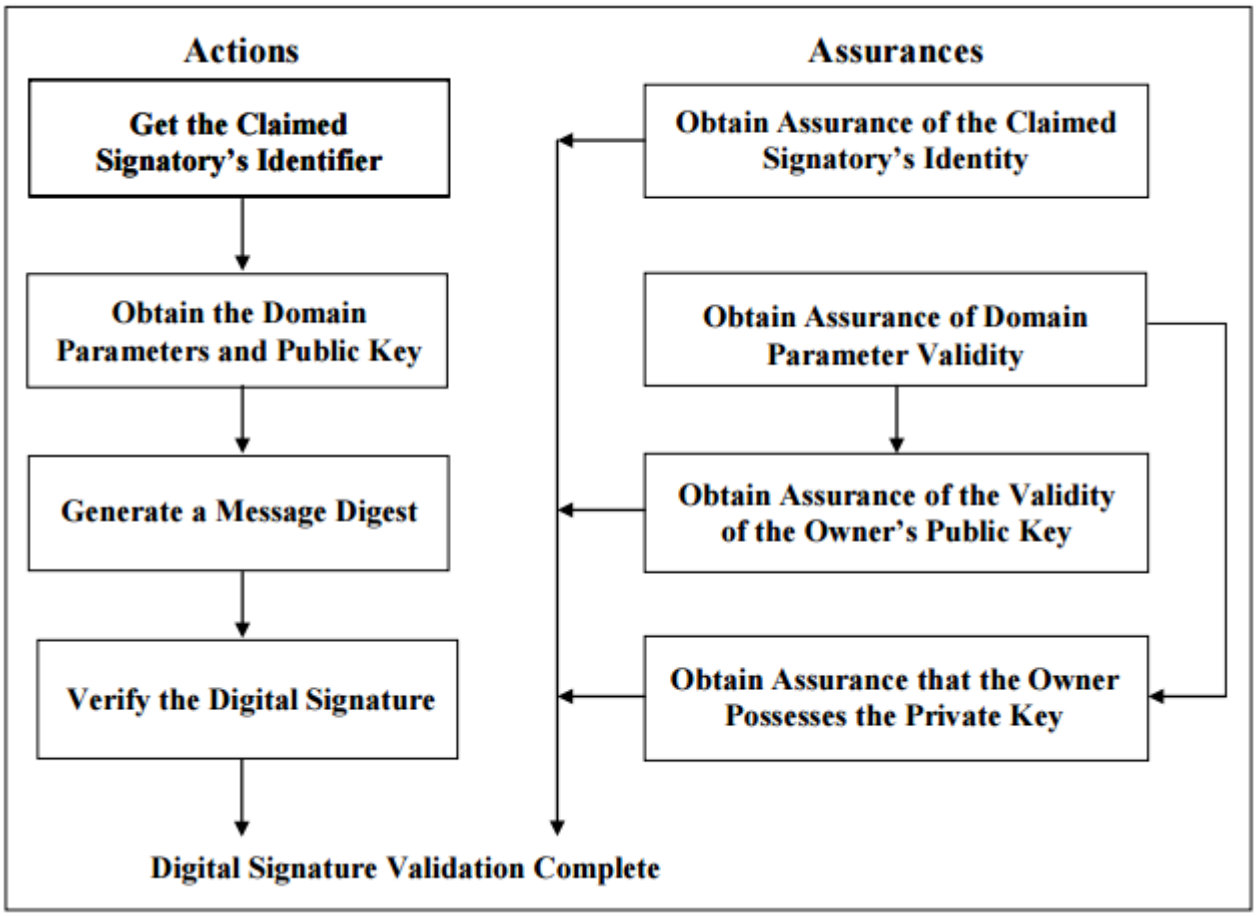
Figure depicts the digital signature verification and validation process that are performed by a verifier (e.g., the intended recipient of the signed data and associated digital signature).

Note that the figure depicts a successful verification and validation process (i.e., no errors are detected).

If the verification and assurance processes are successful, the digital signature and signed data shall be considered valid.

However, if a verification or assurance process fails, the digital signature should be considered invalid.

An organization’s policy shall govern the action to be taken for an invalid digital signature. Such policy is outside the scope of this Standard.



Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security

4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool
10. Categories of security assessments
11. Intrusion terminology
12. Cryptography attacks
13. Cryptography
14. SSH
15. MD5
16. Message digest functions
17. Digital signature
18. Authentication Functions
19. One way hash function
20. Hash function in network web security
21. SSL Secure socket layer