Department of Software

The University of Babylon

LECTURE NOTES ON DIGITAL SIGNATURES & HASH FUNCTION

By

Dr. Samaher Hussein Ali

College of Information Technology, University of Babylon, Iraq

Samaher_hussein@yahoo.com

18 December 2012

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory

Functional Standards for Authentication of Electronic Records

- **Authentication**: the process of assuring that an electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.
- **Digital Certificate**: An attachment to an electronic message used for security purposes, which enables a user sending a message via an unsecured network.
- **Electronic**: relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. For the purposes of this standard, “electronic” is not meant to encompass activities involving facsimile transmission.

Authentication Processes

For purposes of this standard, the process to ensure the authentication of an electronic signature in an electronic record shall, at a minimum, be of one of the following types:

- **Type 1:** This process uses a signature pad or other similar device to associate with an electronic record a digital representation of a physical signature of the person signing the record. To authenticate the electronic signature on the electronic record, the signature shall be created in the presence of a deputy clerk other than the signer. Either the signer or the witness shall immediately submit the record to the e-filing or case management system.
- **Type 2:** This process is used to authenticate an electronic signature on an electronic record by the sender logging-in to an application recognized by the court (i.e., a case management system, or an e-filing system/portal) which will receive the electronic record. The electronic record may be created from within the court's case management system (court user) or from an application outside of the court (non-court user). The login will involve a user name and password which are unique to the sender. The local court, or a vendor under a contract with the court, will maintain a secure register of the user name and password for each authorized user. The user name and/or password may be either created by the user, or assigned to the user by the administrator of the court application. The court must utilize secure password procedures.

Authentication Processes

- **Type 3:** This process is used to authenticate an electronic signature on an electronic record by a two-step process. First, the sender must log in to the application as described above for the Type 2 process, plus the sender must additionally verify the transaction by either entry of a separate unique personal identifier (e.g., a personal identification number [“PIN”]) or the use of a physical identification device (e.g., smart card, biometric reader, etc.).
- **Type 4:** This process is used to authenticate electronic signatures on electronic records by complying with specific secure data transfer protocols (e.g., FTP, web services, etc.) negotiated by the clerk of the court with a trusted authority, such as a financial institution, large employer, or government agency (e.g. BMV, BCI&I, Ohio Courts Network, other courts, local law enforcement agencies, etc.).

Digital Signature Generation

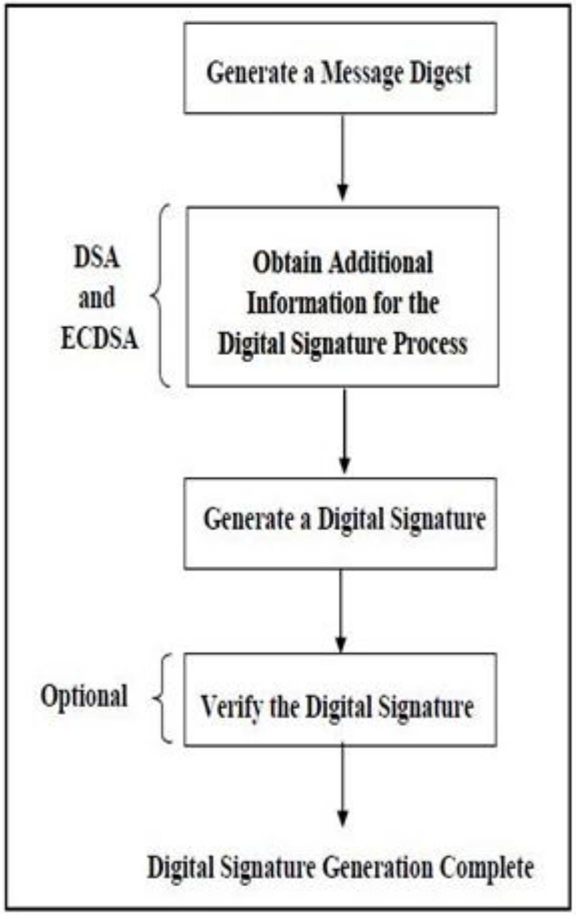
The Figure depicts the steps that are performed by an intended signatory (i.e., the entity that generates a digital signature).

Prior to the generation of a digital signature, a message digest **shall** be generated on the information to be signed using an appropriate approved hash function.

Depending on the digital signature algorithm to be used, additional information **shall** be obtained. For example, a random per-message secret number **shall** be obtained for DSA and ECDSA.

Using the selected digital signature algorithm, the signature private key, the message digest, and any other information required by the digital signature process, a digital signature **shall** be generated in accordance with this Standard.

The signatory may optionally verify the digital signature using the signature verification process and the associated public key. This optional verification serves as a final check to detect otherwise undetected signature generation computation errors; this verification may be prudent when signing a high-value message, when multiple users are expected to verify the signature, or if the verifier will be verifying the signature at a much later time.


Generate a Message Digest
DSA and ECDSA
Obtain Additional Information for the Digital Signature Process
Generate a Digital Signature
Optional
Verify the Digital Signature
Digital Signature Generation Complete

Digital Signature Generation

Hash Function

- **Cryptographic hash function**

  A mathematical transformation that takes a message of arbitrary length and computes it a fixed-length (short) number.

- **Properties**

  Let the hash of a message *m* be *h(m)*

  - For any *m*, it is relatively easy to compute *h(m)*
  - Given *h(m)*, there is no way to find an m that hashes to *h(m)* in a way that is substantially easier than going through all possible values of m and computing *h(m)* for each one.
  - It is computationally infeasible to find two values that hash to the same thing

- Password hashing
  - The system store a hash of the password (not the password itself)
  - When a password is supplied, it computes the password's hash and compares it with the stored value.

- Message integrity
  - Using cryptographic hash functions to generate a MAC