Digital signatures and certificates

...

Digital signature

Digital signature - History

- Authentication technique
- Defined by the U.S. Federal Information Processing Standard (FIPS)
- The standard specified by the U.S. National Institute of Standards and Technology (NIST)
- Multiple specifications over the years
    - Currently in use - FIPS 186-4 specified in 2013

Digital signature - Definition

“The result of cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation” - (Digital signature standard [DDS], 2013)

- The receiver of signed message knows:
  - Who the message is from
  - The message has not been altered

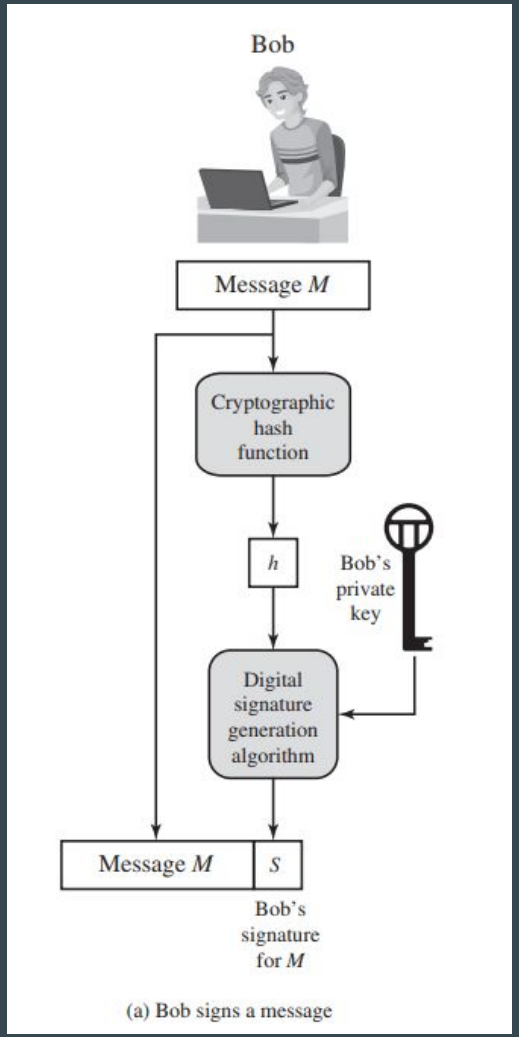
- Signatory non-repudiation = signer cannot deny sending the message
  - Similar to a witnessed handwritten signature on a paper document

Digital signature - Algorithms

- FIPS 186-4 (the current standard) specifies 3 digital signature algorithms
  - DSA - Digital Signature Algorithm - originally approved algorithm in 1996
  - RSA DSA - RSA Digital Signature Algorithm - based on the RSA public key algorithm
  - ECDSA - Elliptic curve digital signature algorithm - based on elliptic-curve cryptography

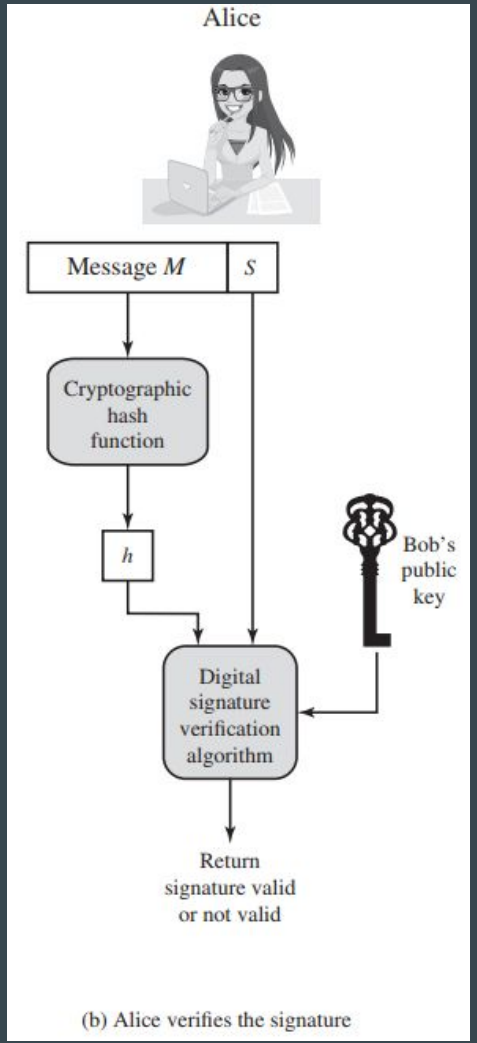
Digital signature - Generic model

- Bob sends a message to Alice
  - Message does not need to be encrypted
  - Needs to prove that is it from him
- Using a hash function (ex. SHA-512) to generate a hash value for the message
- Hash value + Bob's private key -> digital signature generation algorithm
- Signature is attached to the message and sent to Alice



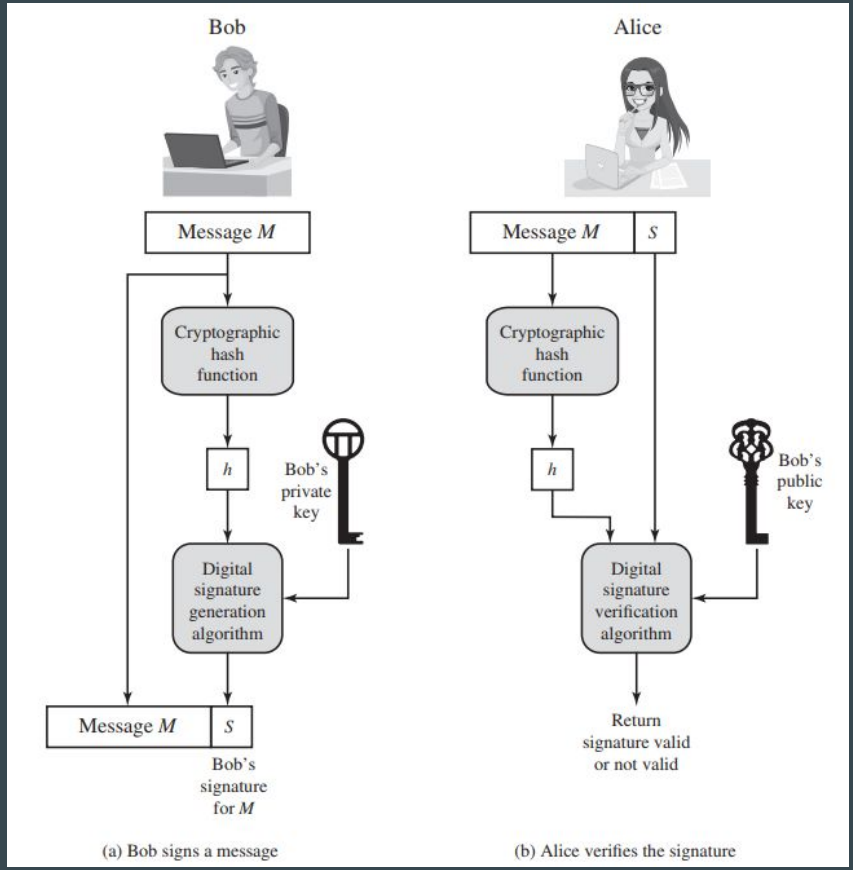
Digital signature - Generic model

- Alice receives Bob's message with signature
- Calculates hash value for the message
- Hash + Bob's public key -> Digital signature verification algorithm
- If signature is valid - proof of authenticity



Digital signature - Generic model

- Proof of authenticity
  - nobody has Bob's private key and could have encrypted the message
- Proof of integrity
  - Impossible to alter the message without Bob's private key
- No Confidentiality
  - Not safe from eavesdropping
  - Message is transmitted in clear
  - Even if encrypted observer can decrypt message using the sender's public key



Public-key certificates

Public-key certificates

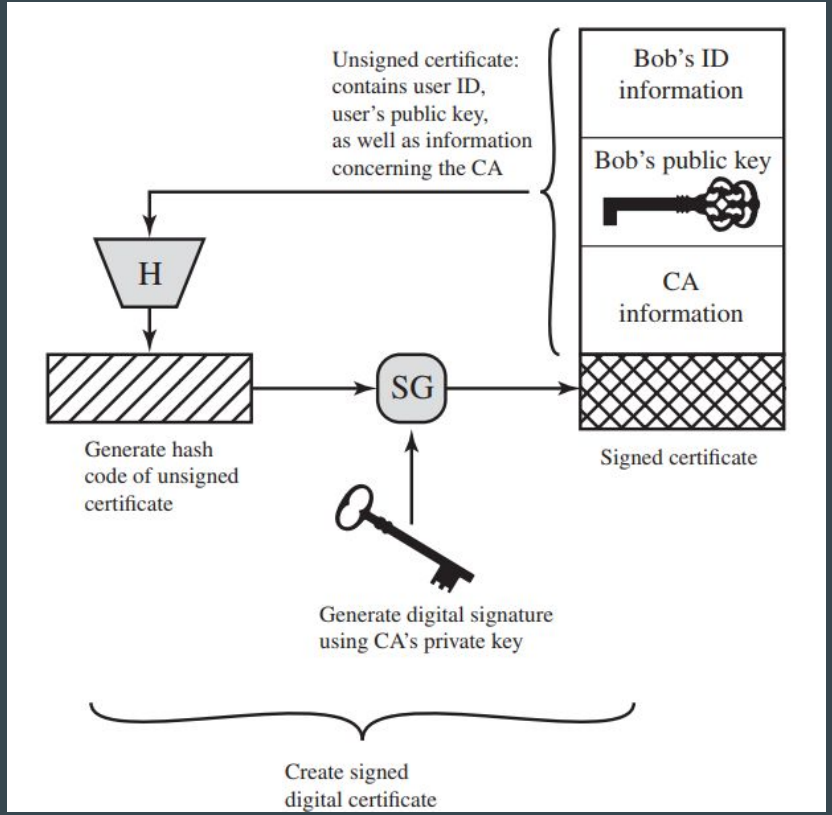
- Issue with public keys
  - They are public
  - Anyone can broadcast their public key
  - Anyone can forge such an announcement
    - Can pretend to be someone else
- Solved by public key certificates

Public-key certificates

- Proof of public-key authenticity
- Consists of public key + user ID + CA's info
- CA - certificate authority
  - Trusted third party
  - Certifies the public key
  - usually a government agency or a financial institution

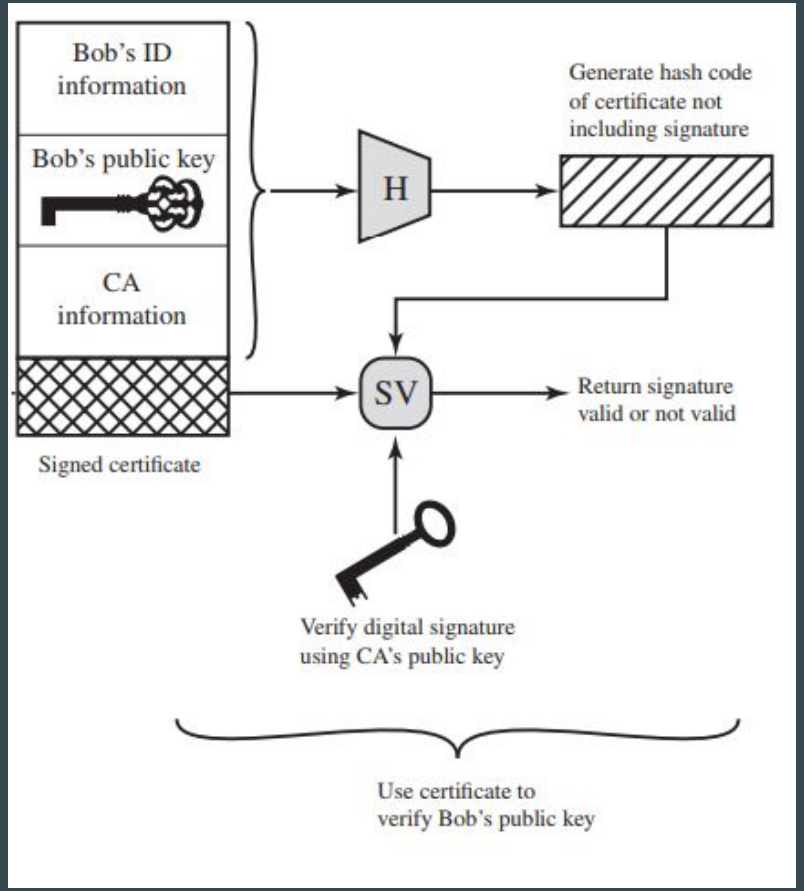
Getting Public-key certificates

- Client creates a pair of keys - public and private
- Client prepares an unsigned certificate
    - user ID + public key + CA info
- Client gives certificate to CA in a secure way (ex. Face-to-face, registered email, web form with email verification)
- CA creates a signature:
    - Generates the hash code of the unsigned certificate
    - Hash value + CA's private key = CA's digital signature
- Unsigned certificate + CA's signature = Signed certificate



Using Public-key certificates

- Client can give the signed certificate to any other user
- Other users can verify that the certificate is valid:
  - Calculate hash code of the certificate (not including the signature)
  - Verify digital signature using CA's public key and signature verification algorithm



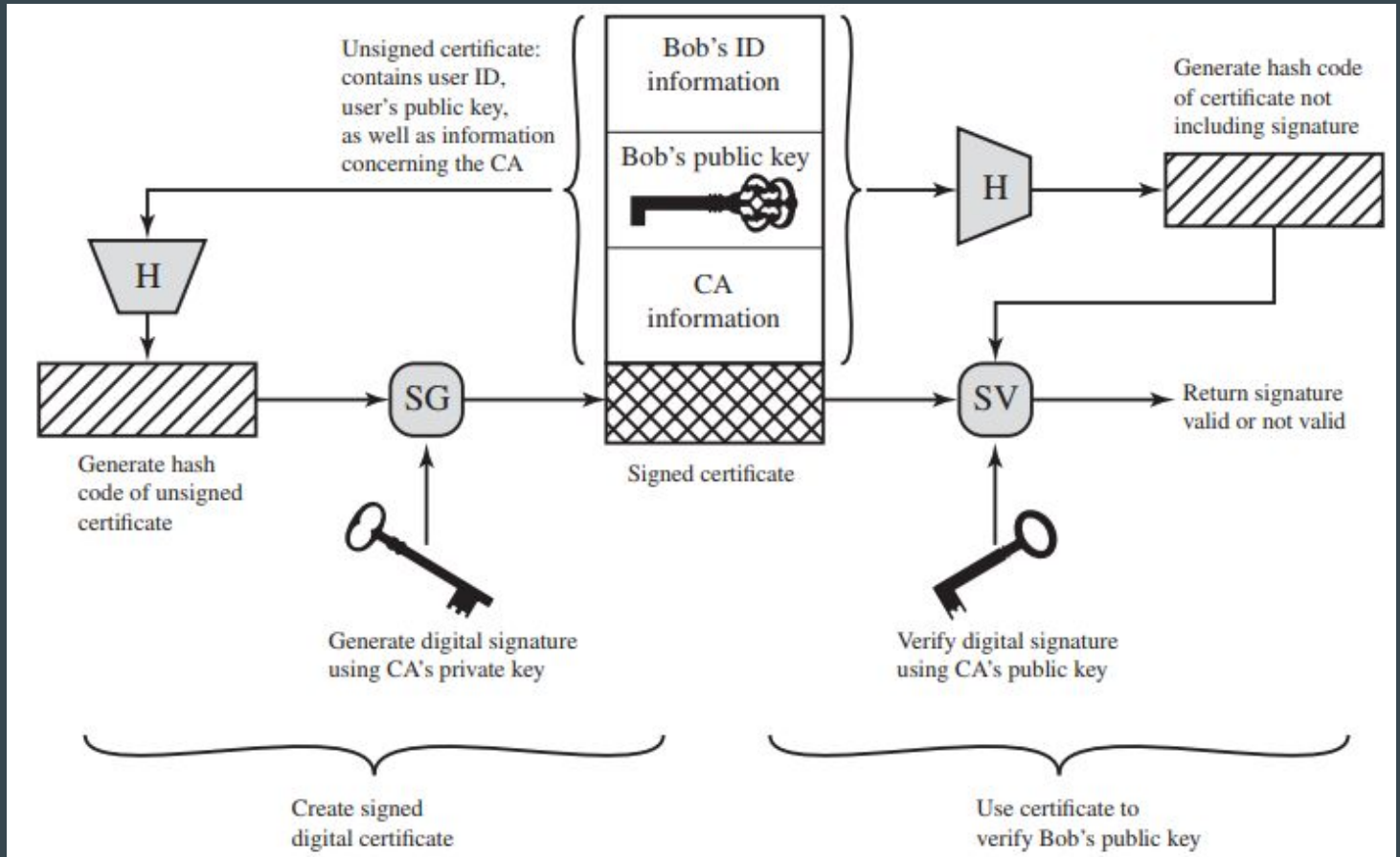


Figure 2.8 **Public-Key Certificate Use**