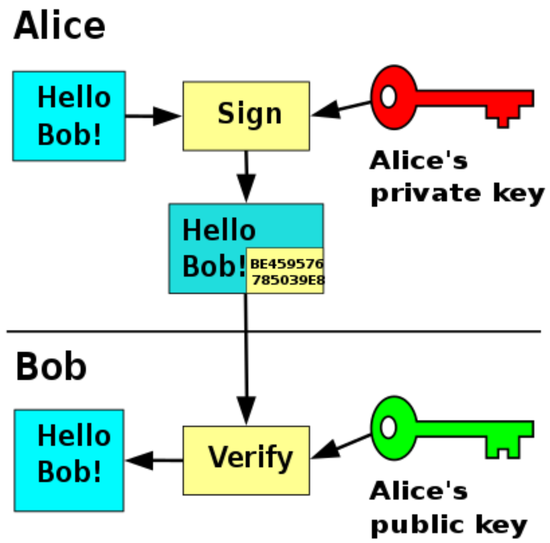
Digital Signatures

Applied Cryptography

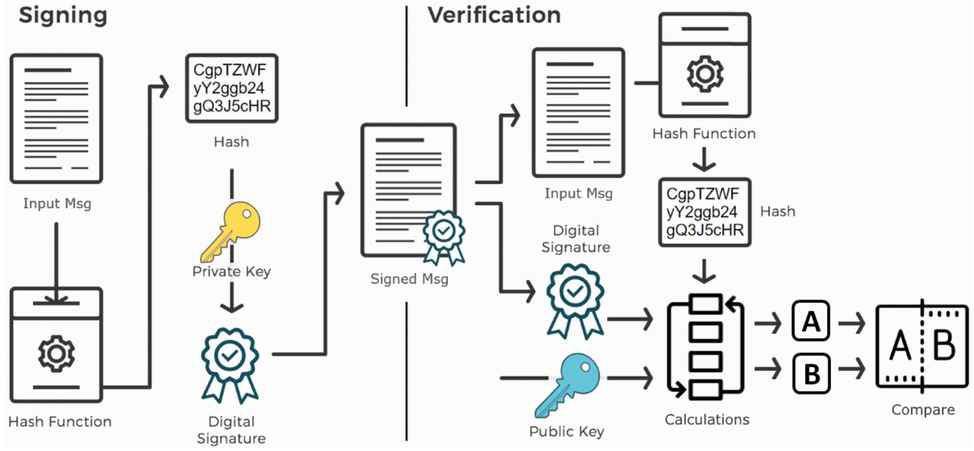
Overview



https://en.wikipedia.org/wiki/Digital_signature

- A digital signature is a block of data that can be used to provide assurances that a message is authentic and unaltered
- They are used in many ways
  - financial transactions
  - software distribution
  - contract management
  - and many more, including having legal standing in many countries because they can provide non-repudiation
- Digital signatures may include timestamps, allowing the signature to remain valid, even if the private key is subsequently compromised
- Digital signatures employ asymmetric encryption to create much stronger assurance of authenticity than a hand-written signature

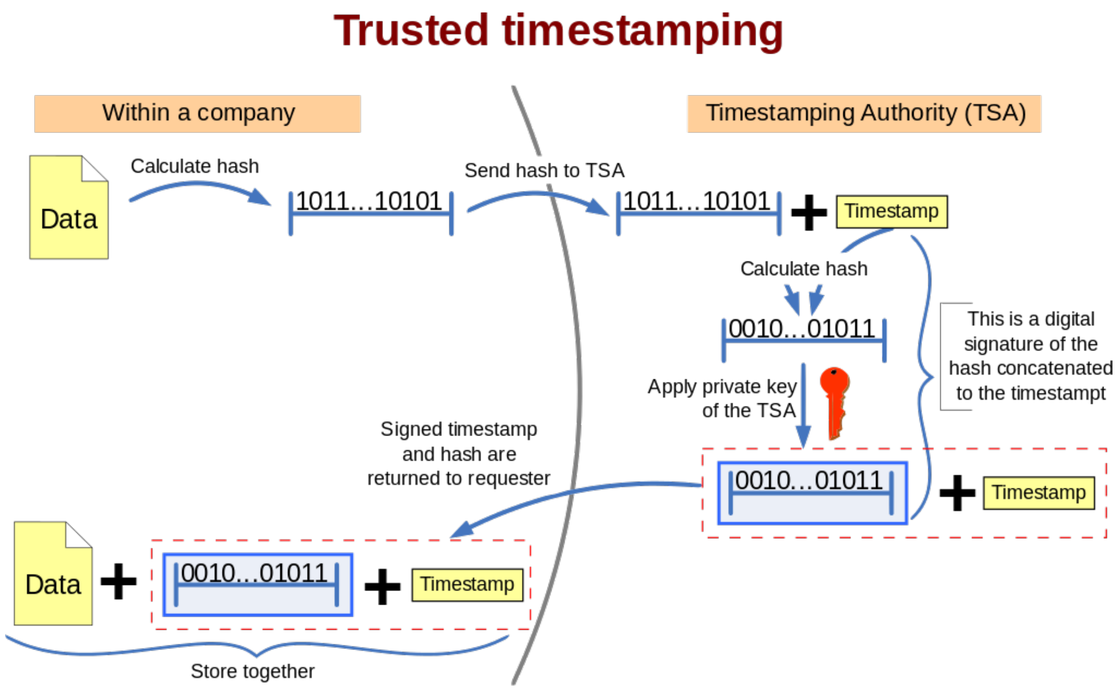
Digital Signature Content



https://cryptobook.nakov.com/digital-signatures

- A digital signature contains an encrypted hash for a message
- It is encrypted with a private key which should be distinct from a private key used for encryption of other kinds of information
- The signature can be decrypted with the author's public key from their signing certificate
- The decrypted hash can be compared to a generated hash for the message being validated
- If they match, this provides an integrity check and an author verification

Digital Signature Time Stamp



https://medium.com/signaturit-tech-blog/how-we-built-a-pki-and-a-tsa-and-got-them-certified-in-6-months-part-1-context-and-problem-9db07f290aac

- The signature may also include a timestamp which can be signed by a Time Stamping Authority
- To include a timestamp, the message author sends the message hash to a TSA who adds the timestamp and encrypts the hash+timestamp with the TSA's private key
- The message recipient can use the TSA's public key to verify the timestamp validity

Signing Certificates

- Used to identify a publisher of code in the case of a code signing certificate
- Used to identify a signatory to a document in the case of a document signing certificate
- Very similar to a web certificate
- The subject is a person or organization (OV/IV type of certificate)
- The certificate is tagged for use in signature verification
- Signing certificates can be signed by any trusted CA

Non-repudiation

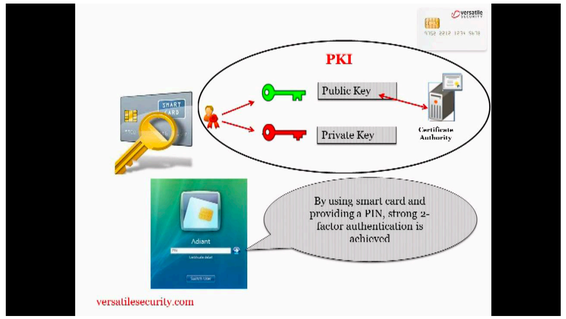
- To provide non-repudiation, a digital signature must include a timestamp from a trusted source
- If the owner of the private key claims the private key to be safe and secure up to that point in time then they cannot claim they did not create the message containing that signature
- The non-repudiation principle is at the heart of the legal standing of digital signatures in countries that legally recognize digital signatures
- To be able to demonstrate that the key has been compromised requires the key holder to publish a key revocation
- Note that authentication of a message source does not imply receipt of the message from that source, only that the original message was created by that source
- Non-repudiation is unrelated to message meaning and only makes claims about the specific data content of the message

WYSIWYS

- When you sign a piece of information, you are vouching for that content
- Content is more than the set of bits in a piece of information
- If you sign a document that is a Word document, you may be signing content you have no awareness of because a single Word document can be presented differently on different computers
- Some digital signature systems include their own viewer and signing tool in the attempt to ensure that when you sign something, you have some assurance that you have full visibility of the complete content of the thing you are signing
- Note that this issue is an issue of semantics, and therefore also includes concerns about the interpretation of the data which can be related to the presentation of the data

- **WYSIWYS**
  - What You See Is What You Sign

Smart Cards



https://www.youtube.com/watch?v=GfPcz1y0JoE

- A private key is generated on or for a smart card, which contains a cpu, some memory, and non-volatile storage for both code and private keys and many also contain additional biometric information
- Smart cards typically require a PIN number to unlock the stored private key in order to use the card
- The card keypair is used to obtain a certificate from a trusted CA, the certificate then identifies the card
- Use of smart cards requires applications that are aware of the specific hardware and API details of the smart card in use (e.g. they send a message to the smart card for encryption - the resulting encrypted message is decrypted using the public key from a certificate that is trusted - the certificate provides the identity attached to the card)
- The private key is only kept on the smart card and cannot be exported from it
- If the key (smart card) has been lost or compromised, the certificate containing the associated public key is revoked to make the card an orphan

MACs and HMACs

- A MAC is a block of data attached to user data that can be used to verify the data has not been altered and is authentic
- HMACs are keyed-hash message authentication codes that incorporate symmetric encryption and hashing functions
- HMACs are used to ensure integrity of communications and are used in IPSec, TLS, and SSH
- The shared secret key used with HMACs are established during key exchange
- HMACs only exist for the duration of a message transfer and are only used to secure the transfer, as opposed to signatures which are treated as part of the message

- **MAC**
  - Message Authentication Code
- **HMAC**
  - Keyed-Hash MAC

Signing Services

- There are companies around the world providing signing services online which create and manage keys and certificates for users
- Yozons patented this in 2001 and their USA patents have expired since then so this technology is now in wide use
- The EU has a different set of laws governing this than the USA or Canada, but they all allow legally binding signatures made using this technology
- To use these services, a user creates an account with a signing service, and all signing and signature verification is performed on the service's websites
- Docusign is a very popular digital signing service provider used widely for real estate and other legal transactions in North America (e.g. estate administration), services like these can manage all aspects of document signing, including transmission of documents requiring more than one signature
- Private eSign servers are also out there, signserver and openesign are examples - these are java based and while they are cross-platform, they are also non-trivial to install