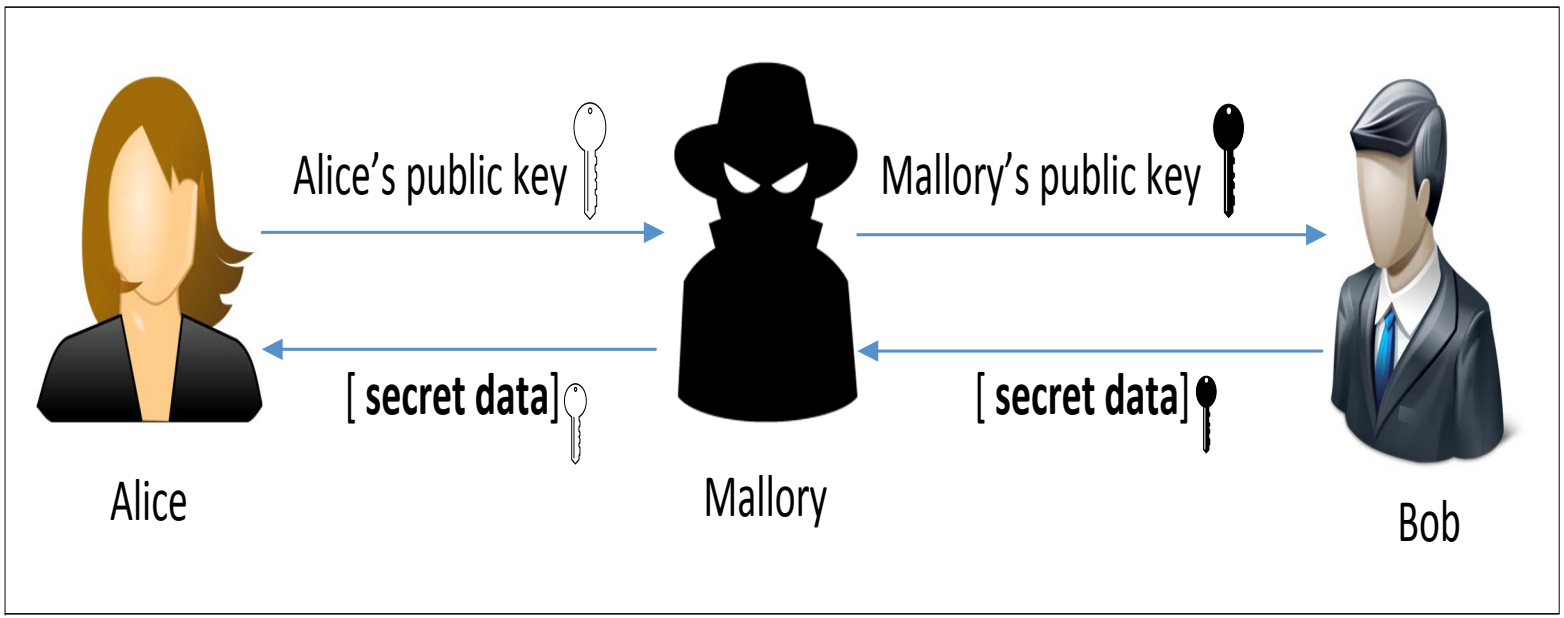
Agenda

- Public Key Infrastructure (PKI) - Part 2

Terminology

- `Certificate Authority`: verify the subject and issue digitally signed certificates.
- `Public Key Certificate`: certifies the ownership of a public key.

Man-in-the-Middle Attack



Digital Signature

- Based on public key cryptography: signed with the signer's private key, verified by anybody who has the signer's public key.
- Once a message is signed, altering the content of the message would make the signature invalid.

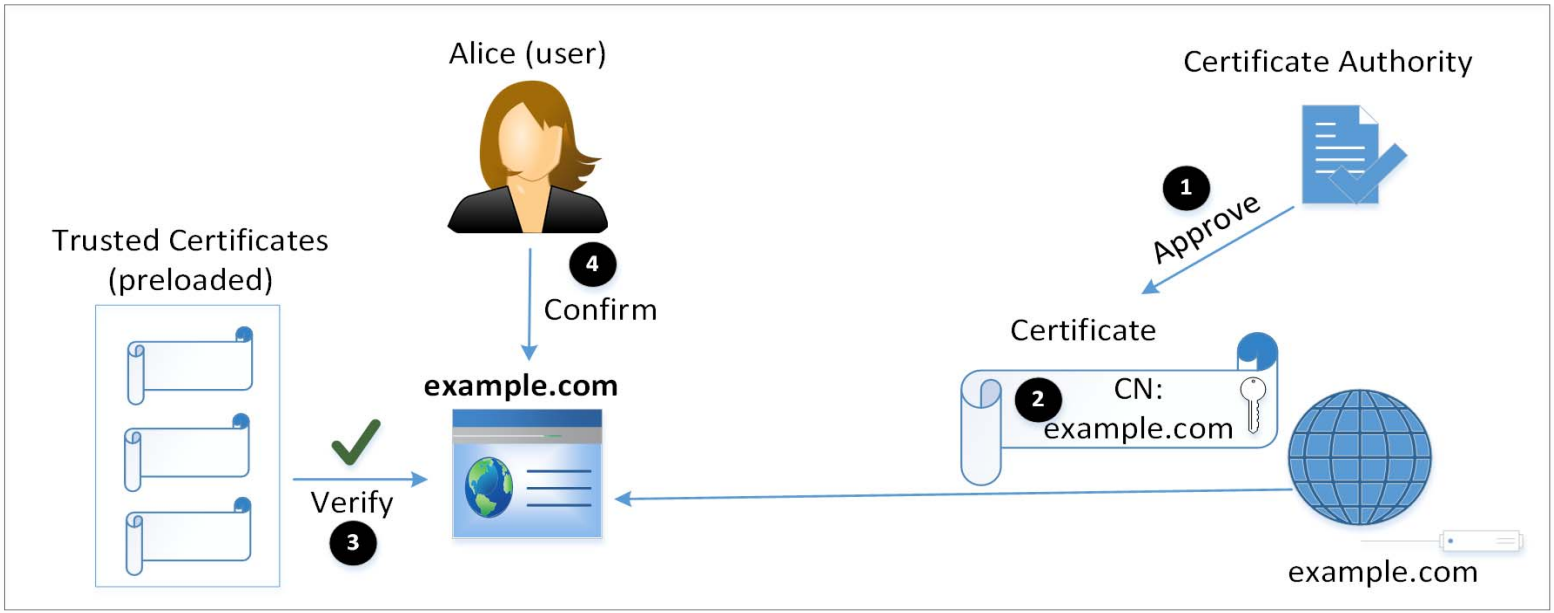
Public Key Certificate

- Consists of a public key, identity of the owner, signature of a trusted party (i.e., certificate authority).
- Recipient can verify the signature to ensure the integrity of a certificate.

Certificate Authority Market Share (2017)

- Comodo (42.2%)
- IdenTrust (25.2%)
- Symantec (15.0%) (In 2010 Symantec bought the VeriSign certificate authority.)
- GoDaddy (7.6%)
- GlobalSign (4.8%)
- DigiCert (2.3%)

Public Key Infrastructure



References

A large portion of the material is adapted from:

- Computer Security - A Hands-on Approach by Wenliang Du
- Usage of SSL certificate authorities for websites: https://w3techs.com/technologies/overview/ssl_certificate/all