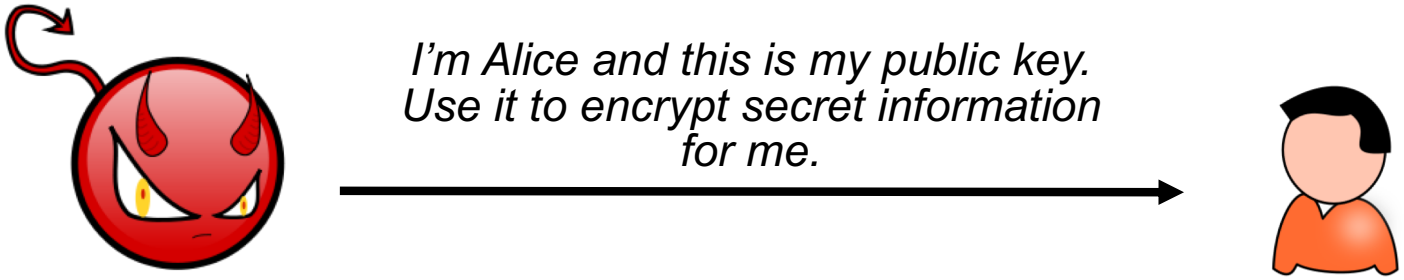
Certificates and Public Key Infrastructures

IV1013

Peter Sjödin

Public Key Authentication

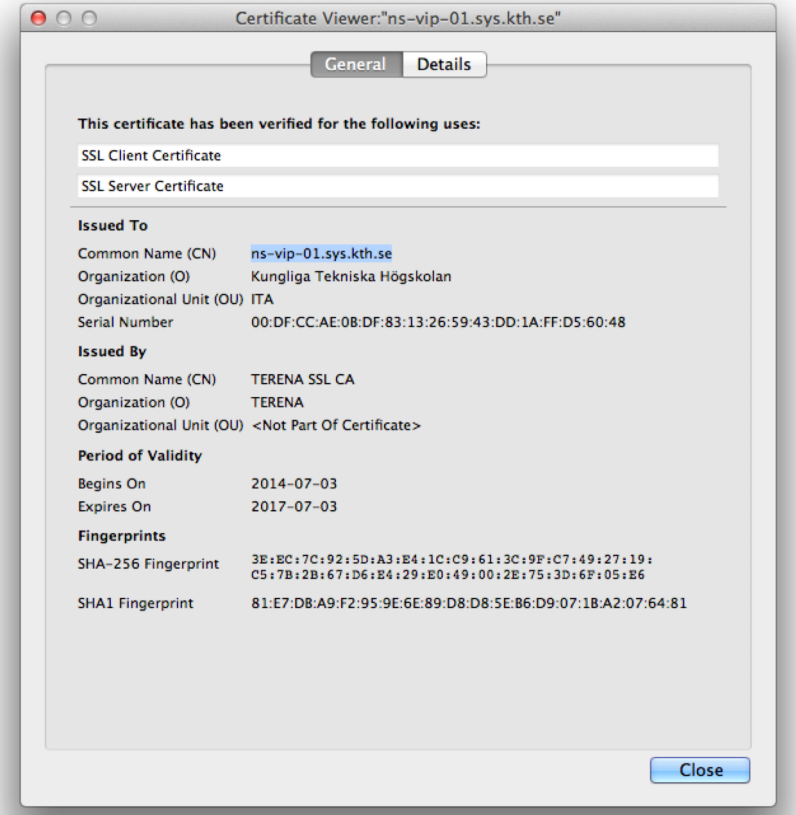


- How can I trust a public key?
  - More precisely, how can I verify the owner of a public key?
- Use digital signatures!
  - Non-forgeable document
  - Authenticity, integrity

- Question: What should be in the signed document?
- Question: Who should sign the document?

Certificate

- A document that associates a user (identifier) with a public key
- Digitally signed by a trusted third party
  - Certificate Authority (CA)



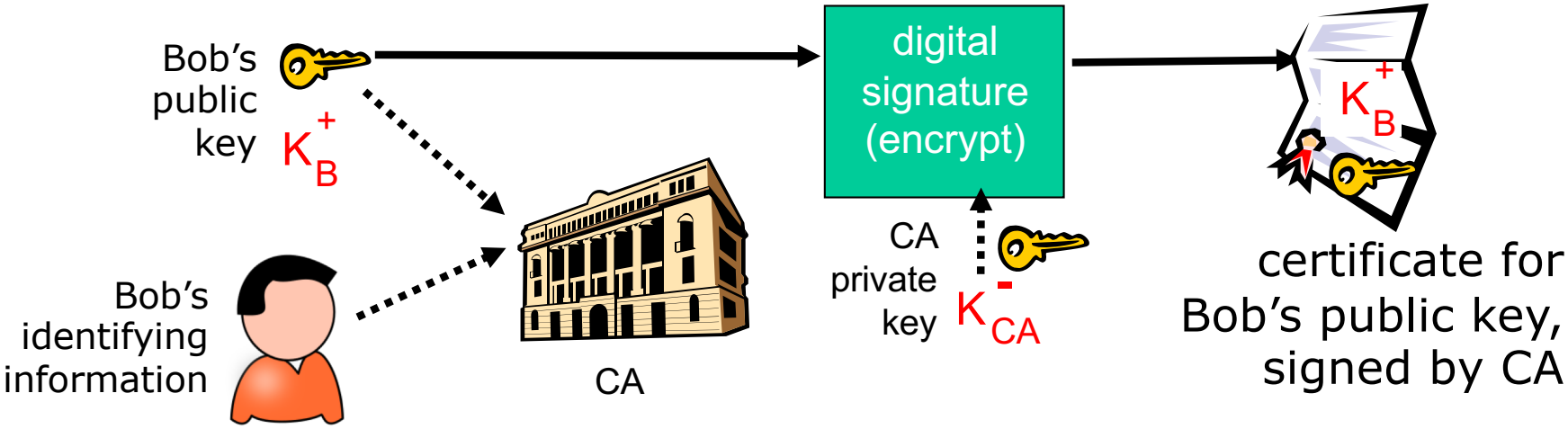
Certificate Authority (CA)

Bob registers its public key with CA

- Bob provides "proof of identity" to CA

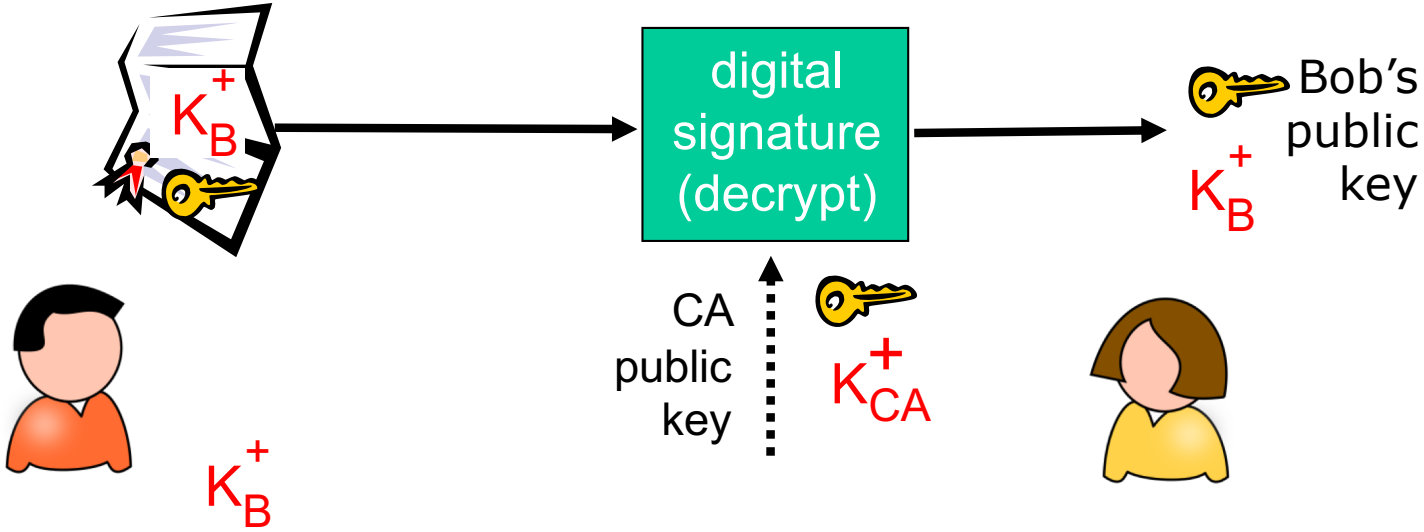
CA creates certificate that binds Bob's identity to the public key

- certificate containing Bob's identity and public key digitally signed by CA



Certification Validation

- When Alice wants Bob's public key:
  - get Bob's certificate (from Bob or elsewhere)
  - apply CA's public key to Bob's certificate, to get Bob's public key



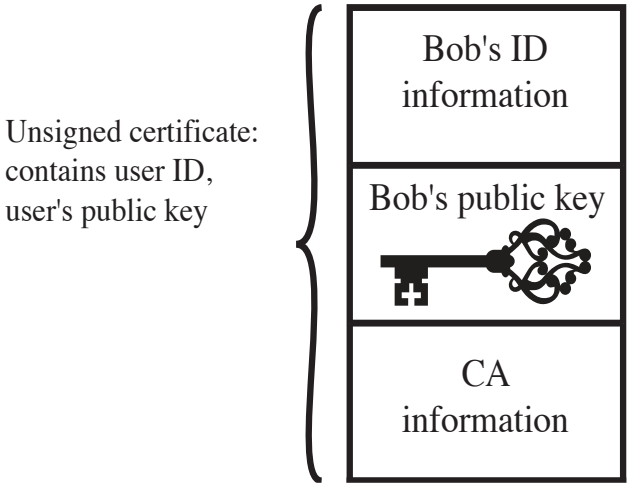


Figure 4.3 Public-Key Certificate Use

From W. Stallings, Network Security Essentials, 5th ed.

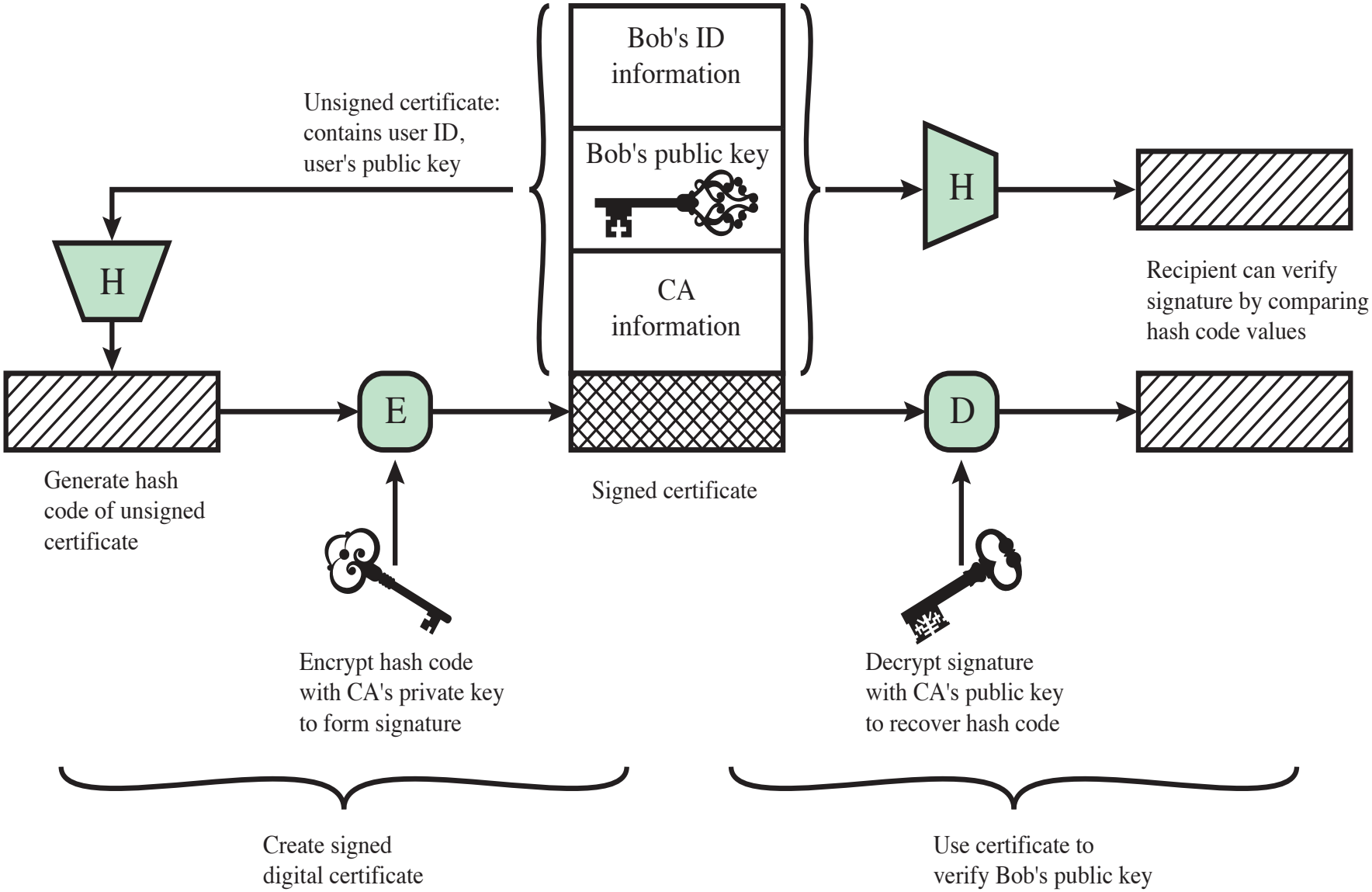


Figure 4.3 Public-Key Certificate Use

From W. Stallings, Network Security Essentials, 5th ed.

Certificate Example

X.509 certificate in Firefox on Mac OS X

Certificate Viewer:"ns-vip-01.sys.kth.se"

General | Details

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	ns-vip-01.sys.kth.se
Organization (O)	Kungliga Tekniska Högskolan
Organizational Unit (OU)	ITA
Serial Number	00:DF:CC:AE:0B:DF:83:13:26:59:43:DD:1A:FF:D5:60:48

Issued By

Common Name (CN)	TERENA SSL CA
Organization (O)	TERENA
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	2014-07-03
Expires On	2017-07-03

Fingerprints

SHA-256 Fingerprint	3E:EC:7C:92:5D:A3:E4:1C:C9:61:3C:9F:C7:49:27:19: C5:7B:2B:67:D6:E4:29:E0:49:00:2E:75:3D:6F:05:E6
SHA1 Fingerprint	81:E7:DB:A9:F2:95:9E:6E:89:D8:D8:5E:B6:D9:07:1B:A2:07:64:81

Close

info about certificate owner

Serial number (unique to CA)

Information about CA (“issuer”)

Validity period

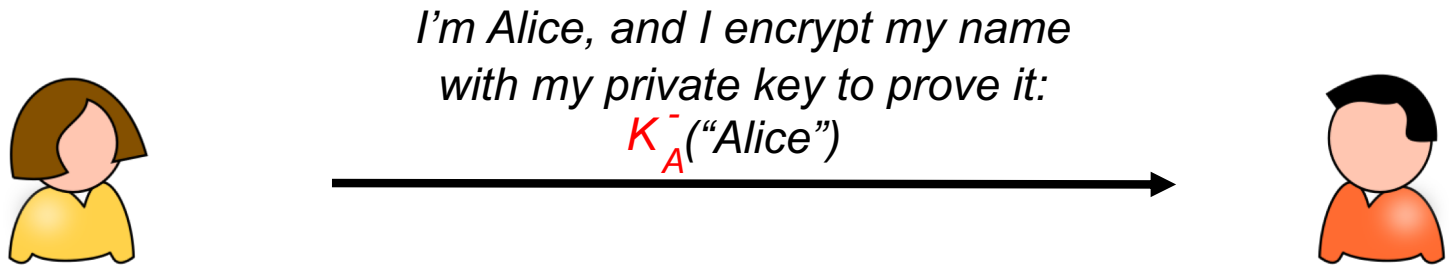
Digital signatures by CA

User Certificates

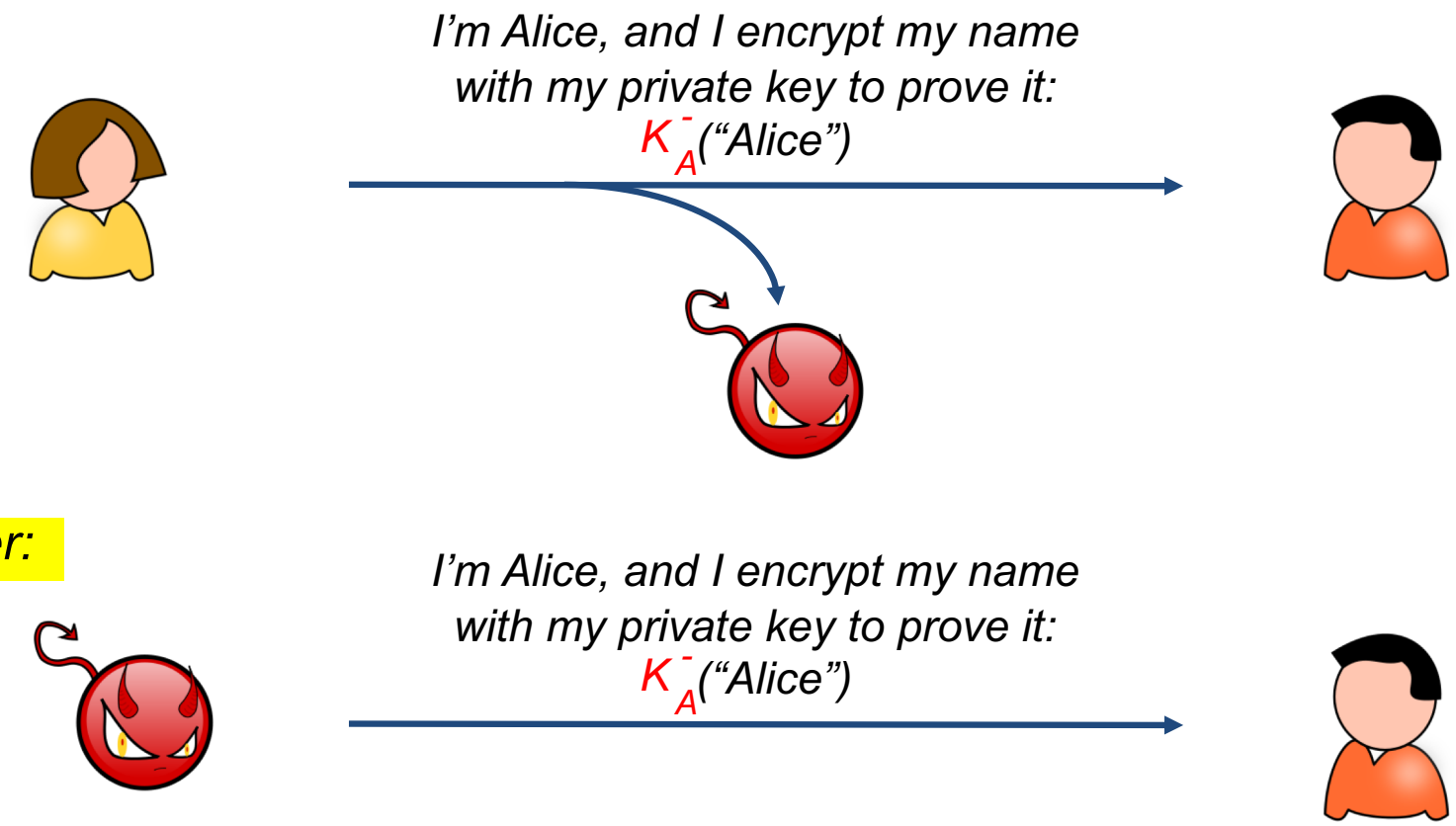
- Authenticity
  - Anyone with access to the CA's public key can verify a certificate
- Integrity
  - Only the CA can modify a certificate
- Availability
  - Certificates are unforgeable, and therefore can be stored and published without further protection

Public Key Authentication (Revisited)

- Still not done!
- How can we identify the owner of a public key?
- Only the owner can encrypt with the matching private key!
  - To authenticate herself, Alice presents information encrypted with her private key

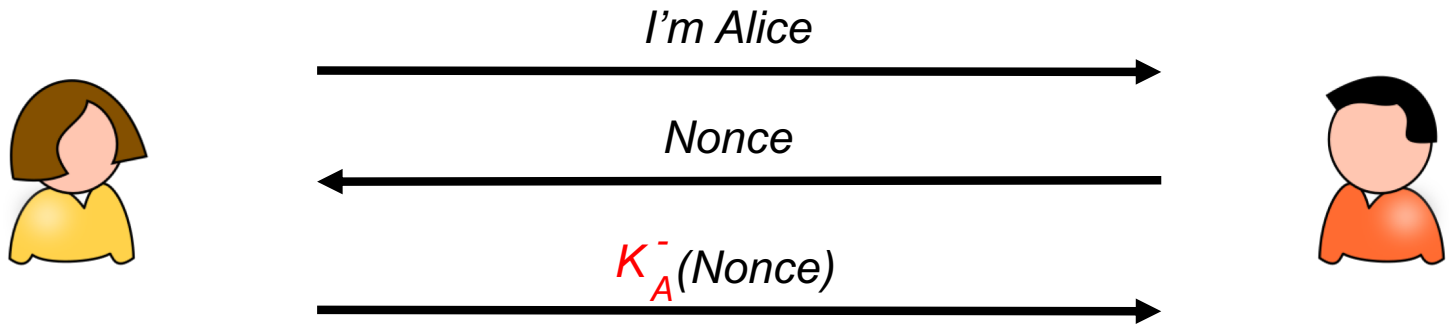


Replay Attack



Attacker records the message, and repeats (replays) it later to make Bob believe he is communicating with Alice.

Challenge Protocol with Nonce



- Bob *challenges* Alice to encrypt fresh material with her private key
- Nonce – number used once. Could be:
  - Sequence number
  - Timestamp
  - Random number
  - …

Key Distribution and Authentication with Public Key Encryption

- Certificate Authorities
- Public Key Infrastructures

Certification Authorities

- One CA for everyone is impractical
- So we want to use multiple CAs
- Deploy a Public Key Infrastructure (PKI)

Who is in charge of what?

Where can we find the certificate of a given user?

How are certificates transmitted over the network?

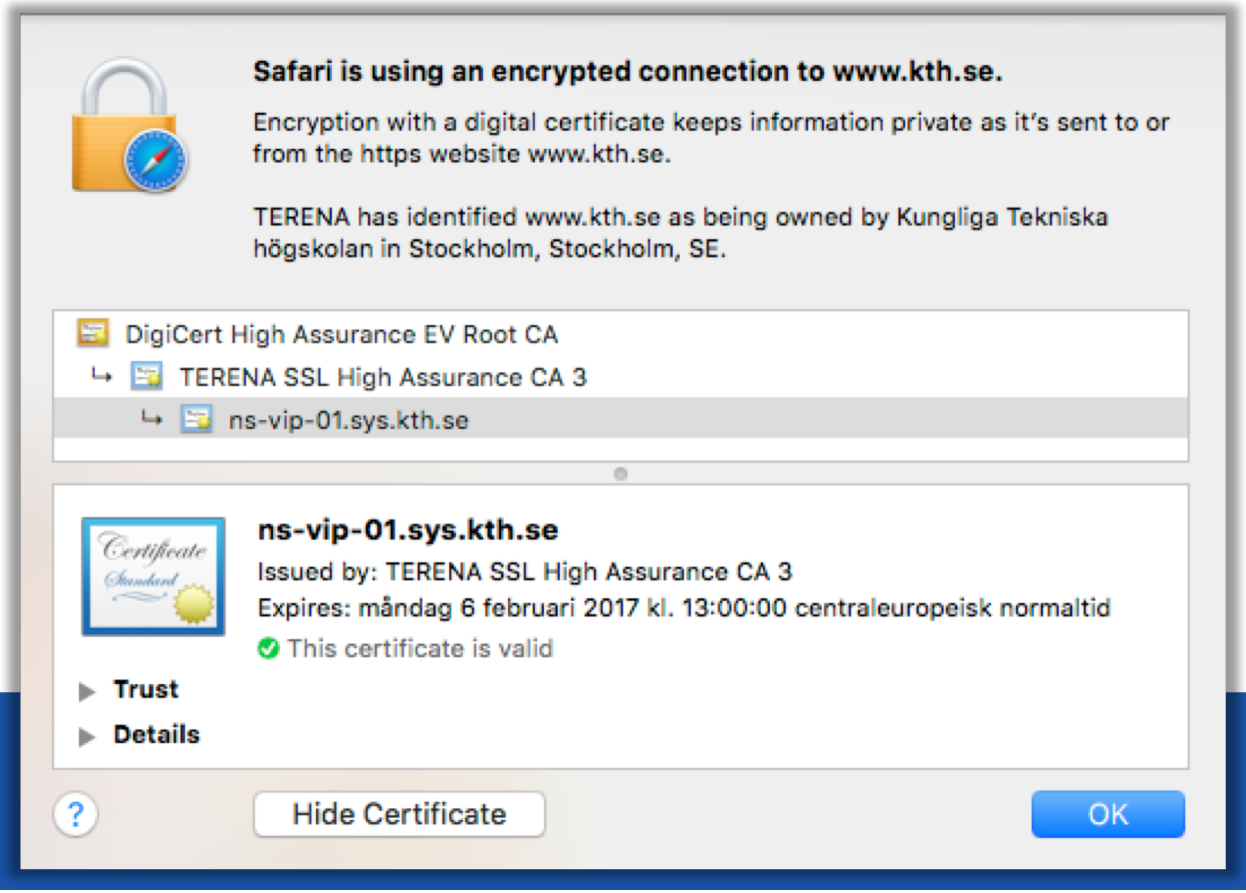
What is the certificate format?

Hierarchical Approach

- Use a trusted root authority
  - For example, Verisign and DigiCert
- Everybody must know the public key for verifying root authority's signatures
  - Root authority signs certificates for lower-level authorities, lower-level authorities sign certificates for individual networks, and so on

Certificate Chain

- KTH web server's certificate signed by TERENA
- TERENA's certificate signed by DigiCert
- DigiCert's certificate signed by DigiCert – self-signed

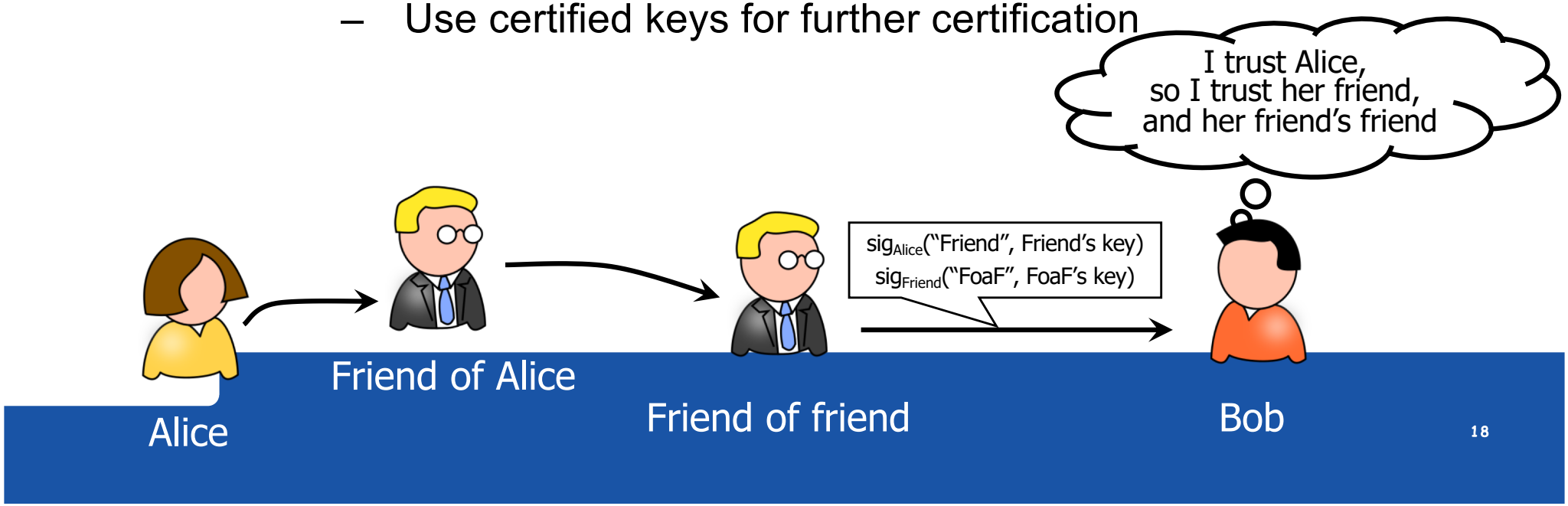


Oligarchy Model of Trust (Web model)

- A set of trusted CAs are pre-installed and trusted.
  - DigiCert, for instance
  - Large CA vendors pay to get pre-installed in browsers
- New CAs can be added by “clicking ok”
  - “Do you want to ... ? “
- I currently trust 46 CAs in my browser
  - Well, do I really?
  - What happens if a single of these CAs becomes compromised?

Alternative: “Web of Trust”

- A.k.a. ”Anarchy model”
  - Used in PGP (Pretty Good Privacy)
- Instead of a single root certificate authority, each person has a set of keys they “trust”
  - If public-key certificate is signed by one of the “trusted” keys, the public key contained in it is considered valid
- Trust can be transitive
  - Use certified keys for further certification



How do we find a certificate

- If Bob wants to send an encrypted message to Alice, how does he find her certificate?
  - Alice could give it to Bob.
  - Use a directory service where Bob can search for certificates.
    - DNS
    - X.500/LDAP (Lightweight Directory Access Protocol)
  - …

Certificate Revocation

- Revocation is very important
- Many valid reasons to revoke a certificate
- Private key corresponding to the certified public key has been compromised
- User stopped paying certification fee to this CA
- CA's certificate has been compromised

Expiration is a form of revocation, too

- Many deployed systems do not bother with revocation
  - Browsers may not check for revocation, by default
- Re-issuance of certificates is a big revenue source for certificate authorities

Certificate Revocation Mechanisms

Online revocation service

- When a certificate is presented, recipient goes to a special online service to verify whether it is still valid
  - Like a merchant dialing up the credit card processor
- Online Certificate Status Protocol (OCSP), RFC 2560

Certificate revocation list (CRL)

- CA periodically issues a signed list of revoked certificates
  - Credit card companies used to issue thick books of canceled credit card numbers
- Can issue a “delta CRL” containing only updates
- Download into browser

Questions

The root CA signs its own certificate. What is the point of self-signed certificates (if any)?

An attacker successfully impersonates Bob and gets a certificate (as Bob) from a CA. What can Bob do?

An attacker gets hold of the private key of a CA and issues fake certificates. What can the CA do?

Nonces are central to authentication with public keys. It is a theoretical concept though. How can nonces be approximated in practice? Discuss possible implementations, advantages and disadvantages.

Summary

- Certificates
  - Document binding user identity and public key
  - Validity assured through digital signature by Certificate Authority
- Public Key Infrastructure
  - Distributed system for certificate management
  - Relationship among CAs
  - Certificate format
  - Certificate directories
  - Certificate authentication
  - Certificate revocation
- …