8.4. Public Key Infrastructure

Most important components:

- Certificate issuance
- Certificate revocation
- Key backup / recovery / retrieval
- Time stamping

PKI-enabled services:

- Secure communication
  (PGP, GPG, SSL, TLS, VPN, ...)
- Access control
  (privilege management, ...)
- Privacy architecture
  (anonymous certificates, anonymous web browsing)

Example SSL:

A (client) wants to purchase something from B (server).

Client A		Server B	
	hello, I'm A →		Hello phase (no cryptography)
	← hello, I'm B		
	← $PK, sig_{CA}(PK)$		B sends his PK, signed by a trusted authority
verify PK			
generates MS	$y = e_{PK}(MS)$ →		A generates a master secret, sends it to B encrypted by PK of B
$(K_1, K_2) = h(MS)$		$MS = d_{PrK}(y)$ $(K_1, K_2) = h(MS)$	

K_1 is used to authenticate data by a MAC(K_1)

K_2 is used for en/decryption (e.g. DES, triple DES, AES, IDEA, ...)

Problem: How to accept the identity of a party that you never met.

Conventional face-to-face identification is by a trusted third party (friend) who presents the two parties to each other.

Such a presentation protocol is also required for cryptographic purposes.

The presenting party in the cryptographic environment is called a certification authority (CA).

The management of the CAs requires a public key infrastrucure (PKI).

Borrowing from slides of Eli Biham, see http://www.cs.technion.ac.il/ cs236506/#slides

RWTH RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

During face-to-face presentation, the presenter gives the relation between the name and the face of a person, together with some side information (friend, relative, employee, etc.).

For cryptographic use the CA should give the relation between the public key and the identity of a party.

This information should be transmitted authenticated from the CA to the receiver, e.g., signed under the widely known public key of the CA.

The signed information is called a certificate.

It is not necessary that the receiver communicates directly with the CA. Instead, the CA can sign all required information of some potential sender. The sender may publish the signed information widely, or send it to a specific party he wants to communicate with.

Certificates (cont.)

RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

A certificate includes:

- The CA name
- A sequential number of the certificate
- The public key of the user
- The identity of the user
- The issuing date
- The expiration date
- The signature of the CA on all the above.

The CA should maintain a blacklist of canceled certificates, e.g., after the private key of some user has been discovered and a new key pair has been generated.

After the ~~validation~~ expiration date entries in the blacklist may be deleted, since the certificates become invalid anyway.

The PGP Hierarchy

RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

In the PGP hierarchy, every user is also a CA, and other users can select which CAs they trust and which they do not trust.

As a CA a user signs certificates to his friends. His signature ensures that he recognizes the friend, and checked his identity. It does not mean that the friend is trustworthy.

Each user collects as many certificates as he wants to. To prove his identity, he publishes or sends the collected certificates to other parties.

Receivers can select their own trust scheme.

- Trust certificates of certain CAs unconditionally.
- Trust some CAs only conditionally (sufficiently many certificates, additional certificates required).
- They can design their own certificate trust scheme in any way.