Chapter 5

5.1 Public key infrastructure (PKI)

5.1.1 TLS protocol

TLS is a software, which more than 95% of secure connections over internet uses.
It's old name is SSL, since version 3.0 its called TLS (Transport Layer Security).

Typical services which use TLS are f.e net banks, ecommerce, newspapers, email.

5.1.2 TLS is a hybrid cryptosystem

A hybrid cryptosystem uses many algorithms for different purposes.
TLS is a typical hybrid cryptosystem with following functions:

1. Authentication
2. Key exchange
3. Encryption of transmitted data
4. Digital signatures

5.1.3 Public key infrastructure

TSL requires a **Public Key Infrastructure** consisting of hierarchical network of Certification Authorities (CA's)

Every server needs a certificate from some member of CA network. Certificate contains the public key of the server. Certificate is digitally signed by the CA . The purpose of the certificate is to ensure the autenticity of the web server to avoid Man in the Middle attack. A link to one certificate provider: https://www.sectigo.com/products

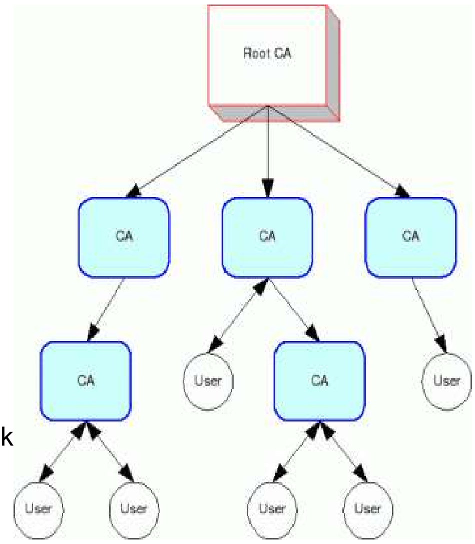
Hierarchy of CA network

The public keys of web servers are issued by some CA.

CA network maintains a register of public keys.

TLS –servers get their public keys as digitally signed, standard form certificates.

Objective of the system is that there cannot be actors in web, who would deliver false public keys as in man-in-the-middle attack authorization.



Chain of Trust. Root CA’s

Big demand of certificates requires lots of certificate providers. CA networks has different levels.
At the top of the hierarchy are **root CAs**, which issue certificates for the second level CAs etc.

If server X:s certificate is from CA which is not in X:s list of trusted CAs,

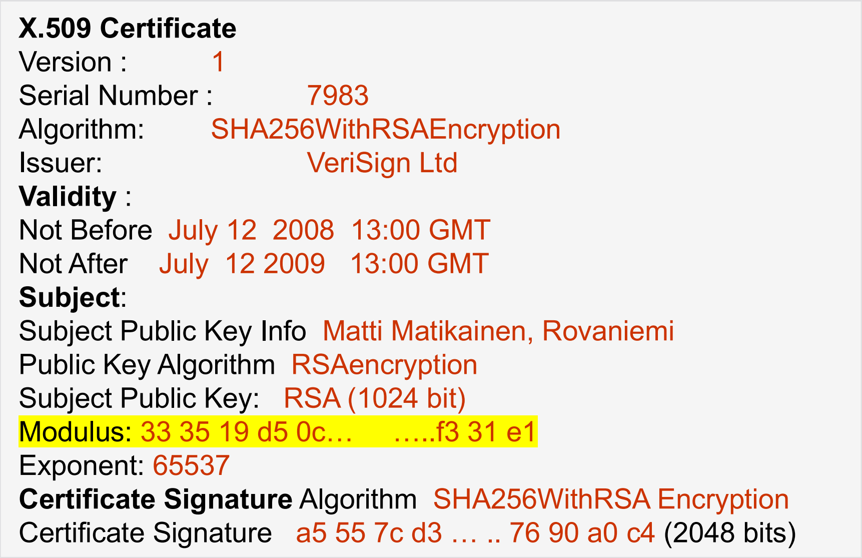
X may need to follow the whole chain of trust up to the root CA. Root CA at the top has no certificate.

The public key of the root CA is hidden in the code of operating system or browser.

Standard certificate form X.509

The most important information in the certificate is the public key of the server. Other information in certificate is validity time, servers name, CA’s name, digital signature of CA which ensures the authenticity of certificate, digital signature algorithm.

In the example certificate below the public key is highlighted.

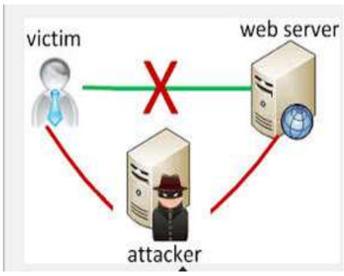


X.509 Certificate
Version : 1
Serial Number : 7983
Algorithm: SHA256WithRSAEncryption
Issuer: VeriSign Ltd
Validity :
Not Before July 12 2008 13:00 GMT
Not After July 12 2009 13:00 GMT
Subject:
Subject Public Key Info Matti Matikainen, Rovaniemi
Public Key Algorithm RSAencryption
Subject Public Key: RSA (1024 bit)
Modulus: 33 35 19 d5 0c… …..f3 31 e1
Exponent: 65537
Certificate Signature Algorithm SHA256WithRSA Encryption
Certificate Signature a5 55 7c d3 … .. 76 90 a0 c4 (2048 bits)

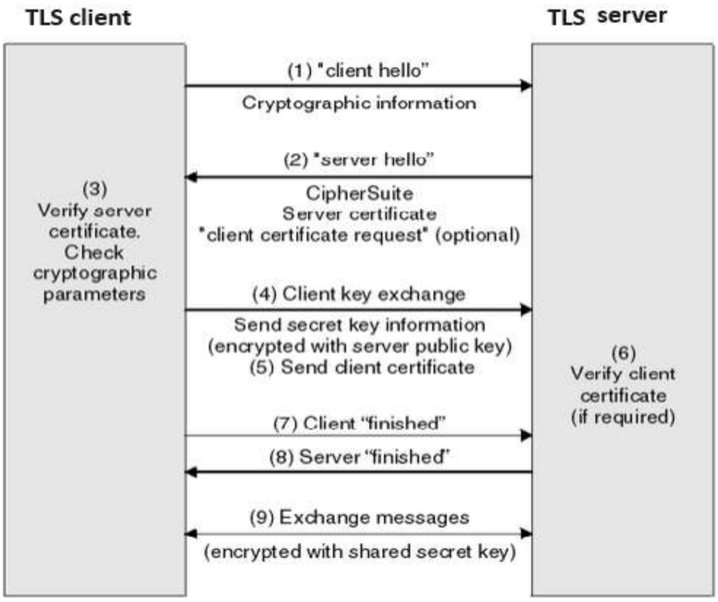
Man in the Middle Attack

CAs and certificates are intented to prevent the **Man in the Middle attack**, where a third party E comes between A and B pretending to be the other party to both directions sending them E’s own public key.
E can read and alter messages.

CA -network is built to prevent distribution of false public keys. **The certificate contains the authentic public keys signed by CA with a strong digital signature**, which in theory is impossible to forge.



5.1.4 TLS sessions phases


TLS client
TLS server
(1) "client hello"
Cryptographic information
(2) "server hello"
CipherSuite
Server certificate
"client certificate request" (optional)
(3)
Verify server certificate.
Check cryptographic parameters
(4) Client key exchange
Send secret key information
(encrypted with server public key)
(5) Send client certificate
(6)
Verify client certificate
(if required)
(7) Client "finished"
(8) Server "finished"
(9) Exchange messages
(encrypted with shared secret key)

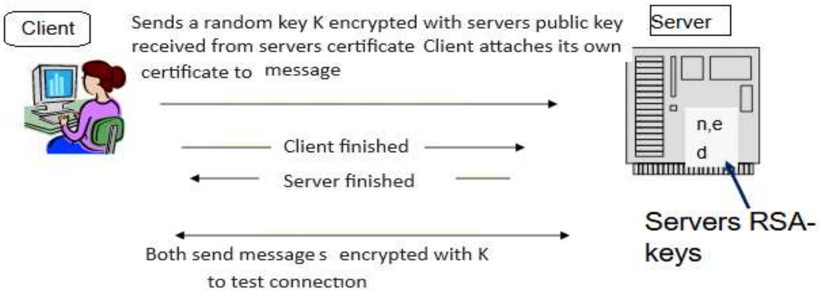
1. Handshake

When the clients browser contact the server, it gives information about its highest TLS -version and suitcase of available algorithms: f.e ”Highest version is TLS 1.1. Supported algorithms AES, RSA, sha1RSA Servers answer fix the configuration of TLS version and algorithms.

2. Authentication is combined with the key exchange protocol

At first the client checks the digital signature of the CA in the servers certificate. The CA which has signed the certificate must be found in the clients list of trusted CA:s.

Then the client creates a random symmetric key K and sends it to the the server encrypted with servers public key, which is found in its certificate.
Case1: two-way authentication with keys:
If the clients also has RSA keys and certificate, the clients signs the key message with its own private key and sends its own certificate to the server. The server verifies the digital signature of client in the key message.
Case2: A private person may also authenticate himself in an oldfashioned way using UserID and password.


Client
Sends a random key K encrypted with servers public key received from servers certificate Client attaches its own certificate to message
Server
n,e
d
Client finished
Server finished
Servers RSA-keys
Both send message s encrypted with K to test connection

Methods of key agreement in TLS are either RSA exchange or ECDHE
Now encryption of messages with AES can start.

In newest TLS versions authentication and key exchange are separated.

3 Encryption of messages

Transmitted data is encrypted using a block cipher, which is mostly AES

5.1.5 S/MIME email encryption protocol

Email without encryption is no more secure than a post card. When it moves through the net, it can be read at every nod of the network.

According to the statement of Finlands data privacy commissioner (Dnro 1431/41/2007) a Finnish company must not send personal data of clients and employees with not encrypted email. Name and personal ID in the same unprotected email is not allowed.

Outlook and Outlook365 email software support email protection with S/MIME- protocol.

In order to use secure email you need to get RSA keys with ”Get Digital ID” option.

S/MIME works very much in the same way as TLS in web services

* Email is encrypted with block cipher , usually AES

* AES key is sent using RSA exchange attached to the email.

* The whole ”package” is encrypted with senders private key to prove senders identity

* The recipient decrypts first the ”package” with senders public key, then attached key message is decrypted.

* Finally recipient decrypts message from AES encryption**.**

The measures ensure the confidentiality of the message and authenticity of sender.

5.1.6 Authentication: concepts and terminology

”**Authentication is a process** in which one party becomes convinced of the identity of the other party by some indisputable proof.”

Authentication can be also regarded as a protocol executed at the beginning of **online -service** to verify the identities of the parties. The result of the protocol is immediate: acceptance or rejection.

Three factors which authentication can be based on

1. Some characteristics of you	*(fingerprint)*
2. Something you own	*(ID card)*
3. Something you know	*(pin, private key)*

Two factor authentication

A generally accepted principle that none of the factors in the list alone is adequate. In authentication a **combination of at least two factors is required** (for example ID card + PIN code or fingerprint + user ID)

Weak authentication and strong authentication

- These terms do not include security assessment

”Weak authentication” means traditional authentication without using cryptography.
Examples: User ID + fixed password or User ID + one-time password list

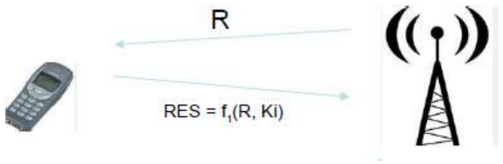
”Strong authentication” means authentication which uses cryptoalgorithms like RSA.
Challenge – response authentication mentioned earlier belongs to this category

One-way authentication and two-way authentication

In **one-way authentication** only one party is authenticated

(In GSM calls only phone is authenticated, not the mast)

F*igure. Traditional one-way* ***challenge-response authentication****. The operator mast sends a random challenge R to the phone. An algorithm f calculates the response RES from R and SIM-key Ki. The operator verifies the response with same calculation.*



In **two-way authentication** both parties are authenticated

(In 4G calls both the phone and mast are authenticated)

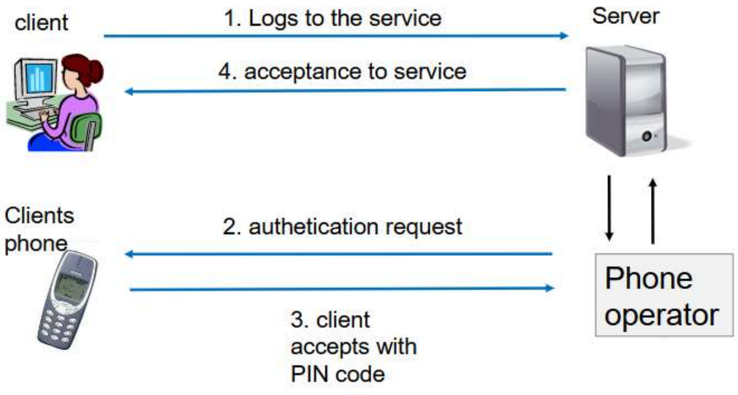
In two-way challenge-response authentication both parties of communication send challenge numbers each other and verify responses.

Mobile phone certificates

Mobile phones have also factory installed certificates, which uniquely authenticate the phone. Mobile certificate together with a PIN provide a secure access to services over Wifi or TLS-browser sessions

In Finland mobile phone operators offer authentication services called ”Mobile certificate”

Diagram of the ”Mobile Certificate ”


client
1. Logs to the service
Server
4. acceptance to service
Clients phone
2. authetication request
Phone operator
3. client accepts with PIN code