Public key infrastructure (PKI)
Certificates
Authentication

Public Key Infrastructure (PKI)

* TLS certificates
* Certification Authorities (CA)
* TLS – session
* S/MIME email encryption

TLS – protocol

TLS is a software, which more than 95% of secure connections over internet use.

It’s old name is SSL. From version 3.0 its called TLS (Transport Layer Security).

Typical services which use TLS are for example net banks, e-commerce, newspapers, email.

TLS is a hybrid cryptosystem

A hybrid cryptosystem is a secure protocol , which uses many algorithms for different purposes.

TLS is a typical **hybrid cryptosystem** with following functions:

1. Authentication of communicating parties
2. Key exchange
3. Encryption of data transmission (AES)
4. Digital signatures

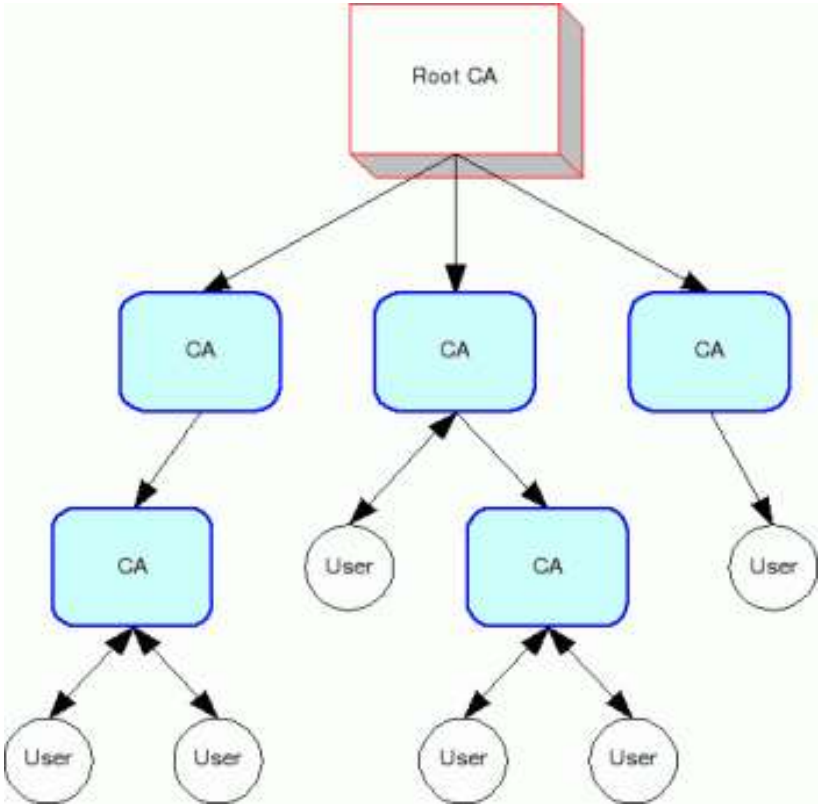
TLS requires a **Public Key Infrastructure** consisting of hierarchical network of Certification Authorities (CA's)

Every TLS – server needs a certificate from some member of **CA network.** Certificate includes **the public key of the server. Certificate is digitally signed by the CA** who has given the certificate. The purpose of the certificate is to ensure the autenticity of the web server and avoid Man in The Middle attacks.

Example of CA: https://www.sectigo.com/products

PKI = Public Key Infrastructure

Hierarchy of CA network



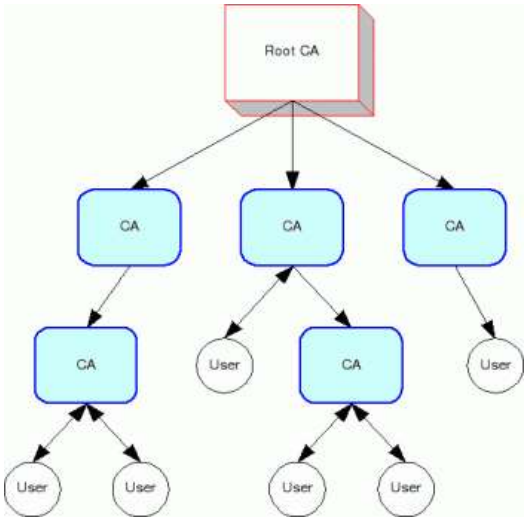
The public keys of web servers are issued by some CA.

CA network maintains a register of public keys.

TLS –server get its public key in the form of digitally signed standard form certificate.

Objective of the system is that there cannot be actors in web, who would give false public keys (as in man-in-the-middle attack) and read messages without authorization.

Chain of Trust Root CA's



Big demand of certificates requires lots of CA's giving certificates. CA networks has different levels. **At the top** of the hierarchy are **root CA's**, which give certificates for the second level CA's and so on.

An example of lower level CA's are CA's of universities, which issue certificates for universitys own web-servers.

If servers certificate is from CA which is not in the list of well known, trusted CA's, the client may need to follow the whole chain *(chain of trust)* up to the root CA.

Root CA at the top has no certificate. **The public key of the root CA is somewhere in the code of operating system or browser.**

X.509 isthe standard form of certificate

The most important information of 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.

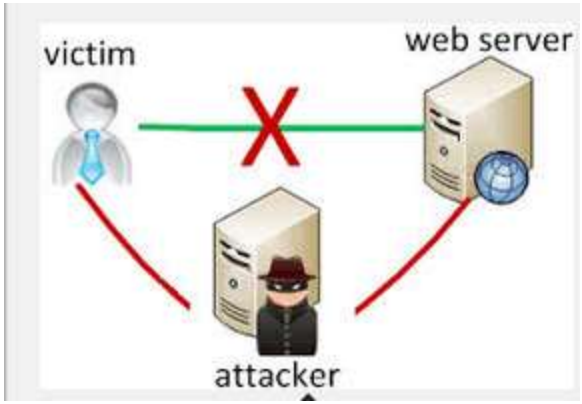
X.509 Certificate
Version : 1
Serial Number : 7983
Algorithm: SHA256WithRSAEncryption
Issuer: VeriSign Ltd
Validity :
Not Before July 12 2008 13:00 GMT
Not After July 12 2009 13:00 GMT
Subject:
Subject Public Key Info Matti Matikainen, Rovaniemi
Public Key Algorithm RSAencryption
Subject Public Key: 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)

Server's public key n

Certificate system prevents Man in the Middle Attack

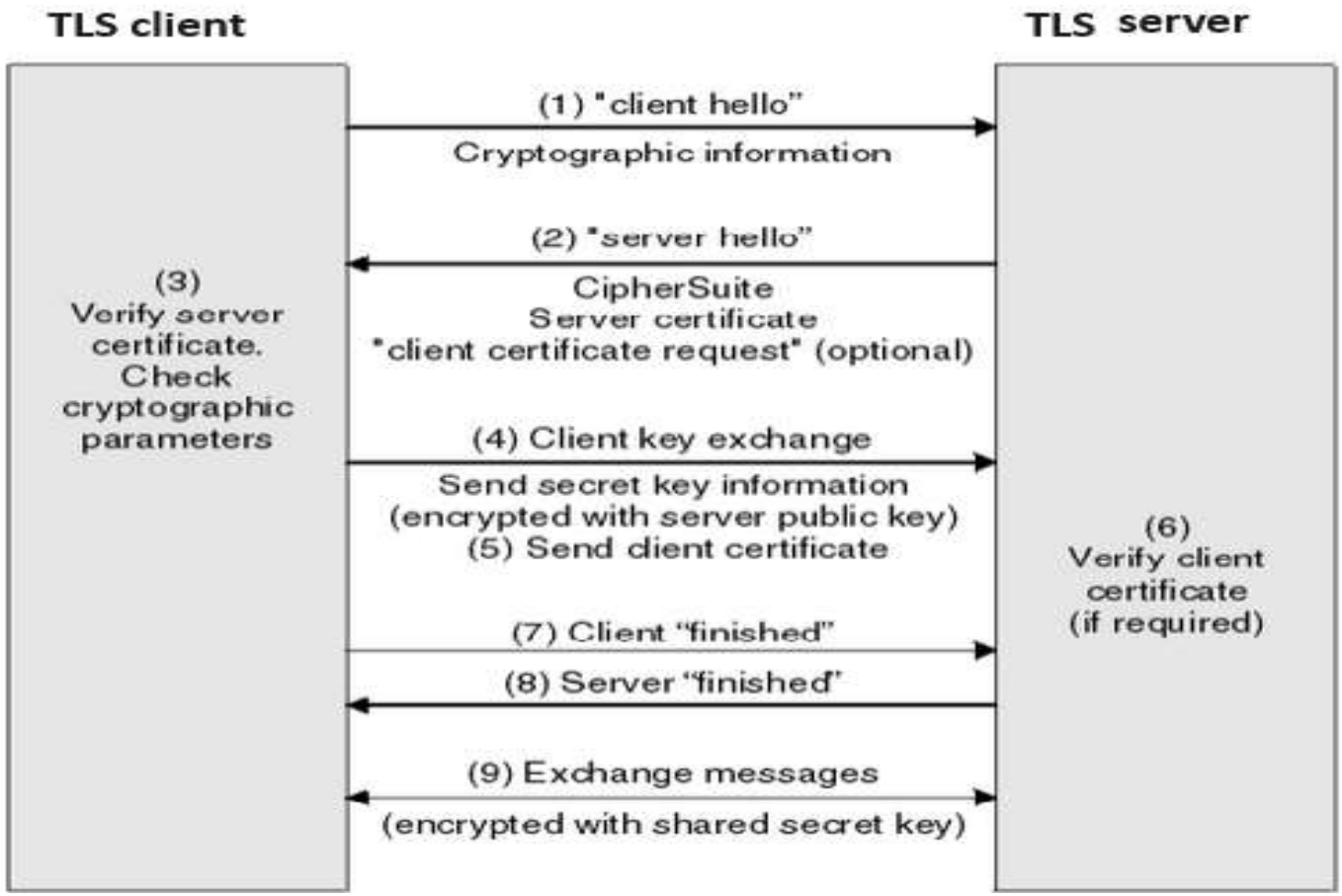
Man in the Middle attack

CA's and certificates are intented to prevent Man in the Middle attacks, 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 with strong digital signature, which in theory is impossible to forge.



Phases of TLS session

”Handshake” | **Authentication** | **Key Exchange** (**RSA** **ECDHE**) | **Encrypted transmission** (**AES**)



1. Handshake

- When the clients browser contact the server, server asks the highest TLS – version and list of algorithms supported by browser.

- Browser may answer: ”Highest version is TLS 1.1. Supported algorithms AES, RSA, sha1RSA

- Servers answer fixes the configuration of TLS version and algorithms for the session.

2. Authentication of server and client

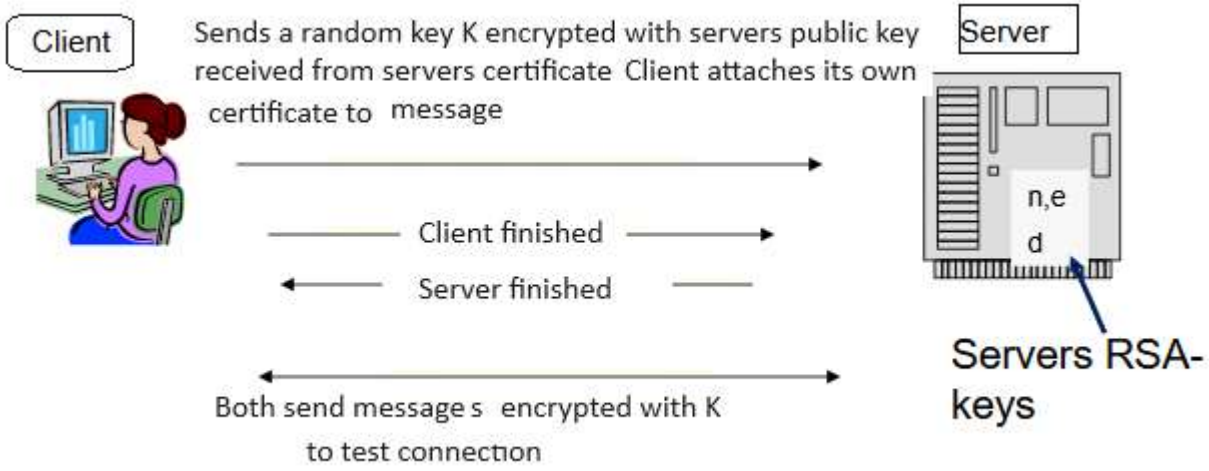
In many TLS versions server authentication is combined with the key exchange protocol.

Success of key exchange proves that the server knows the private key and is authenticated.

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 server encrypted with servers public key, which is found in its certificate.

If server manages to decrypt the key message, the server is authenticated.



Client authentication

Method 1: two-way authentication with keys:

If the clients 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.

Method 2: A private person may also authenticate himself in an oldfashioned way using User ID and password.

The method is not secure and it is getting rare.

3. Key exchange

Methods of key agreement in TLS are usually either RSA exchange or ECDHE.
After key agreement encyption with AES can start.
In newest TLS versions authentication and key exchange are separated.

4. Encryption of transmitted data

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

S/MIME email encryption protocol

Email without encryption is no more secure than a post card. When it moves in the net it can be read.

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 by choosing ”Get Digital ID” option. Instructions can be found with Google.

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

- Email is encrypted with block cipher , usually AES

- the 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..

Authentication

In Finnish: varmennus todennus

”**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 yours (finger print)
2. Something you know (pin code)
3. Something you own (ID card, SIM)

”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” and ”Strong” Authentication

(These concepts do no include security assessments)

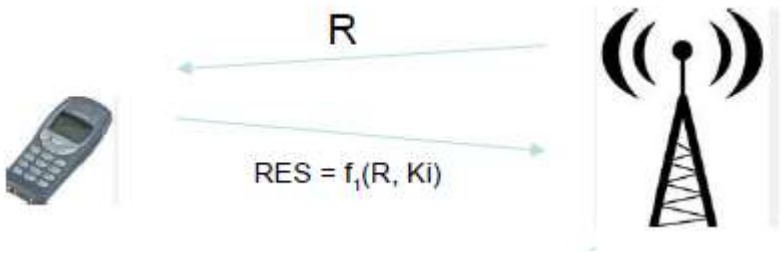
”**Weak authentication**” means traditional authentication without cryptography.
Examples: User ID + fixed password or
User ID + one-time password list

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

One-way and two-way authentication

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

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



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

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

Mobile phone certificate

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”

.
Mobile certificate uses RSA keys, which are in the SIM card of the phone.

Diagram of mobile certificate service