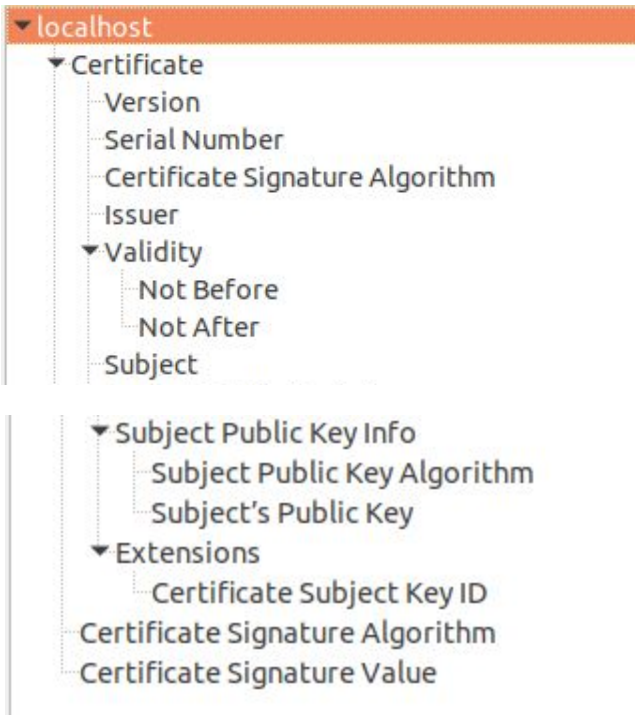
Vad är PKI?

Stands for Public key infrastructure. It is a framework, set of rules, that different systems and technologies can use. It is based on two-key (asymmetric) encryption. Associating a public key with a particular individual or authority with the help of digital certificates. The certificate can be officially recognized by a Certificate Agency and Registration Authority for a universal trust chain to be created.

Vad löser PKI för problem?

It solves the problem of confidentiality (encryption), protects information from unauthorised read. And it solves the problem of authentication, identifying the source of the sent information over the communication channel. This together solves the problem of providing secure communication channels. The PKI system defines the standard formats for certificates and their use.

Vad innehåller ett certifikat? Förklara alla fält.



Version - The version of the certificate structure that defines the format of the certificate. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed.

Serial number - Unique identifier for the certificate

Certificate Signature Algorithm - Method of signature used to sign the certificate and hashing algorithm. (Like RSA with SHA for example)

Issuer - The name of the Certificate authority that issued the certificate. Or if self signed same as owner of certificate

Validity - the validity period of the certificate

Subject - The details of owner of certificate.
CN: Common Name
OU: OrganizationalUnit
O: Organization
L: Locality
S: StateOrProvinceName
C: CountryName

Subject Private Key Info
Algorithm associated with the key and the actual public key of the subject

Certificate Signature Value
Value of the actual certificate signature.

Extensions
Optional additional information, not critical

Hur valideras ett certifikat?
The server sends a certificate containing the public key of the server and a signature from an intermediate authority that has been encrypted with the authorities private key. The server also sends the intermediate authority certificate alongside their own signed certificate containing the public key of the authority.

The client now begins to validate by decrypting the signature of the server certificate with the public key of the intermediate authority. That should give the hash value of the certificate. The Hash value of the certificate is calculated by looking at the algorithm the authority used and if they match the certificate is validated. The client now looks in the list of trusted root certificate authorities and does the same steps to see if the intermediate authority can be trusted

Vilka algoritmer används på vilka fält och i vilken ordning?

1. RSA decryption(public key decryption) of signature field
2. Hash is calculated of entire certificate (check if match)

Hur levereras root-certifikaten till din dator?
Delivered by web-browsers, hardwired in their certificates list.

Vad är en trust chain?
Parent child relationships. There exists both intermediate authorities and root certificate authorities. The root certificate authorities are hardwired into the browsers, browsers trust them automatically. They are the root of the trust chain. They can generate their own certificates and self-sign it by hashing the certificate and sign it with their own private key and still be trusted. They have certificates of the intermediate certificate authorities and can validate them and have signed them. The entire trust chain depends on the root authorities. The private key of the root authority is the most critical item in the chain.

Är det säkert att lagrad lösenorden till certifikaten till din dator? Varför/Varför inte?
Yes and no, Attackers can use stolen keys and certificates to gain trusted status and perform trust based attacks to evade detection and bypass security controls. If no extra layer of security is present and they are kept carelessly, a attacker can get ahold of them. If stored they should be kept well hidden and safe in cryptographic storage vaults or similar.

Förklara HELA handshaket.
Step 1:
The client initiates communication with the server with a ClientHello message containing a list of supported cryptographic algorithms and data compression methods as well as the tls/ssl version.

Step 2: Server responds with a ServerHello message containing a list of the cryptographic algorithms chosen by the server picked from the clients list of supported methods. Server also sends the certificate, sessionID and the server public key.

Step 3:
Client contacts the servers Certificate Authority to verify if the certificate is valid. Establishing trust.

Step 4:
If the certificate is valid or if the client chooses to proceed anyway. The Client performs the Client-Key-Exchange. Client encrypts a shared secret key with the servers public key and sends it to the server.

Step 5:
Client send a Finished message to the server encrypted with the shared secret key to the server. Ending the clients part of the handshake

Step 6:
Server sends a response with Finished message encrypted with the shared secret key to the client. Ending the servers part of the handshake

Explain how the PKI work.
The certificate is sent by the server in response to the ServerHello(in ssl communication)
The certificate is sent to the issuing CA for verification. The public key contained in the certificate linking it to the server/organisation is either verified or denied by the CA. Since the CA is trusted through the trust chain can be sure the communication is with the correct entity.

När i handshaket används symmetriskt kryptering?
After the encrypted shared secret key has been sent to the server. All communication is then encrypted with the shared secret key

När används asymmetriskt kryptering?
When the shared secret key is sent to the server. It is first encrypted with the public key of the server.

Varför är TOR så säkert?

Tor relies on a system of tor nodes or relays. A relay can be of the types bridges,middle or exit relays. Where the exit relays send the traffic to the destination and middle relays passes on traffic to other relays. The traffic from node to node inside the tor network is encrypted. Different keys are used between each relay so if one of them has been compromised by an attacker, it would not be able to trace back traffic to the source.
The tor client creates a new circuit through the relay (each time at startup or when requested) and the keys are disposed of after a session and new ones are established. This way an attacker can not link previous requests to new ones and exposed keys will become useless after some time.

Hur kan någon råka avslöja vem de är eller bli spårade? Nämn åtminstone två olika sätt.

The payload is whatever data is being sent and even if that data is encrypted, traffic analysis will still reveal a lot of information about the connection. It focuses on the header of the packets and will reveal information such as timing ,source, destination, size and so on.
To stay anonymous it is important to never reveal any personal information, e.g. names, addresses, work, in web forms. Another important thing is to use different aliases on websites so that two different accounts on different websites can't be connected to each other. Otherwise the user is revealing what websites he or she might be visiting and it becomes easier for other people to track them. Visiting clearnet sites i.e. sites not using the hidden service protocol with the Tor browser will not ensure the anonymity of the user. The sites has to use the hidden service protocol in order for the Tor browser to make the user stay hidden.
The traffic from node to node inside the tor network is encrypted. Whereas from the exit relay to the web server it is in the clear. The nightmare scenario would be that both the first relay and the exit relay are compromised, in that case the attacker would see who the source is and what their destination and request was.