Armaan Shamsaasef

Certificates

Certificates - SY0-701 1.4

Core Concept: A digital document that binds a public key to an identity (a person, device, or organization). It is the foundation for trust on the internet.

The Problem: Trusting Public Keys

- In asymmetric encryption, how can you be sure that a public key you receive actually belongs to the person or website you think it does?
- An attacker could easily create their own key pair and claim to be your bank.

The Solution: Public Key Infrastructure (PKI) and Certificates

A Certificate Authority (CA) acts as a trusted third party that vouches for the identity of the key owner.

The Certificate Creation Process:

1. Request: You generate a public/private key pair. You create a Certificate Signing Request (CSR), which contains your public key and your identifying information.
2. Validation: The Certificate Authority (CA) validates your identity (the rigor of this check depends on the certificate type).
3. Signing: The CA creates your digital certificate, which includes your public key and your identity.
4. Issuance: The CA signs the certificate with its own private key and gives you the signed certificate.

How Certificate Trust Works (The Chain of Trust)

When your client (e.g., a web browser) connects to a secure website (HTTPS):

1. The website presents its certificate to your browser.

2. Your browser checks the certificate's digital signature. It uses the CA's public key (which is pre-installed in your browser's Trusted Root CA store) to verify the signature.
3. If the signature is valid, your browser trusts that the CA has authenticated this website, and therefore it trusts the website's public key inside the certificate.

Video Analogy: A government-issued Driver's License.

- The license itself is the certificate.
- Your face and personal details are the public key and identity.
- The government's hard-to-forge seal is the CA's digital signature.
- Everyone trusts the license because they trust the issuing government (the CA).

Certificate Contents (X.509 Standard)

A certificate contains standardized information, including:

- Subject: The entity it identifies (e.g., `www.google.com`).
- Issuer: The Certificate Authority that signed it.
- Validity Period: Start and end dates for when the certificate is valid.
- Subject's Public Key: The core piece of information being certified.
- Digital Signature: The CA's signature, which validates all the other contents.

Key Concepts

- Root of Trust: Your device's built-in list of trusted Root CAs. This is the starting point for all verification.
- Intermediate CA: Subordinate CAs that are signed by the Root CA. They issue most end-user certificates to keep the Root CA secure offline.
- Certificate Chain: The hierarchical list of certificates from the end-entity certificate back to the trusted Root CA (e.g., `Website Cert` -> `Intermediate CA Cert` -> `Root CA Cert`).

Summary

- Purpose: To provide trust by binding a public key to an identity.

- Issuer: A trusted Certificate Authority (CA).
- Core Mechanism: The CA's digital signature on the certificate, which can be verified by anyone with the CA's public key.
- Foundation: Relies on a Chain of Trust that begins with the pre-installed Root Certificates on your device.