Life Cycle of an X.509 Root Certificate

Part 1:

Certificate Issuance and Expiration (CA Side)

1. Key Generation
The CA generates a pair of keys: one public and one private.

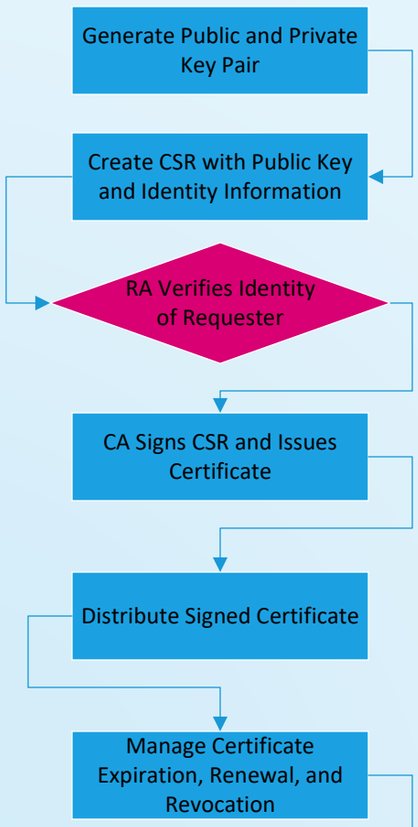
2. Certificate Signing Request (CSR)
The entity requesting the certificate creates a CSR.

3. Verification by RA
The RA ensures the requester is who they claim to be.

4. Certificate Issuance
The CA signs the CSR with its private key, creating the certificate.

5. Certificate Distribution
The CA provides the certificate to the entity and makes it available to others.

6. Certificate Expiration and Renewal
Certificates must be renewed before they expire or revoked if compromised.



Part 2:

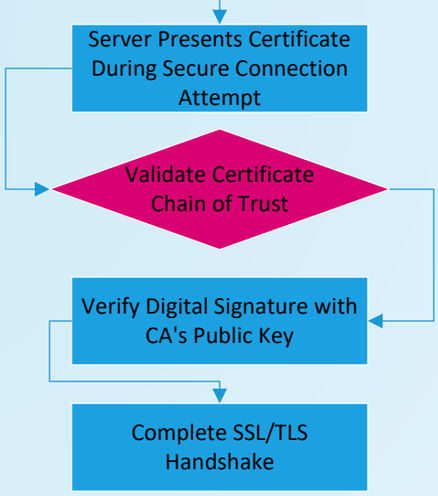
Certificate Verification (User Side)

7. Certificate Presentation
The server shows its certificate to the client.

8. Chain of Trust Validation
The client checks the certificate chain to ensure it's trusted.

9. Digital Signature Verification
The client ensures the certificate was signed by a trusted CA.

10. Establishing Secure Connection
The client and server set up a secure, encrypted communication link.



Roles of CA and RA

Certificate Authority (CA) — Issues, Renews, and Revokes Certificates

Registration Authority (RA) — Verifies Identity of Certificate Requesters

Comparison: X.509 vs. PGP Certificates

X.509 Certificates — Widely Used, Standardized, Centralized Trust Model

PGP Certificates — Decentralized Trust Model, Complex Web of Trust Management

Martin Grobisen