PKI

DURATION : 0’30

Introduction

- Public Key Infrastructure (PKI) is a set of hardware, software, people, policies and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
- Components of PKI:
  - Certificate Management System :
    Generates, distributes, stores, and verifies certificates.
  - Digital Certificates :
    Establishes credentials of a person when doing online transactions.
  - Validation Authority (VA):
    Stores certificates (with their public keys).
  - Certificate Authority (CA):
    Transmits and verifies digital certificates.
  - End User:
    Requests, manages, and uses certificates
  - Registration Authority (RA):
    Acts as the verifier for the certificate authority

Terms

- Certificate Signing Request (CSR):
  Request for certification. Contains public key and ID to be certified.
- Certificate Revocation List (CRL):
  List of revoked certificates. Transmits by a CA at regular intervals.
- Certification Practice Statement (CPS):
  Document describing structure and processes of a CA.
- X.509:
  Standard defining the format of public key certificates.
- Online Certificate Status Protocol (OSCP):
  Protocol used for obtaining the revocation status of an X.509 digital certificate.

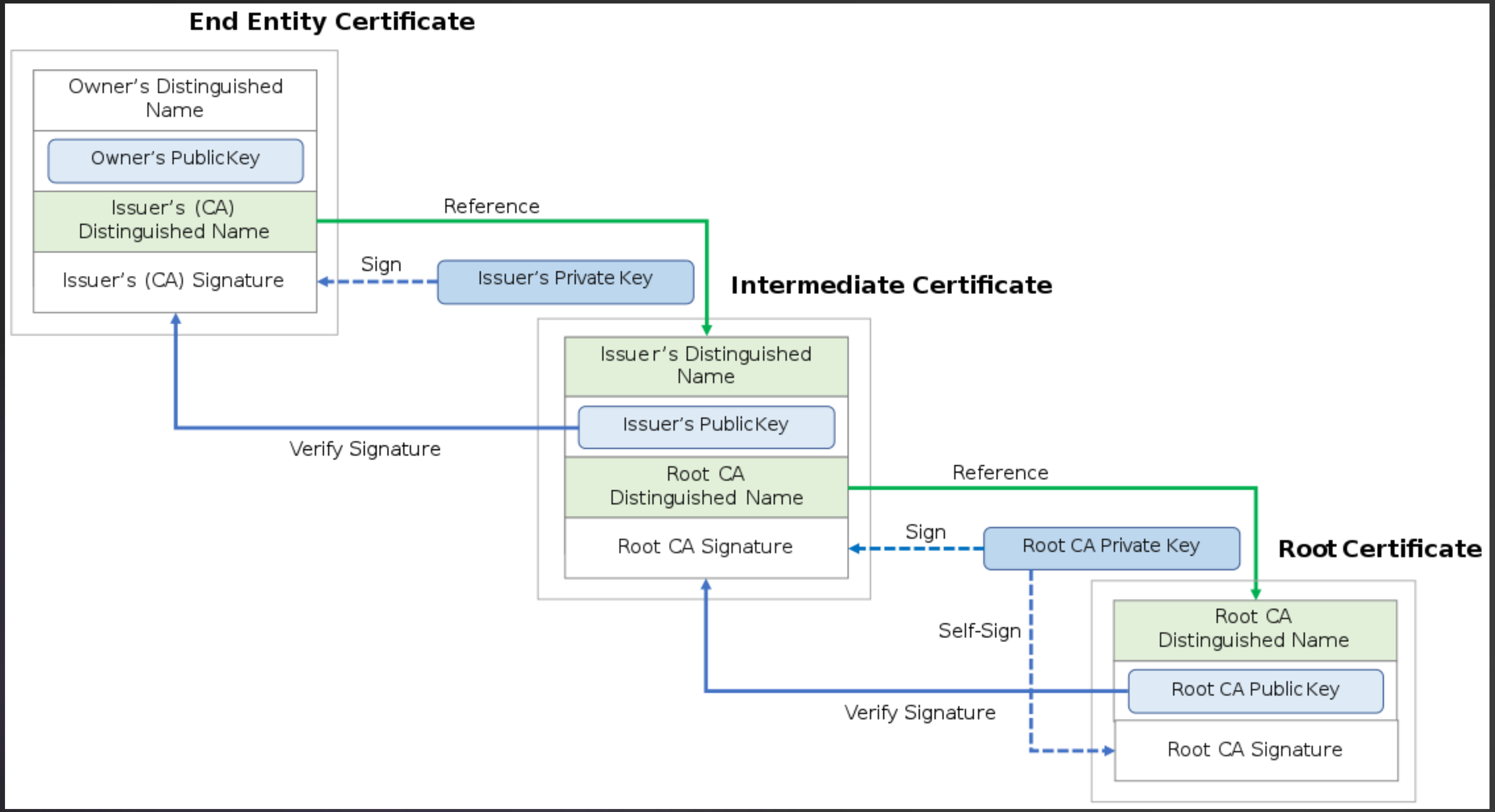
CA types

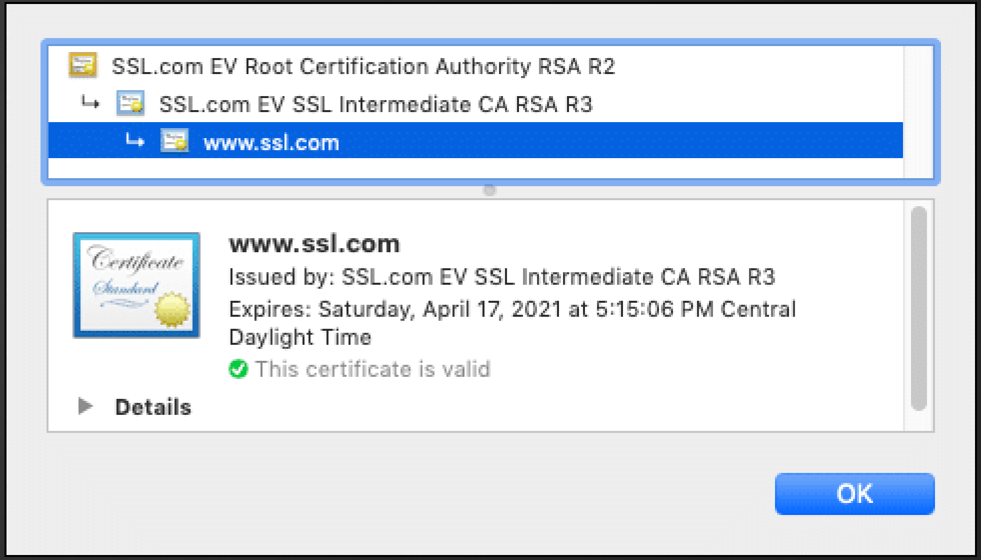
- Root CA:
  A root CA is a CA that issues the root certificates that are used to sign other CA certificates. Root certificates are self-signed certificates.
- Intermediate CA:
  CA below the root CA but not a signing CA. Transmits only CA certificates.
- Signing CA:
  CA at the bottom of a PKI hierarchy. Transmits only user certificates.

Certificate Types

- CA Certificate:
  Certificate of a CA. Used to sign certificates and CRLs.
- Root Certificate:
  Self-signed CA certificate at the root of a PKI hierarchy. Serves as the PKI's trust anchor.
- Cross Certificate:
  CA certificate transmits by a CA external to the primary PKI hierarchy. Used to connect two PKIs and thus usually comes in pairs.
- User Certificate:
  End-user certificate transmits for one or more purposes: email-protection, server-auth, client-auth, code-signing, etc.

CA and certificate Types



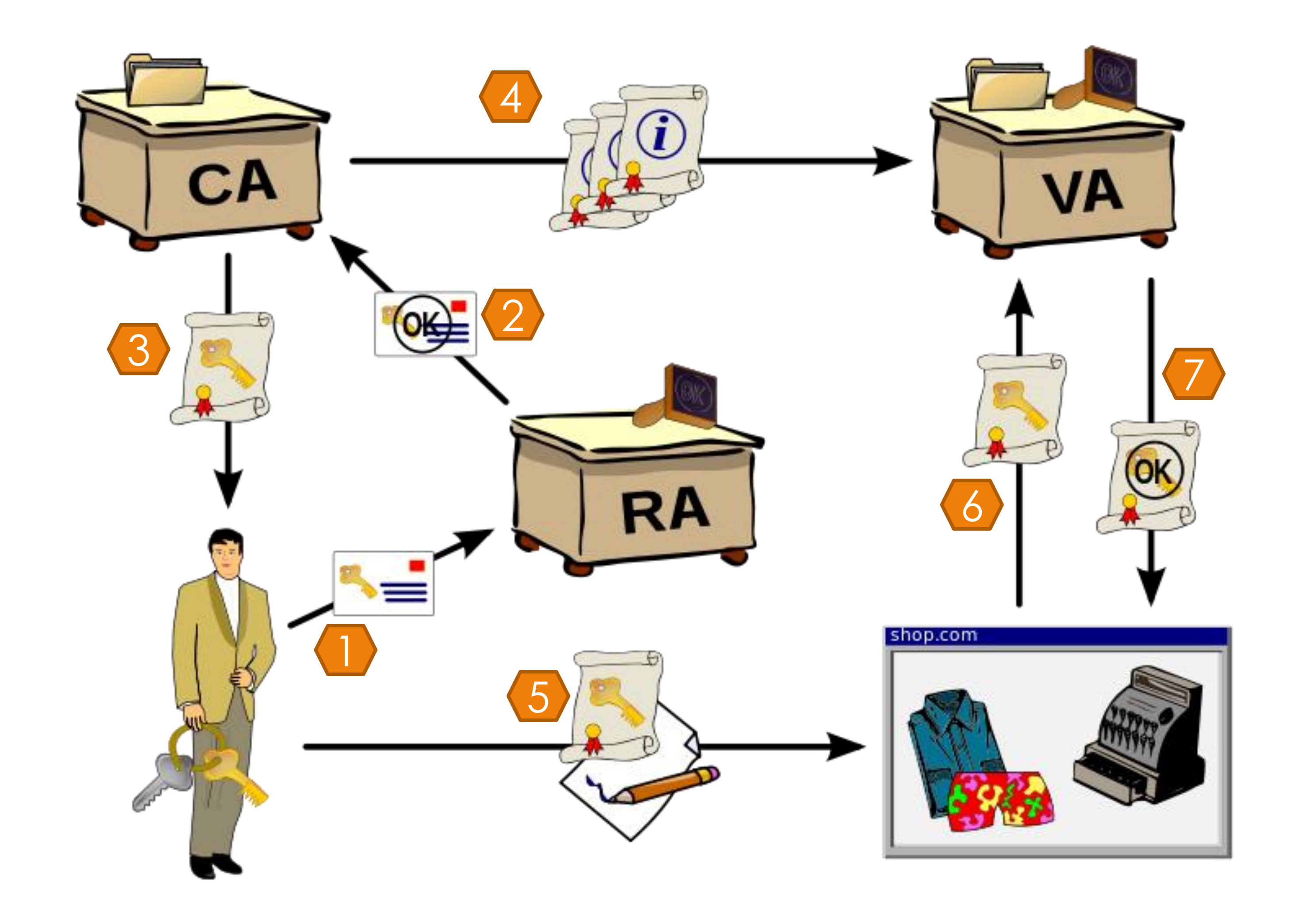


SSL.com EV Root Certification Authority RSA R2
↳ SSL.com EV SSL Intermediate CA RSA R3
↳ www.ssl.com

www.ssl.com
Issued by: SSL.com EV SSL Intermediate CA RSA R3
Expires: Saturday, April 17, 2021 at 5:15:06 PM Central Daylight Time
✓ This certificate is valid

Diagram

1. User applies for issuing certificate.
2. Request for issuing certificate.
3. Public Key certificate.
4. Updates information.
5. Message with digital signature and copy public key certificate.
6. Public Key certificate.
7. Determined result.



Signed Certificate

- User approaches a trustworthy Certification Authority (CA) and purchases digital certificate.
- User gets the public key from the CA and he signs the document using it.
- The signed document is delivered to the receiver.
- The receiver can verify the certificate by enquiring in Validation Authority (VA).
- VA verifies the certificate to the receiver, but it doesn’t share private key.

Self-signed Certificate

- User creates public and private keys using a tool (like Java Keytool).
- User uses public key to sign the document.
- The self-signed document is delivered to the receiver.
- The receiver request the user for his private key.
- User shares the private key with the receiver.

x509 Certificate

- X.509 is a standard defining the format of public key certificates.
- Structure of an X.509 v3 digital certificate is :
  - Serial Number
  - Signature Algorithm
  - Issuer Name
  - Validity period
    - Not Before
    - Not After
  - Subject Public Key Info

PEM : Privacy Enhanced Mail

- PEM is the most common format for X.509 certificates, CSRs, and cryptographic keys.
- PEM is a text file containing one or more items in Base64 ASCII encoding, each with plain-text headers and footers like:

  -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

  -----BEGIN RSA PRIVATE KEY---- and -----END RSA PRIVATE KEY----
- PEM files are usually seen with the extensions .crt, .pem, .cer, and .key

PKCS : Public Key Cryptography Standards

- PKCS#7 (also known as P7B) is a container format for digital certificates that is most often found in Windows and Java server contexts, and usually has the extension .p7b.

- PKCS#12 (also known as PKCS12 or PFX) is a common binary format for storing a certificate chain and private key in a single, encryptable file, and usually have the filename extensions .p12 or .pfx.