Presentation on Chapter 8
Public key Certificate management & use cases

Group 6

Members:

Nurul Absar
Sarose Datta
Roky Das
Jabed Hosen
Rakin Intisar Muhammed
Sazzad Hossain
Nishan Barua
Saiful Islam Tareq

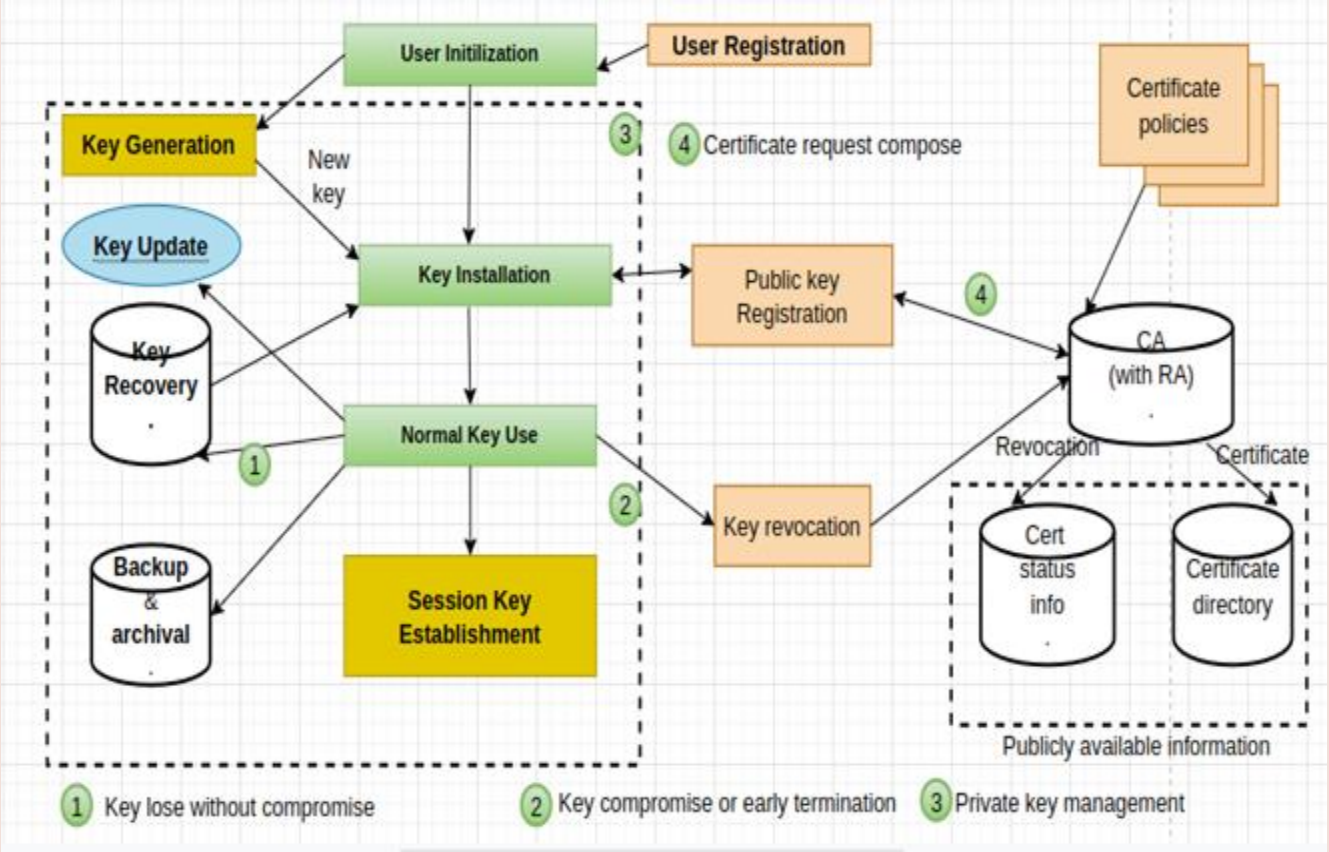
Introduction

- **What is public key?**
- **What is a public key certificates?** Also known digital certificate.
- **What is CA?** Authority(CA) issue digital certificate that verify the identity of user information generating digital signature.
- **What's certificate field contain?** Attributes such as subject and issuer name, format version, serial number,validity period, and signature algorithm details etc.
- What is PKI ?
- What is purposes of PKI?

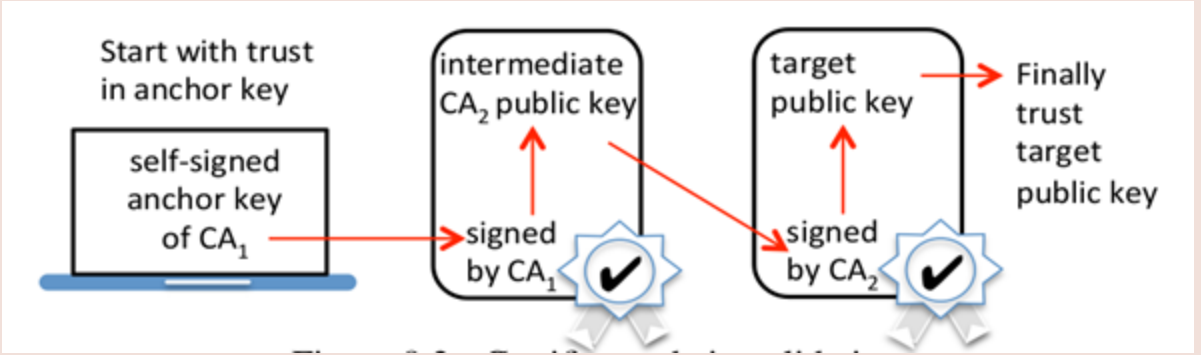
PKI components and lifecycle

PKI involve-

- Certification Authority(CA)
- Registration Authority(RA)
- Public Key
- Private key
- Digital Certificate
- Certificate Directory
- Certificate Revocation list.
- Hardware security module



CERTIFICATE CHAIN VALIDATION



What is CA?

Verified by trusted organizations
SSL certificates

Intermediate CA

Substitute of root certificate
Verify by PKI between two CA's

Certificate chain

Made of a list of certificates
Start from a server's certificate and terminate with the root certificate

Trust anchor CA

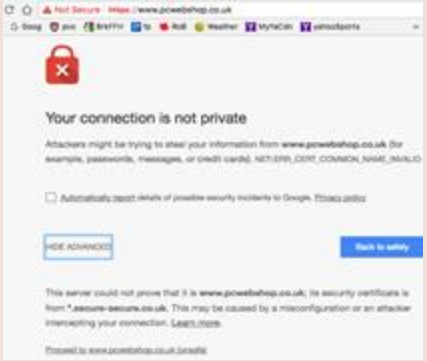
Public key stores in root certificate
X.509v3 extensions

Out of band channel

Ensure trust that hackers not access or alter
Arises term of fingerprints
Out of band authentication

Certificate Extensions

- **Self signed certificates**
  - Not signed by private or public CA
  - Signed with it's own private key
- **Browser trust anchor**
  - Public or symmetric key
  - Trusted because it is directly built into hardware or software
- **What is certificate extensions**
  - Allow further information to be inserted within the certificate
  - Provide more functionality in a PKI implementation
- **Trust On First Use (TOFU)**
  - It is a security model
  - Client needs to create a trust relationship with unknown server
  - After finding a indentifier, client can establish the connection
- **X.509v3 extensions**
  - It is a digital certificate
  - Cross check and verify certificate between client and server using public key
  - Work as a safeguard against malicious network



CERTIFICATE REVOCATION

❖Certificate have a period of validity(for 1-2 years)

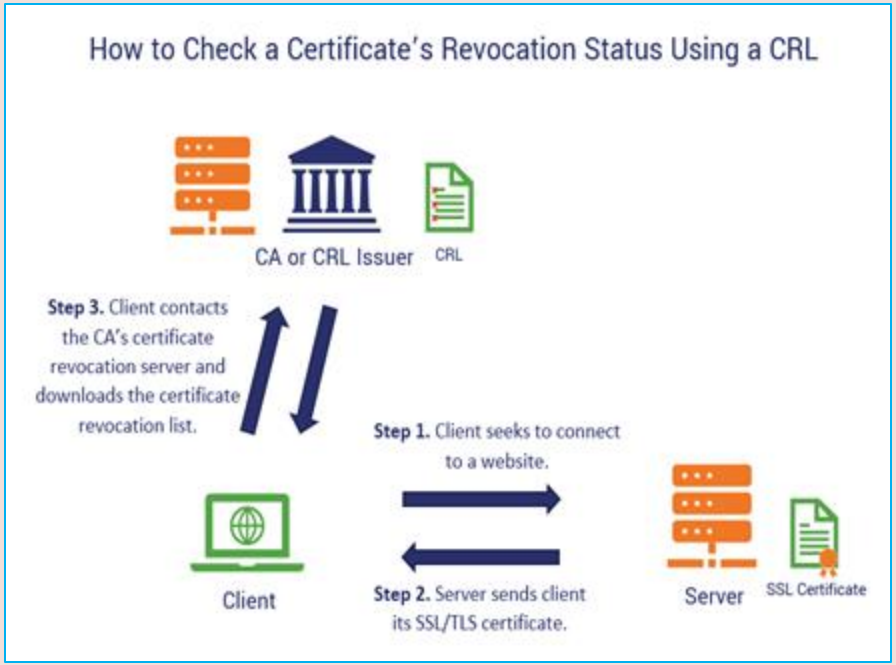
❖**Many valid reason to revoke a certificate.**

- ❑ Private key has been compromised(Most common reason).
- ❑ Certificate owner no longer owns the domain .
- ❑ Certificate owner do not pay to CA(Certificate Authorities).
- ❑ Original certificate has been replaced with a new certificate from another issuer.

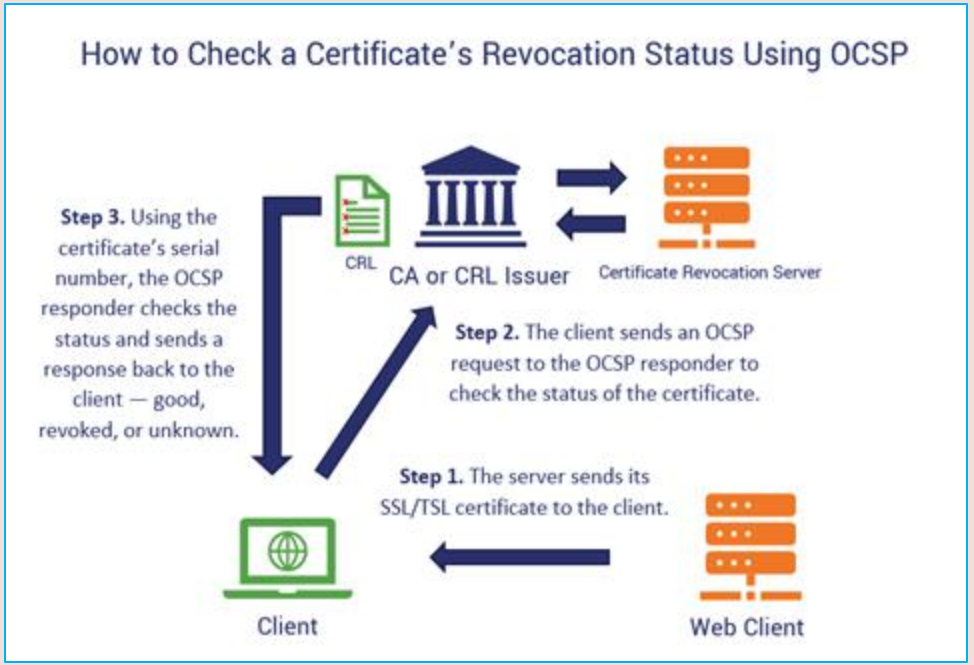
❖ **Some of main approaches used for revoking certificate:**

- ❑ Certificate Revocation List(CRL)
- ❑ CRL Fragments-Partitions and Deltas.
- ❑ Online Status Checking(Using Online Status Check Protocol)

CERTIFICATE REVOCATION MECHANISM



Certificate Revocation List



Online Status Check Protocol

PKI Architecture

- PKI : Public Key Infrastructure.
- It’s a standard using for managing , storing and revoking **digital certificate**.
- Follow asymmetric key cryptography. That means 2 keys. One for encryption and for decryption .

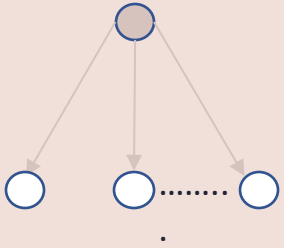
Architecture has 3 parts

1. certificate repository
2. entity
3. certification authority

Architecture

Model 1

- **Single CA domain**

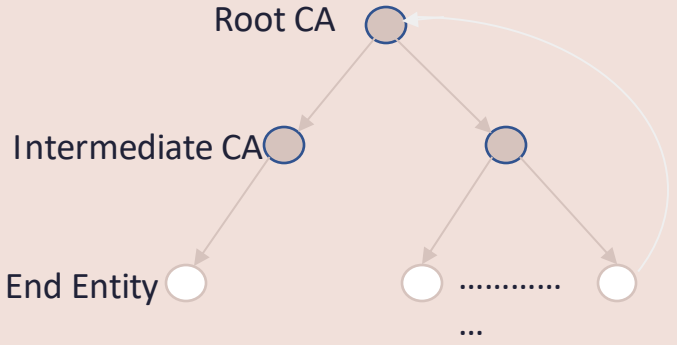


CA

Entity

Model 2

Strict Hierarchy



- Trust models **provide a framework to create and manage trust relationships among the different entities of a public key infrastructure (PKI)**.
- These trust relationships are verified through the certification path validation process, which involves: path discovery, signature verification and revocation status checking.

TLS web site certificates and CA/browser trust model

- world's most widely deployed security protocol
- Follows de facto standard
- TLS security goals:
  - encryption of traffic between endpoints (confidentiality)
  - server authentication (through public-key certificates)
- Trusted Certificate
  - Checked by browsers to validate
- GRADES OF TLS CERTIFICATES:
  - DV (Domain Validated) CERTIFICATES
  - OV (Organization Validated) CERTIFICATES
  - EV(Extended Validation) CERTIFICATES
  - IV(Individual Validation) CERTIFICATES(Combination of DV, OV, EV certificates)
  - CA/BROWSER FORUM AND EV CERTIFICATES
  - SELF-SIGNED TLS SERVER CERTIFICATES

TLS web site certificates and CA/browser trust model

- Main Limitations of browsers while browsing:
  - Rogue certificates
  - TLS-stripping attacks
  - Poor revocation
  - Poor Trust agility
  - Uncountable Intermediate CAs

Thank You