9.8.4 Certificate Lifecycle Facts

A *digital certificate*, also referred to as a public key certificate or identity certificate, is an electronic document that uses a digital signature to bind together a public key with an identity. Identity information includes the name of a person, computer, or organization, and optionally an object identifier (OID). The OID is used to map a certificate policy to a certificate authority. The certificate is the best way to provide non-repudiation and can be used to verify that a public key belongs to an individual.

A *public key infrastructure* (PKI) is a hierarchy of computers that issues and manages certificates. A Certificate Authority (CA) is the entity that issues certificates. The following process is used to request, issue, and manage certificates:

1. To request a certificate, a client must first generate a public and private key pair. The key pair is generated by an application called a cryptographic service provider (CSP). The CSP uses a specific algorithm for generating the key pair.
2. The client requests a certificate from a CA by sending identifying information along with a copy of the public key. This is called a certificate signing request (CSR). The certificate request is digitally signed using the private key.
3. The CA performs identity proofing by verifying the information submitted to prove identity. The purpose of this process is for the CA to validate that you are who you say you are. How the certificate is approved is dictated by the approval policy on the CA.
   - A manual policy requires an administrator to manually approve or deny all requests coming in.
   - An automatic policy allows the CA to review information within the request to determine if it is valid information. Based on that information, it can approve or deny automatically.
4. If the certificate request is approved, the certificate is issued to the client. Issuance policies on the CA identify the certificates that the CA is allowed to issue. For example, issuance policies can restrict a CA to:
   - Be able to issue only certain types of certificates.
   - Be able to issue certificates only for a particular use.
   - Issue certificates that are valid only for a specific amount of time.
5. Certificates are issued with a valid lifetime period. As the expiration time period approaches, certificates can be renewed by submitting a renewal request. Instead of requesting a new certificate, clients should renew existing certificates.
6. If a certificate becomes compromised, such as the private key being lost or stolen, it can be revoked. This can be accomplished by going to the CA and revoking the certificate. Before accepting a certificate, a client validates that the certificate has not been revoked. Two methods exist for checking for revoked certificates:
   - The Certificate Revocation List (CRL) is a list of certificates revoked by the CA. Clients download the entire CRL and check the CRL for a certificate.
   - With the online certificate status protocol (OCSP), clients can submit a verification request for a specific certificate to a special server called an *online responder*. The online responder maintains a list of revoked certificates and responds to certificate status requests on a certificate-by-certificate basis.

Certificates are used for proof of identity and secure communications. The following process is an example of using SSL and certificates to secure web transactions:

1. A client with a web browser accesses a web server that is using HTTPS (SSL).
2. The server sends the client a copy of the SSL certificate that it obtained from a CA.
3. The client verifies information in the SSL certificate to decide if it trusts the certificate. The client asks the following questions:
   - Does the subject name in the certificate match the URL that was typed in the web browser?
   - Has the certificate expired?
   - Does the client trust the issuing CA? Every browser has a Trusted Root CA list that identifies trusted CAs on the internet. The browser compares the signature of the issuing CA on the certificate to the list of trusted root CAs. If it does not exist in the list, the client will not trust the certificate.
4. If the certificate passes all three checks, the client trusts the issuing CA and trusts any certificates that the CA issues; therefore, the client trusts the web server.

The following table reviews terms you should be familiar with.

Term	Function
Certificate Authority	The *Certificate Authority* (CA) is an entity trusted to issue, store, and revoke digital certificates.
Subordinate Certificate Authority	The subordinate CA is responsible for issuing certificates, holding the CPS, and publishing the CRL. Subordinate CAs function within the hierarchy in a parent-child relationship with the root CA or another subordinate CA.
Certificate Practice Statement	The *Certificate Practice Statement* (CPS) is a declaration of the security that the organization is implementing for all certificates issued by the CA holding the CPS. This statement tells potential partners or others relying on the security of the PKI system how well the security of the PKI system is being managed.
Cryptographic Service Provider	A Cryptographic Service Provider (CSP) resides on the client and generates the key pair.
Online and Offline	A chain of trusted authorities begins with a root CA. Once the root CA is installed and its root certificate is created, it can be used to issue certificates authorizing intermediate CAs. An intermediate CA can issue, distribute and revoke certificates without the root CA.

Certificate Authorities	If a root CA is compromised, it requires that every certificate in the chain of trusted authorities is re-issued. To ensure the security and integrity of root CAs, they are commonly kept it in an offline state and only brought online when needed.
Online Certificate Status Protocol	The *Online Certificate Status Protocol* (OCSP) is a protocol used for checking the status of an individual digital certificate to verify if it is good or has been revoked.
Certificate Revocation List	The *Certificate Revocation List* (CRL) consists of a list of certificates that have been previously revoked and resides at the CA. This list can be accessed by the client to verify the validity of a digital certificate.
Certificate Chaining	There are two types of CAs, root CAs and intermediate CAs. When validating a certificate, the client device (usually a web browser) will check the issuing CA, which may be an intermediate CA. The certificate of the issuing CA is then checked. If it is not trusted, the issuing CA of that certificate is checked and so on up the chain until a root CA is found. If no trusted CA in the chain is found, the browser will normally display an error.
CRL Distribution Point	The CRL is published at the CRL Distribution Point (CDP). Four areas where the CRL is usually published are: ▪ On the issuing CA ▪ On an internet or intranet website ▪ To a file so it can be exported to other distribution points ▪ In a directory service, such as Active Directory
Registration Authority	A registration authority (RA) can be used in large enterprise environments to offload client enrollment request processing by handling verification of clients prior to certificates being issued. The RA: ▪ Accepts registrations. ▪ Distributes certificates and keys. ▪ Validates identities in a certificate request for the CA. ▪ Does not issue certificates directly. Though certificates are not issued until the RA validates the information, the RA cannot issue certificates.
X.509	X.509 is the official standard of ITU Telecommunication Standardization Sector (ITU-T) that identifies the format for public key certificates and certification path validation. All X.509 certificates include the following data: ▪ tbsCertificate ▪ Versions that apply to the certificate ▪ Serial number ▪ Signature ▪ Issuer ▪ Validity ▪ Subject ▪ Subject public key information ▪ IssuerUniqueID and SubjectUniqueID ▪ Extensions
Enrollment Agent	An *enrollment agent* is a user who is authorized to request certificates for other users. Enrollment agents are typically authorized to request certificates that are used on smart cards. These agents can request the certificate and create the smart card that the authorized user can then use.
Authority Information Access	Users can obtain a copy of the CA's certificate from the authority information access (AIA). This is useful if the root CA is offline. It is common for root CAs to be offline so that they are less susceptible to compromise. The CA's certificate can be published to other locations that users can access. A copy of the certificate and the root CA's public key is necessary to verify digital signatures that the CA has implemented.
OSCP Stapling	OCSP stapling is an efficient way to handle the verification of certificate information. Stapling allows the CA to be queried regularly and the responses to be cached.Otherwise, a request to a CA's server must be made for each certificate verification action.
Pinning	Pinning is the process of associating a host with its expected certificate. Once the certificate is obtained for a host is is pinned to the host. Thereafter, all communication with that host should use the same certificate. If not, the communication is suspect.

The certificate life cycle summary is as follows:

1. The CSP generates the key pair.
2. A certificate request is made to the CA.
3. The CA approves or denies the request.
4. The certificate is issued.
5. The certificate may be renewed.
6. The certificate may be revoked.

Types of certificates:

Certificate Type	Description
Wildcard	Wildcard certificates allow you to protects an unlimited number of subdomains within a single domain. For example, a certificate for corpnet.xyz will secure www.corpnet.xyz, help.corpnet.xyz, etc.
SAN	A Subject Alternate Name (SAN) certificate can protect more than one FQDN, even if there is no relationship to the names. For example a SAN could protect corpnet.xyz, corpnet.com and newcorp.org.
Code Signing	A Code Signing certificate allows software developers to sign their products before the distribute them. In this way users who download the software can be confident that it has not been modified since it was signed by the developer.
Self-signed	Self-signed certificates are not issued by a CA. They are signed by the person or device that created it. They are often used in an internal network to offer the same level of encryption as other certificates. However, they can't be used to prove identity since any attacker can create a self-signed certificate. They should not be used for pubic facing web sites and other applications.
Machine/Computer	Machine or Computer certificates are used as proof of identity for a computer.
Email	Email certificates are used on mail servers to protect username, passwords and email correspondence.
User	User certificates are used as proof of identity for a person or user.
Root	A root certificate is issued by a trusted certificate authority and identifies a root certificate authority. The private key in a root certificate is used to sign other certificates.
Domain Validation	A domain validation certificate is typically used for Transport layer security. It is used to validate the identity of domain name servers who have control over a DNS domain.
Extended Validation	An extended validation certificate is the highest form of SSL certificate. It is granted by a CA after the company's ownership, organizational information, physical location, and legal existence are verified.

Different platforms and devices require SSL certificates in different encodings. The certificate file extension indicates the encoding or format

Encoding/Format	Description
DER	A file with a DER extension indicates that the certificate is DER encoded. A DER file contains a single certificate.
PEM	A file with a PEM extension indicates that the certificate is ASCII (Base64) encoded.
PFX	A PFX file can contain multiple certificates. It contains both the public and private keys for the certificates and should never be shared outside the organization.
CER	CER is the Microsoft convention for a CRT file which contains a certificate that is DER or PEM encoded.
P12	P12 (or, more formally, PKCS #12), is a format for storing multiple certificates in a single file. It is commonly used to package a private key with its certificate or package all members of a chain of trust.
P7B	P7B is a format used by Microsoft for certificate interchange.