7.5.2 Public Key Infrastructure Facts

Asymmetric encryption methods, which use a public key to provide confidentiality and trust, are generally used to encrypt data transmitted over the internet. Proper management and safety of these keys is important. Public key infrastructure (PKI) provides an environment in which public encryption keys can be created and managed. At the heart of PKI are certificate authorities (CAs) who are responsible for issuing, validating, and revoking certificates.

This lesson covers the following topics:

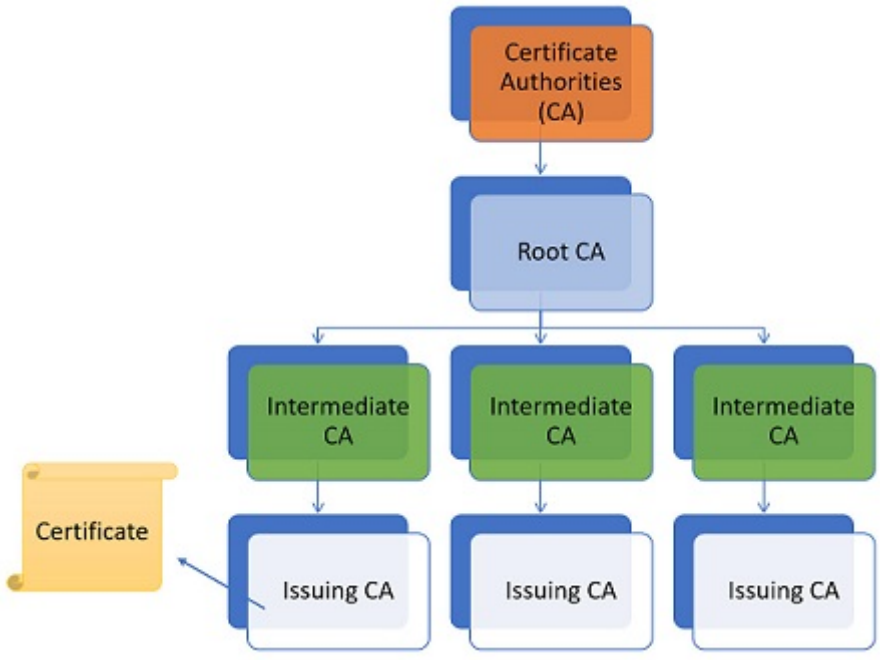
- Certificate authorities.
- Certificate process.
- Certificate attributes.

Certificate Authorities

Certificate authorities are reputable organizations, responsible for issuing public certificates to other companies or organizations for secure communication over the internet. Certificate authorities are generally set up in a hierarchy of multiple CAs to increase security. This is also known as certificate chaining. CAs are usually set up as follows:

- The first CA created is the root CA. The root CA has a self-signed certificate which is used to validate additional subordinate CAs.
- The subordinate CAs are known as intermediate CAs. These CAs validate issuing CAs.
- Issuing CAs validate and distribute the certificates.

The follow graphics depicts the CA hierarchy.



This structure is commonly used to protect the root CA. If the root CA is ever compromised, all issued certificates must be replaced. By implementing certificate chaining, only certificates issued by the compromised CA need to be replaced.

Certificate Process

For an organization to get a certificate, it submits a certificate signing request (CSR). This request generally includes the following information:

CSR Information	Description
Common name	The fully qualified domain name (FQDN) of the website. Example: www.testout.com
Subject alternative name (SAN)	An optional field. The SAN allows the organization to have multiple host names covered in one certificate. Example: site1.testout.com and site2.testout.com
Organization	The legal name of the organization. The name cannot be abbreviated and any suffixes, such as LLC, must be included. Example: TestOut Corporation
Organizational unit	This is the division that is handling the certificate. Example: IT Department
City/locality	City where the organization is located. Example: Pleasant Grove
State/county/region	State where the organization is located. This should not be abbreviated. Example: Utah
Country	The two-letter code for the country where the organization is located. Example: US
Email address	The email address for the person managing the certificate in the organization. Example: sysadmin@testout.com
Public key	Before filling out the CSR, the organization needs to generate a key pair. The public key will be included here.

Once the CSR has been submitted to the certificate authority, the certificate authority validates the information and issues the certificate.

Sometimes, the certificate authority may rely on a third party to perform the validation. These third parties are called registration authorities (RA). The RA is certified by a root certificate authority and is

authorized to issue certificates for specific uses only.

Certificate Attributes

Each CA has the responsibility of maintaining a database that contains the information, or attributes, of each certificate. The attributes that can be included are:

- Version - The X.509 version used for the certificate.
- Serial Number - A unique identifier for each certificate.
- Signature algorithm - The algorithm used to sign the certificate (SHA-2, RSA, etc.).
- Issuer - The CA that issues the certificate.
- Valid From and Valid To - The two fields that show the validity period of the certificate.
- Subject - The field that contains the name and location information of the organization.
- Public Key - The algorithm used to create the key and the public key information.

Depending on the organization, there may also be additional optional fields called extensions in the certificate.

One of the key attributes is the Valid To field. If a certificate is not renewed by this date, it will expire and no longer be valid. Aside from expiration, some other reasons a certificate might be invalidated are:

- The organization no longer exists.
- The private key has been compromised.
- The issued certificate is discovered to be fake.

If a certificate is invalidated for these or other reasons, it will be added to a certificate revocation list (CRL). The CRL is a blacklist of certificates. CAs must maintain and constantly update the CRLs as part of their databases. Web browsers automatically download updated CRLs at set intervals.

The X.509 standard also defines an internet protocol which can be used to determine the validity or state of a certificate. This is called the Online Certificate Status Protocol (OCSP). OCSP can be used to simplify the process of checking whether or not a certificate is valid.

OCSP is designed to replace CRLs. Instead of a CA maintaining the CRL, an OCSP server called a responder maintains the lists of any revoked certificate. When the browser connects to a site, the browser sends a request to the OCSP responder to check the validity of the certificate. OCSP provides the following benefits:

- Timely information on the status of a certificate.
- Better bandwidth management because the client does not download the entire CRL.
- A grace period for expired certificates.