7.5.4 Certificate Types Facts

PKI certificates are used to verify an organization's identity and ownership of a public key. When an organization requests a certificate, they must choose which type they need. The Certificate Authority needs to validate the organization before issuing the certificate. The level of validation depends on the certificate type being requested.

This lesson covers the following topics:

- Certificate types
- SSL validation levels

Certificate Types

Depending on the use and situation, there are different types of public key infrastructure (PKI) certificates. The following table explains what these certificate types are and how they can be used:

Certificate Type	Description
Root Certificate	A root certificate is the first certificate that a Certificate Authority creates. Root certificates are: ▪ Self-signed certificates. These certificates go through a different validation process which varies depending on the certificate and organization. ▪ Used to sign lower-level certificates such as intermediate certificates.
Subject Alternative Name (SAN)	SAN certificates allow an organization to cover multiple domains with one certificate. For example, TestOut could cover the following domains in a single SAN certificate: ▪ TestOut.com ▪ TestOut.net ▪ LabSim.com
Wildcard Certificate	Wildcard certificates are similar to SAN certificates. But instead of covering multiple domains, the organization can cover one domain and multiple subdomains. For example, TestOut could cover the following in one certificate: ▪ quiz.testout.com ▪ labs.testout.com ▪ videos.testout.com
Code Signing Certificate	Code-signing certificates are used by app developers to prove that their application is legitimate. If a user tries to run an app that does not have a certificate, they will receive an error stating that the app cannot be trusted. The user can decide to close the app or run it.
Self-Signed Certificate	Self-signed certificates are certificates that have not been validated or signed by a CA. ▪ Self-signed certificates are easy and free to make. ▪ Self-signed certificates do not provide the same protection and security as a CA-validated certificate.

	▪ When a user visits a website using a self-signed certificate, they see a warning that the certificate is not trusted.
Email Certificate	Secure, encrypted emails are sent using the S/MIME Protocol. ▪ Senders need to know the recipient's public key when sending a secure email. The public key is found in email certificates. ▪ Email certificates are mainly used in an organization that uses its own CA. But some public CAs provide email certificates as well.
User and Computer Certificate	User and computer certificates are used in a network environment to identify and validate specific users or computers. When a user or computers logs into a network, their certificate is sent to the server for validation. This provides extra security to the network.

SSL Validation Levels

The most common use of certificates is for websites using SSL or TLS. These certificates prove to the user that the site is legitimate and trustworthy. When a user visits a website that has been issued a certificate, they see a lock icon in the address bar. The user can click that lock to view the certificate information.

When a website purchases a certificate, there are three different levels of validation a CA can offer. The following table shows each level and how they are validated and used:

Validation Level	Description
Domain Validation	Domain validation is the lowest level of validation. With domain validation: ▪ A CA issues a domain-validated certificate to anyone listed as an administrator on the WHOIS record. ▪ Validation generally consists of a phone call or email. ▪ Certificates are usually issued within minutes.
Organization Validation	The organization validation is one step up from the domain validation. With organization validation: ▪ The purchaser needs to prove they are a domain administrator and also prove the organization is legitimate. ▪ The validation process includes proving the organization is real and some basic information. But it is not as in depth as the extended validation. ▪ These certificates can be issued in 1-3 days.
Extended Validation	Extended validation is the highest level of validation offered by a CA. With extended validation: ▪ The purchaser needs to prove they are a domain administrator and the CA will also validate all information on the organization. ▪ The CA will validate using a thorough and standardized identity verification process. This process includes proving: ▪ Exclusive rights to the domain ▪ The organization's legal, physical, and operational existence

	▪ The organization has authorized the issuance of the certificate ▪ These certificate can take up to 5 days to be issued.