7.5.10 Certificate Concepts Facts

Using digital certificates to share public keys and validate organizations is a critical component of doing business over the internet. Certificate authorities (CAs) are the trusted organizations that validate and administer digital certificates.

This lesson covers the following topics:

- Certificate chaining
- Certificate revocation list (CRL) management
- Trust models
- Private key safety

Certificate Chaining

Certificate authorities are generally setup in a hierarchy of multiple CAs to increase security.

- The first CA created is the root CA. The certificate is self-signed and 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.

This structure is known as certificate chaining or the Chain of Trust. It is commonly used to protect the root CA. For example, if the root CA is compromised, then all the certificates issued by that CA would need to be replaced. By implementing certificate chaining, if a CA is compromised, only the certificates issued by that CA would need to be replace.

Another common method of protecting the root CA is to bring it online only when it needs to authorize a new intermediate CA. Being offline means the root CA is isolated from all network access and is usually turned off.

Certificate Revocation List Management

A certificate revocation list contains a list of digital certificates that have been revoked by the issuing certificate authority before their scheduled expiration date and should no longer be trusted. If the root CA is taken offline, it can no longer maintain the CRL.

The following table describes other methods that can be used to keep track of these revoked certificates:

CRL Management	Description
Intermediate CA	An organization can choose to setup and configure an intermediate CA whose sole purpose is to maintain and update the CRL.
Online Certificate Status Protocol (OCSP)	The Online Certificate Status Protocol (OCSP) is a protocol that web browsers can use to quickly check the status of a certificate. The purpose of OCSP is to replace the need for the CRL. OCSP is commonly implemented using: - OCSP Stapling - OCSP stapling can be used to help with performance. Stapling means that the

	server holding the certificate also provides revocation information. This server sends a query to the OCSP responder at set intervals to verify the status of it's certificate. The server will attach, or staple, the response to it's certificate. - During the initial SSL or TLS handshake between the server and a user's web browser, the OCSP validation is sent along with the certificate removing the need for the browser to send a separate request for the certificate status. - Certificate pinning - Certificate pinning is when an application, such as a web browser, has a server's certificate hard coded into it. When the application connects to the server, it downloads and checks the certificate. If the two certificates don't match, the application takes appropriate action including blocking the connection. - Certificate pinning was never truly adopted by web browsers and is mostly used in organizations that have their own CA setup.

Trust Models

Trust models are configurations you can use to setup certificate authorities. The trust model you choose depends on the number of certificate authorities being implemented and their use. The following table explains each of these models:

Trust model	Description
Single trust model	All CAs start with a single trust model. This is the simplest model to setup. The single trust model has the following characteristics: - There is only one CA that issues and distributes certificates. - All users trust the CA and there are no trusts established with other CAs. - This model works properly only in a small organization. - If the CA is compromised, all certificates must be replaced.
Hierarchical model	A hierarchical model looks like a tree. - The first CA created is the root CA. It is a self-signed certificate and is used to validate additional subordinate CAs. - The subordinate CAs are known as intermediate CAs. The intermediate CAs validate issuing CAs. - Issuing CAs validate and distribute the certificates.
Mesh model	In the mesh model, multiple CAs are setup to issue certificates to each other. No CAs are configured in a subordinate relationship. - If a CA is compromised, certificates can still be trusted because multiple CAs have authenticated them. - This model is difficult and expensive to expand on a large scale.
Bridge model	The bridge model is a hybrid model that connects the hierarchical models of two organizations. - Clients in both organizations will trust certificates issued by CAs of either organization. - Trusts can be setup further down the tree for deeper customization and security.

Web of trust	A web of trust is typically used with Pretty Good Privacy encryption (PGP). Instead of implementing a CA, everyone is considered a trusted authority. For example, if User1 trusts User2 and User2 trusts User3, User1 will also trust User3.

Private Key Safety

To ensure data can always be recovered, you should create a backup of the private keys. It is important to have a backup and equally important that the backup is kept safe. The following table shows two main methods to backup private keys:

Key Backup Method	Description
Key archival	In key archival, the key is backed up by the CA. To do this, the user sends the private key in a secure transmission to the CA to back it up. This method is often used in an organization that manages its own CA. If keys are lost, they will be readily available and easily accessed. However, if the CA is breached, all private keys will be compromised.
Key escrow	Key escrow is a common method of key archival. With this method, keys are sent to a trusted 3rd party instead of a CA. This is often done for security and legal purposes. Legal action might be required to access the keys. This is done by design to ensure security and safety of the keys.