9.8.7 PKI Management Facts

Certificate management is the process of ensuring the security and availability of digital certificates. It requires meticulous planning, as well as maintenance and management throughout the public key infrastructure (PKI) system's lifetime. The integrity of the system is dependent on each system component. If any aspect of the initial and ongoing management of the keys is flawed, the strength of the entire cryptosystem can be compromised. Be aware of the following certificate management areas:

Management Area	Description
Key Protection	*Key protection* refers to using a different key structure for each service or function, such as files, messages, email attachments, transactions, etc. This allows an organization to limit its exposure if a key is compromised. ▪ Private keys should be protected and should never be shared or exposed. ▪ Public keys can be freely distributed.
Certificate Validation	*Certificate validation* is the process used by recipients of certificates to verify the identity of the certificate holder. The following are important considerations: ▪ Most certification validation occurs by PKI-enabled applications that receive the certificate and use the information in the certificate to validate the identity of the subject. ▪ The more information or points that are validated, the stronger the validation process, and the stronger the security of the PKI system. ▪ A requirement for the release of PKI-enabled applications should be the validation of the subject's digital certificate.
Key Archival	*Key archival* is the backup and archival of private keys for end users in case they lose their private keys. Normally, private keys are kept secret and the CA would never get a copy of the private key. Key archival and recovery is a complex, highly secure process that requires a significant amount of administrative overhead. With a key archival system: ▪ Private keys are sent to the CA and backed up by the CA. ▪ To protect the private keys during transit, they are encapsulated in a secure transmission of data to the CA. ▪ The location of the private keys' backup is secured. ▪ *Recovery agents* are usually administrators who are given the rights to restore private keys from the archive. Key archival uses a centralized approach to key management, where keys are managed by the CA and not only by individual users.
Key Escrow	*Key escrow* is a form of key archival. The main difference between key escrow and key archival is that escrow stores keys with a trusted third party, either to increase security or to allow access only under controlled circumstances. With key escrow, keys might be retrieved by a business that needs access to employee files, or it might allow key access to law enforcement with the proper authorization to investigate crimes or enforce laws.
Certificate Revocation	*Certificate revocation* is the process of breaking the bond of a public key pair to a specific individual. Revocation occurs when the end entity falls out of the PKI system's scope of trust. The following are situations in which a digital certificate would be revoked: ▪ The identity of the subject (either a person or the computer) changes, such as changing from a maiden name to a married name. ▪ An employee is terminated. ▪ An organization sells a division or changes its name. ▪ A private key is compromised by a hacker. ▪ A laptop with a PKI-enabled application is lost or stolen. Revoked certificates that are On Hold can be unrevoked. Certificates revoked for other reasons cannot be unrevoked.
Crypto Period	The *crypto period* is the amount of time that a pair of keys is valid. When determining the crypto period, take the following into consideration: ▪ A long crypto period requires less overhead but provides less security. Use a longer crypto period for less sensitive data. ▪ A short crypto period requires more overhead but provides more security. Use a shorter crypto period for data that has high sensitivity and heavy use. ▪ The life of a key should not be greater than the life of the entity or object for which it was created.
Certificate Renewal	*Certificate renewal* is the process of extending the validity of a certificate. Certificates that are nearing expiration do not need to be reissued; instead, they can be renewed. To ensure that certificates remain valid, they should be renewed before they expire.
Key Disposal	*Key disposal* refers to removing the key when the it (or the storage mechanism) is no longer being used.

	▪ Keys should not be disposed of until all data that was encrypted with those keys has been unencrypted or is no longer used. ▪ Use degaussing, overwriting, or media destruction to prevent the key from being recovered.

Be aware of the following when managing a PKI:

Consideration	Description

PKI Hierarchy	A typical PKI involves multiple certificate authorities (CAs) arranged in a hierarchy.
	▪ A *root* CA is the first CA in the hierarchy and the first CA to be set up. The root CA has a self-signed certificate and is often offline to protect the CA from compromise. The root CA does not usually issue certificates to end users or computers, unless the PKI structure is very small.
	▪ A *subordinate CA* is a CA authorized by the root CA to issue certificates to other CAs, users, computers.
	  ▪ The subordinate CA gets its certificate from the root CA.
	  ▪ Subordinate CAs are added to the hierarchy in order to to distribute the workload of issuing certificates, or to designate specific CAs to issue certificates for specific uses.
	  ▪ A subordinate CA is responsible for issuing certificates, holding the CPS, and publishing the Certificate Revocation List (CRL).
	  ▪ Qualified subordination is implemented on a subordinate CA to restrict the issuance and usage of certificates.
	The following are two types of subordinate CAs:
	  ▪ An *issuing* CA is at the bottom of the hierarchy, and actually issues the certificate to the clients.
	  ▪ An *intermediate* CA is in the middle of a multi-tier system, and certifies issuing CAs or other intermediate CAs.

Cross Certification	A cross-certification or bridge model is used when one organization with a CA structure needs to trust certificates from another organization that has its own CA structure. By default, clients in an organization will trust certificates issued by their organization, but they don't trust other root CAs unless they are in an official third party list on the internet for trusted root CAs. Cross certification can be set up so both hierarchies trust each other. ▪ A root-to-root configuration allows clients in one organization to trust any certificate issued by the other organization's CAs, and vice versa. ▪ A mesh configuration provides trust paths that can be configured for more restrictive certificate validation. This could include root-to-subordinate CA, or even subordinate-to-subordinate.
Dual Key Pairs	Each certificate that is issued has a corresponding public and private key pair. If users are issued a single key pair, that key pair is used for both digital signatures and encryption. In an enterprise environment, it might be beneficial to use two key pairs: one key pair for digital signatures, and the other for encryption. ▪ The private key used for digital signatures is kept completely private. Only the user has access to this key and the key is never archived. ▪ The private key used for encryption is archived so that encrypted documents can be recovered if the private key is lost. If a single key pair is used for both digital signatures and encryption, it is possible for a recovery agent to obtain the private key from the key archive and use that key for signing documents. This violates the principle of non-repudiation, because someone other than the original user could have signed the document.