Key Generation

- The key is created through key management by utilizing a hardware security model process.
- The key is generated from a cryptographically secure random bit generator.
- Alternatively, the key can be derived from an already existing key.
- Key derivation can also be done using a password and a key agreement performed by two entities using an approved key agreement scheme (Barker et al., 2020).
- Two admissible cryptographic keys have been identified by the federal government: symmetric and asymmetric keys (Barker & Roginsky, 2018).
- Elliptic Curve Cryptography (ECC) is typically used for smaller key sizes and better performance.

Provisioning

- Once a key is created, the database will store the key and its attributes.
- Attributes of the key may include name, date, activation size, etc.
- Each key has its strength, usually measured in bits, and is capable of protecting data throughout its lifetime.
- With the generated key, a Certificate Signing Request (CSR) is generated.
- The CSR is passed on to a Certificate Authority (CA), which:

  Validates the resource for which the certificate was requested.

  Issues a certificate, signed by the CA, that identifies the public key and the resource it is authenticated for.

Monitoring

- Once the key is generated and the certificate issued, it is crucial to ensure the safety of keys from unauthorized access, which is a part of key management (Furtak, 2020).
- A hardware security module (HSM) protects keys in a tamper-resistant vault, separate from the network.
- Key Encryption Keys (KEKs) can be used to encrypt keys before storing them in offline devices or databases.
- Secure storage API's can be used for further protection.
- Security is ensured by allowing only authenticated and authorized users or machines to use keys to encrypt or decrypt data.
- Implement multi-factor authentication (MFA) for key and certificate access to improve security.

- Use robust hash functions like SHA-256 or SHA-3 (NIST SP 800-57 Part 1) to prevent data integrity loss.

Management

- Keys must be regularly managed and monitored for the expiration of issued certificates to prevent downtime.
- Automated alert systems should notify administrators nearing the certificate's expiry date.
- Use the ACME protocol to automate certificate lifecycle management communications between the CA and the organization’s servers.
- Before certificate expiry, initiate a renewal process.

  The CA issues a new certificate with the same public key.

  A new CSR may need to be sent to the CA to authenticate ownership.

  Upon validation, a new certificate is issued, mostly using the same public key unless key renewal is necessary.

Revocation

- A cryptographic key that is compromised or lost can be detected using an intrusion detection system.
- Once a key is revoked, its status is communicated to users, and they are informed that the key can no longer be used for:

  Encrypting or decrypting messages.

  Verifying digital signatures.

- Notifications are sent to devices or applications linked to the certificate to stop using it immediately.
- The Certificate Authority (CA) updates the Certificate Revocation List (CRL), which lists compromised or untrustworthy certificates.
- The CRL helps maintain trust in secure communication by flagging certificates that should not be used.
- An alternative to the CRL is the Online Certificate Status Protocol (OCSP), which allows real-time checks of a certificate’s validity.
- Managing revoked certificates and ensuring they are not used is known as blacklist management.

Decommissioning

- Once a certificate has expired or is revoked due to a breach, the key issued by the certificate authority must be destroyed to mitigate risks.
- This process is called decommissioning.
- After key destruction, proof of deletion must be documented for compliance and auditing.
- Compliance with standards such as PCI DSS and GDPR is required for documentation and deletion processes.