Certificates

Digital Signature -> Cryptographic technique used to validate the authenticity and integrity of a message

- Authenticity -> Confirm that the signature was created by the known sender (non-repudiation)
- Integrity -> Ensure the message was not altered in transit

Creation of Digital Signature -> Hash a massage and then encrypt the hash with private key of the sender
Verify Digital Signature -> Use the sender public key to decrypt the hash so could validate the message it is integer

PKI (Public Key Infrastructure) -> A framework used to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. It is used to facilitate the secure electronic transfer of information for a range of network activities.

- Encryption and Decryption -> PKI allows users to encrypt and decrypt data using public and private keys
- Digital Signatures -> PKI provides for the creation and verification of digital signatures, ensuring the authenticity and integrity of data
- Certificate management -> The CA issues and revokes certificates as needed
- Certificate Signing Request (CSR) -> It is a request sent by an entity to a Certificate Authority to obtain a digital certificate (contains the entity's public key and identifying information, which the CA uses to create the digital certificate)
- Certificate revocation lists (CRLs) -> Lists maintained by CAs that contain the serial numbers of certificates that have been revoked before their expiration date
- Online Certificate Status Protocol (OCSP) -> Check the revocation status of a digital certificate in real-time.(It provides a faster and more efficient method than traditional CRLs)

Root of Trust -> Is just the very beginning or the most trusted part of this chain. If the Root CA is trusted, everything it vouches for can be trusted as well (it is typically a trusted entity or mechanism that is used to verify the authenticity of certificates and ensure the security of communications)