Digital Signature Trust Model Documentation

1. Introduction

This document outlines the trust model used in the implemented digital signature system. The model ensures authentication, integrity, and non-repudiation of digital communications through a hierarchical certificate authority (CA) structure.

2. Trust Model Overview

The trust model follows a Public Key Infrastructure (PKI) structure, where trust is established through certificate authorities (CAs) and digital signatures.

3. Components of the Trust Model

- **Root Certificate Authority (Root CA):** A self-signed entity that acts as the root of trust.
- **Intermediate Certificate Authorities (ICAs):** Entities that are signed by the Root CA and used to issue end-user certificates.
- **End-Entity Certificates:** Issued to users, servers, or applications for secure communication.
- **Certificate Revocation List (CRL) & Online Certificate Status Protocol (OCSP):** Used to verify certificate validity.

4. Process Flow

1. **Root CA Creation:**
    - A Root CA generates its own key pair and self-signs its certificate.
2. **Intermediate CA Setup:**
    - The Root CA signs the ICA's certificate, allowing it to issue certificates.
3. **End-Entity Certificate Issuance:**
    - The ICA signs end-user certificates.
4. **Message Signing:**
    - The user signs a message using their private key.
5. **Signature Verification:**
    - The recipient verifies the message using the sender's public key.
6. **Certificate Validation:**
    - The recipient ensures that the sender's certificate is valid by verifying its signature chain up to the Root CA.

5. Security Considerations

- **Private Key Protection:** Private keys must be securely stored.
- **Certificate Expiration & Revocation:** Expired or revoked certificates must be checked using CRL or OCSP.

- **Man-in-the-Middle (MitM) Prevention:** Certificates must be properly validated to prevent impersonation attacks.

6. Conclusion

This trust model ensures a secure and verifiable method for digital signatures, using hierarchical validation through certificate authorities. It forms the foundation for authentication and secure communication in cryptographic systems.