Trust Model Implementation Documentation

Introduction

A trust model defines how entities establish and verify trust in digital communications. This implementation follows a Public Key Infrastructure (PKI)-based trust model, which relies on digital certificates issued by a trusted Certificate Authority (CA).

Certificate Authority (CA)

In our implementation, the CA is responsible for issuing self-signed certificates that authenticate entities in a network. The CA:

- Generates its own RSA key pair.
- Issues and signs certificates for entities.
- Provides a mechanism for verifying certificate authenticity.

Certificate Generation

Each entity generates an RSA key pair consisting of a private key and a public key. The public key is included in a certificate that is signed by the CA. The certificate contains:

- The entity’s identity (e.g., common name).
- The public key.
- The certificate's validity period.
- The digital signature of the CA.

Signature Verification Process

1. When an entity receives a signed message, it also receives the sender’s certificate.
2. The entity extracts the public key from the certificate and verifies:
    - The certificate is issued by a trusted CA.
    - The certificate has not expired.
    - The signature is valid.
3. If all checks pass, the message is considered authentic.

Trust Chain

The model supports hierarchical trust, where multiple certificates can be chained together. A root CA issues certificates to intermediate CAs, which in turn issue certificates to end entities. This ensures scalability and enhanced security.

Certificate Revocation

To maintain trust, certificates can be revoked before their expiration if:

- The private key is compromised.
- The entity is no longer trusted.
- The certificate is found to be fraudulent.

Revocation methods include:

- **Certificate Revocation Lists (CRLs):** Periodically published lists of revoked certificates.
- **Online Certificate Status Protocol (OCSP):** Real-time certificate status verification.

Conclusion

This trust model ensures secure communication by leveraging digital certificates and RSA signatures. By verifying certificates against a trusted CA, entities can authenticate each other securely, preventing unauthorized access and man-in-the-middle attacks.