PKI Service Integration Guidelines (For Developers)

Ensuring the proper integration of Public Key Infrastructure (PKI) services is essential for maintaining the security and integrity of digital systems. RISA offers crucial services for certificate validation and timestamping, which are foundational to secure a proper use of the digital signature service. When using the digital signature and other PKI services, it is important to adhere to specific guidelines that ensure the authentication, integrity and reliability of the provided services. This document outlines the key areas of focus, including certificate validity check, revocation, certificate expiration, and signature validation check, to help users and developers to meet these critical standards.

- Certificate Revocation
- Certificate Expiration
- Signature Validation
- Password Management
- Timestamp Validation (Optional)

Certificate Revocation

Objective:

Ensure your system correctly performs the certificate validity check.

Guidelines:

- The deployed system should be able to checks the certificate validity i.e. to check if the certificate is not revoked. Two protocols are used:
  - OCSP (Online Certificate Status Protocol) and /or
  - CRL (Certificate Revocation List).
- Ensure that revoked certificates are rejected by the system, and log the event for auditing purposes.
  The user should get a proper communication message in case a revoked certificate is used

Certificate Expiration

Objective

Prevent the use of expired certificates in your system.

Guidelines

- Automatically check the certificates validity period during the validation process.
- Ensure that expired certificates are not accepted by the system for any operation.
- The user should get a proper communication message in case they use an expired certificate

Signature Validation

Objective:

Validate the authenticity and integrity of digital signatures, including Long-Term Validation (LTV) or Time-based validity.

Guidelines:

- Implement validation mechanisms to verify digital signatures against trusted certificates.
- Enable Long-Term Validation (LTV) in your EDS to ensure that signatures remain valid even after the signing certificate expires.
- In case limited time validity is applied, the system should be able to check the signature validity type, and provide an understandable message to the user in case the signature validity time is exceeded.

Password Management

Objective:

Ensure secure handling of user certificate passwords.

Guidelines:

- Do not store user certificate passwords in the database or on any easily accessible file.
- It is the user responsibility to ensure the password protection
- Use HTTPS to encrypt data transmitted between the user's browser and your server, protecting passwords from interception during transmission

Timestamp Validation (Optional)

Objective:

Validate the timestamps associated with digital signatures to ensure their reliability and time synchronization.

Guidelines:

- Use a trusted Time Stamping Authority (TSA) to provide accurate and synchronized timestamps for digital signatures.
- The use of a centralized timestamp is mandatory. RISA-GovCA provides a centralized TSA system.

By following these guidelines, developers can ensure that their PKI service integration meets the required standards for security and reliability. Implementing these practices should be a fundamental part of the development process to ensure compliance with industry standards. Before deploying the PKI services, developers must contact RISA at pki@risa.gov.rw . RISA will then perform the PKI service integration assessment.