==========

==========

CATEGORY: WindowsCertificates

==========

==========

Certificate operations directly affect authentication, encryption, secure communications, identity management, and compliance. These SOPs ensure every certificate-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with enterprise security standards.

SOP 1 – List Certificates

Script Name: List Certificates **Category:** WindowsCertificates **Version:** 1.0 **Approved By:** Security Operations / PKI Team

1. Purpose

This script enumerates certificates in a specified certificate store, supporting troubleshooting, compliance, and inventory.

2. Scope

- Local machine and user certificate stores
- All certificate types (SSL, Code Signing, Client Auth, etc.)

3. Definitions

- Certificate Store – Logical container for certificates.
- Thumbprint – Unique identifier for a certificate.

4. Preconditions

- Operator must have permission to read the certificate store

5. Required Inputs

- Store location (LocalMachine or CurrentUser)
- Store name (My, Root, CA, etc.)

6. Procedure Steps

- Input Collection – Wizard prompts for store location and name.
- Store Validation – Confirm store exists.
- Certificate Enumeration – Retrieve certificates.
- Attribute Extraction – Subject, Issuer, Expiration, Thumbprint, Enhanced Key Usage.
- Output Formatting – Present structured certificate list.
- Logging – Store, operator, timestamp.

7. Expected Output

- List of certificates with key metadata

8. Post-Execution Validation

- Operator may verify via certlm.msc or certmgr.msc

9. Error Handling

- Store not found
- Access denied
- No certificates found

10. Security Considerations

- Certificate metadata may reveal sensitive identity information

11. Audit Logging Requirements

- Operator ID
- Store accessed
- Timestamp

12. Organizational Benefit Statement

- Provides a controlled, auditable method for certificate inventory

SOP 2 – Get Certificate Details

1. Purpose

Retrieve detailed metadata for a specific certificate.

5. Required Inputs

- Thumbprint
- Store location
- Store name

6. Procedure Steps

- Input Collection
- Certificate Resolution
- Metadata Extraction – Key length, EKUs, serial number, issuer chain, validity period.
- Output Formatting
- Logging

SOP 3 – Import Certificate

1. Purpose

Import a certificate into a specified store.

5. Required Inputs

- Certificate file path
- Store location
- Store name
- Optional: Password for PFX

6. Procedure Steps

- Input Collection
- File Validation
- Import Operation
- Post-Import Verification
- Logging

SOP 4 – Export Certificate

1. Purpose

Export a certificate (with or without private key).

5. Required Inputs

- Thumbprint
- Export path
- Optional: Include private key
- Optional: PFX password

6. Procedure Steps

- Input Collection
- Certificate Resolution
- Export Operation
- Post-Export Verification
- Logging

SOP 5 – Remove Certificate

1. Purpose

Delete a certificate from a store.

5. Required Inputs

- Thumbprint
- Store location
- Store name

6. Procedure Steps

- Input Collection
- Certificate Resolution
- Safety Check – Prevent deletion of system-critical certificates.
- Removal Operation

- Post-Removal Verification
- Logging

SOP 6 – Test Certificate Chain

1. Purpose

Validate certificate trust chain and revocation status.

5. Required Inputs

- Thumbprint

6. Procedure Steps

- Input Collection
- Chain Building
- Revocation Checking
- Output Formatting
- Logging