==========

CATEGORY: Certificates

==========

SOP 1 – Find Certificate by Thumbprint

Script Name: Find Certificate by Thumbprint **Category:** Certificates **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose

This script locates a certificate in a specified certificate store using its thumbprint. It provides a controlled, auditable method for identifying certificates used for authentication, encryption, signing, or application binding.

2. Scope

- **Systems:** Windows systems with accessible certificate stores.
- **Stores:** LocalMachine and CurrentUser certificate stores.
- **Authorized Personnel:**
    - PKI administrators
    - Security engineers
    - Application support teams

3. Definitions

- **Certificate Thumbprint:** A SHA-1 hash uniquely identifying a certificate.
- **Certificate Store:** A logical storage location for certificates (e.g., My, Root, CA).

4. Preconditions

- Operator must have read access to the target certificate store.
- Certificate store must be accessible on the local system.
- Thumbprint must be known and valid.

5. Required Inputs

- Certificate thumbprint
- Certificate store location (e.g., LocalMachine\My)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for thumbprint and store.
    - Validate thumbprint format (hexadecimal, no invalid characters).
2. **Store Resolution**
    - Open the specified certificate store.
    - If store does not exist, abort and log.
3. **Certificate Search**
    - Normalize thumbprint (remove spaces).
    - Enumerate certificates in store.
    - Compare each certificate’s thumbprint.
4. **Match Handling**
    - If found, retrieve certificate details:
        - Subject
        - Issuer
        - Expiration date
        - Enhanced Key Usages
        - Serial number
    - If not found, return “Certificate not found.”
5. **Output Formatting**
    - Present certificate details in structured format.
6. **Logging**
    - Log thumbprint, store, operator, timestamp.

7. Expected Output

- Certificate details if found.
- Clear message if not found.

8. Post-Execution Validation

- Operator may verify certificate presence using MMC or PowerShell.

9. Error Handling

- Invalid thumbprint format
- Store not found
- Access denied

10. Security Considerations

- Certificate metadata may reveal sensitive information; restrict access.
- Do not export or share certificate details outside approved channels.

11. Audit Logging Requirements

- Operator ID
- Thumbprint
- Store
- Timestamp

12. Organizational Benefit Statement

This script provides a reliable, auditable method for locating certificates, supporting troubleshooting, PKI management, and application configuration.

SOP 2 – List Certificates in Store

Script Name: List Certificates in Store **Category:** Certificates

1. Purpose

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

2. Scope

- LocalMachine and CurrentUser stores
- Used by PKI, security, and application teams

3. Definitions

- **Certificate Store:** Logical container for certificates.

- **EKU:** Enhanced Key Usage, defining certificate purpose.

4. Preconditions

- Operator must have read access to the store.
- Store must exist.

5. Required Inputs

- Certificate store location (e.g., LocalMachine\My)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for store path.
2. **Store Resolution**
    - Attempt to open store.
    - Abort if store unavailable.
3. **Certificate Enumeration**
    - Retrieve all certificates.
    - Extract key attributes:
        - Subject
        - Issuer
        - Expiration
        - Thumbprint
        - EKUs
4. **Output Formatting**
    - Present list in table/JSON format.
5. **Logging**
    - Log store name, certificate count, operator.

7. Expected Output

- List of certificates with key metadata.

8. Post-Execution Validation

- PKI team may compare with MMC or monitoring tools.

9. Error Handling

- Store not found
- Access denied

10. Security Considerations

- Certificate metadata may reveal internal infrastructure.
- Access should be restricted to authorized personnel.

11. Audit Logging Requirements

- Operator ID
- Store name
- Certificate count
- Timestamp

12. Organizational Benefit Statement

This script provides a standardized, auditable method for certificate inventory, supporting compliance and lifecycle management.

SOP 3 – Export Certificate to File

Script Name: Export Certificate to File **Category:** Certificates

1. Purpose

This script exports a certificate (with or without private key) to a file for backup, migration, or application configuration. It ensures the export process is controlled and logged.

2. Scope

- Certificates in LocalMachine or CurrentUser stores
- Export formats: CER, PFX (depending on permissions)

3. Definitions

- **PFX:** Certificate file containing private key (password-protected).
- **CER:** Certificate file containing public key only.

4. Preconditions

- Operator must have read access to certificate.

- Exporting private keys requires elevated permissions.
- Export path must be writable.

5. Required Inputs

- Certificate thumbprint
- Store location
- Export path
- Export type (CER/PFX)
- Password (for PFX)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for thumbprint, store, export type, and path.
2. **Store Resolution**
    - Open store and locate certificate.
3. **Certificate Validation**
    - Confirm certificate exists.
    - If PFX export requested, confirm private key is exportable.
4. **Export Operation**
    - Export certificate to specified format.
    - For PFX:
        - Encrypt with provided password
        - Write to file
5. **Post-Export Verification**
    - Confirm file exists and is readable.
6. **Logging**
    - Log certificate thumbprint, export type, path, operator.

7. Expected Output

- Confirmation of successful export.
- Path to exported file.

8. Post-Execution Validation

- Operator may import file on test system to confirm integrity.

9. Error Handling

- Certificate not found
- Private key not exportable
- Access denied
- Invalid path

10. Security Considerations

- Exporting private keys is highly sensitive; ensure approvals.
- PFX files must be stored securely.
- Passwords must not be logged.

11. Audit Logging Requirements

- Operator ID
- Thumbprint
- Export type
- Export path
- Timestamp

12. Organizational Benefit Statement

This script ensures certificate export operations are performed safely, consistently, and with full auditability, reducing risk during migrations and application deployments.

SOP 4 – Remove Certificate

Script Name: Remove Certificate **Category:** Certificates

1. Purpose

This script removes a certificate from a specified certificate store, supporting certificate lifecycle management, decommissioning, and security cleanup.

2. Scope

- LocalMachine and CurrentUser stores

- Used by PKI, security, and application teams

3. Definitions

- **Certificate Removal:** Deleting a certificate from a store so it can no longer be used.

4. Preconditions

- Operator must have write access to the store.
- Certificate must exist.
- Removal must be authorized (e.g., expired, compromised, replaced).

5. Required Inputs

- Certificate thumbprint
- Store location

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for thumbprint and store.
2. **Store Resolution**
    - Open store.
3. **Certificate Lookup**
    - Locate certificate by thumbprint.
4. **Removal Confirmation**
    - Script may require explicit confirmation (depending on policy).
5. **Removal Operation**
    - Remove certificate from store.
6. **Post-Removal Verification**
    - Requery store to confirm certificate no longer exists.
7. **Logging**
    - Log thumbprint, store, operator, timestamp.

7. Expected Output

- Confirmation that certificate was removed.

8. Post-Execution Validation

- PKI team may verify via MMC.
- Applications relying on certificate should be tested.

9. Error Handling

- Certificate not found
- Access denied
- Store not found

10. Security Considerations

- Removing certificates may break services; ensure approvals.
- Removal of compromised certificates should follow incident response procedures.

11. Audit Logging Requirements

- Operator ID
- Thumbprint
- Store
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for removing certificates, supporting secure lifecycle management and reducing risk from expired or compromised certificates.