SmartCard-HSM

n-of-m Authentication Scheme
SmartCard-HSM is a light-weight, remote-manageable and user-centric hardware security module for secure key generation and storage.

n-of-m authentication allows strict access control for sensitive keys.
Motivation

- Certain cryptographic keys require very strict access control because a loss of control has a dramatic impact on security or data privacy.
- Examples for such keys are:
  - CA Root Keys
  - Escrow Keys
  - System Access Control Keys
  - Code Signing Keys
  - The Internet DNSSEC Root Keys (www.root-dnssec.org)
Dual Control / 4-Eye Principle

- A classical control measure is Dual-Control, also known as 4-Eye Principle
- Two persons (Key Custodians) need to collaborate in order to access the key
- A single person can not act without the other
- An attacker will need to compromise both persons

Problem: If one person is not available, the scheme breaks
n-of-m Control

- n-of-m control requires n key custodians out of a group of m key custodians to collaborate in order to access a key.
- Any combination of n key custodians collaborating allows access to the key.
- If a single key custodian becomes unavailable, then the scheme still works until less than n key custodians are left.
- m is defined initially and cannot be changed at a later stage.
- Classic algorithm: Shamir Shared Secret.
n-of-m and the SmartCard-HSM

- The sc-hsm-tool implements n-of-m control for the Device Key Encryption Key (DKEK) using Shamir Shared Secret
- n-of-m for the DKEK is implemented outside the chip, as the current chip platform does not provide the required primitives to implement the algorithm
- n-of-m for authentication is implemented inside the chip and replaces the User-PIN authentication mechanism
Preconditions

- n-of-m for authentication requires
  - a set-up phase during which key custodians are enrolled
  - a use phase during which key custodians enable access to keys
- The SmartCard-HSM for the sensitive key is initialized during the set-up phase
- Each key custodian has its own SmartCard-HSM that contains his personal authentication key
- Key custodians don't need to be physically present in any phase, as the protocol is designed to work remote
The build-in PKI issues a Card Verifiable Certificate (CVC) for each generated public key.

The authenticity of the public key can be validated using the chain from Scheme Root CA (SRCA), the Device Issuer CA (DICA) to the Device Authentication Certificate (DevAut) in each SmartCard-HSM.
CVC Validation

- The SmartCard-HSM can validate Device Issuer CA and Device Authentication Certificates using the PSO VERIFY CERTIFICATE command.

- The Scheme Root CA certificate is embedded as trust-anchor in each SmartCard-HSM.
Public Key Registration

- Allows to register a public key for authentication during the set-up phase

- All $m$ public keys of key custodians are registered
- After all keys are imported, the device is operational
Set-Up Phase

Administrator
1. Initialize SmartCard-HSM
2. Select number of key custodians (m)
3. Define threshold for verification (n)
4. Import public keys of key custodians

Key Custodian #1
1. Choose PIN
2. Generate Key

Key Custodian #2
1. Choose PIN
2. Generate Key

Key Custodian #3
1. Choose PIN
2. Generate Key
Public Key Authentication

- Authenticate using the private key and a previously registered public key

- Within a session this can be repeated multiple times
- The authentication state is reset during logout or power-off
- Access is granted if n or more public keys are authenticated
Use Phase

n Key Custodians are required to authenticate towards the SmartCard-HSM in order to allow access to keys

Key Custodian #1
Verify PIN
Authenticate

Key Custodian #2
Not involved

Key Custodian #3
Verify PIN
Authenticate

2-of-3

Public Key Authentication
Thank you for your attention

Please direct queries to
andreas.schwier@cardcontact.de
frank.thater@cardcontact.de