SoftHSM2 Setup

CBOM Secure · HSM Sensor (PKCS#11)

Overview

This guide installs, configures, and integrates SoftHSM2 with the CBOM Secure HSM Discovery Sensor. Over PKCS#11 the sensor lists initialized token slots and enumerates private keys, public keys, certificates, and secret keys, reading metadata (label, key type, size, object ID, token label) read-only — never extracting private-key material. SoftHSM2 is well suited to development, CI/CD, and lab environments.

Prerequisites

- root or sudo access on the host (Linux or macOS).
- SoftHSM2 installed (or permission to install it).
- The CBOM Collector agent deployed on the host.
- The SO-PIN and User PIN for each token to scan.

Step-by-Step Guide

Step 1: Install SoftHSM2

```
# Debian/Ubuntu
sudo apt-get install -y softhsm2 opensc       # lib: /usr/lib/softhsm/libsofthsm2.so
# RHEL/Rocky/Fedora
sudo dnf install -y softhsm opensc           # lib: /usr/lib64/softhsm/libsofthsm2.so
# macOS (Homebrew)
brew install softhsm                        # lib: /usr/local/lib or /opt/homebrew/lib
```

Step 2: Configure SoftHSM2

```
sudo mkdir -p /etc/softhsm /var/lib/softhsm/tokens
sudo tee /etc/softhsm/softhsm2.conf > /dev/null <<EOF
directories.tokendir = /var/lib/softhsm/tokens/
objectstore.backend = file
log.level = ERROR
slots.removable = false
EOF
softhsm2-util --show-slots
```

Step 3: Initialize a Token

```
softhsm2-util --init-token --slot 0 --label "CBOM-Test-Token" \
  --so-pin <SO-PIN> --pin <USER-PIN>
# SoftHSM reassigns the slot ID after init:
softhsm2-util --show-slots
```

Note Note the new Slot ID shown for the initialized token — it is used in the sensor config.

Step 4: Collect Credentials

For each token, record: the library path, the slot ID (softhsm2-util --show-slots), the User PIN, and the token label.

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_HSM
  type: softhsm2
  lib_path: /usr/lib/softhsm/libsofthsm2.so
  tokens:
    - slot_id: 1
      token_label: "CBOM-Test-Token"
      user_pin: "${SOFTHSM_USER_PIN}"
  discovery:
    object_types: [CKO_PRIVATE_KEY, CKO_PUBLIC_KEY, CKO_CERTIFICATE,
CKO_SECRET_KEY]
    read_metadata_only: true
scan_name: SoftHSM2Discovery
```

Adjust lib_path per platform (Debian /usr/lib/softhsm, RHEL /usr/lib64/softhsm, macOS Homebrew paths).

Step 6: Validate

```
pkcs11-tool --module /usr/lib/softhsm/libsofthsm2.so --show-info
softhsm2-util --show-slots
```

Confirm the library loads (Cryptoki 2.40, Manufacturer SoftHSM) and tokens show Initialized: yes with the right labels/slot IDs. Run the CBOM discovery task and confirm objects appear under Crypto Assets with no PIN errors.

Common Errors

CKR_PIN_INCORRECT

Cause: The User PIN in the config doesn't match the PIN set at --init-token.

Resolution: Verify by logging in with pkcs11-tool; reset the token with the SO-PIN if the PIN is unknown.

CKR_TOKEN_NOT_PRESENT

Cause: The slot_id doesn't correspond to an initialized token, or SOFTHSM2_CONF is wrong.

Resolution: Re-run --show-slots, update slot_id, and confirm the config file path.

Cannot load PKCS#11 library

Cause: lib_path points to a missing/incorrect file.

Resolution: find /usr /opt/homebrew -name libsofthsm2.so and update lib_path.

Security Recommendations

- SoftHSM2 does not protect key material in hardware — use a hardware HSM for production.
- Restrict the token directory to the collector account (chmod 750).
- Use strong PINs (12+ chars) and store them in a secrets manager, not plaintext YAML.
- Rotate User PINs periodically via the SO-PIN without re-initializing the token.
- Keep the SO-PIN offline, separate from operational credentials.

Conclusion

The HSM Discovery Sensor enumerates public keys, private-key metadata, certificates, and secret-key metadata in SoftHSM2 read-only. The same configuration structure applies to hardware PKCS#11 HSMs (Thales Luna, Entrust nShield, etc.) by updating only the library path and credential fields.