Nitrokey HSM 2 / SmartCard-HSM Setup

CBOM Secure · HSM Sensor (PKCS#11 / OpenSC)

Overview

This guide configures a Nitrokey HSM 2 (or compatible SmartCard-HSM) so the CBOM Secure HSM Sensor can discover its cryptographic material over the OpenSC PKCS#11 interface, read-only:

- Asymmetric private keys (RSA, ECC) in on-device key slots
- X.509 certificates associated with device key pairs
- Key metadata - key ID, type, size/curve, label, slot assignment
- Device/token attributes - manufacturer, model, serial, firmware, supported mechanisms

Prerequisites

- A Nitrokey HSM 2 or compatible SmartCard-HSM connected to the sensor host (or a PKCS#11 proxy).
- OpenSC installed (opensc, opensc-pkcs11); verify opensc-tool / sc-hsm-tool / pkcs11-tool.
- The PKCS#11 library present (e.g. /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so).
- The device SO-PIN (only if initializing); pcscd running.
- The sensor service account has read access to the library and the pcscd socket.
- sudo rights on the host for initial device setup.

Step-by-Step Guide

Step 1: (First-Time) Initialize the Device

Skip if the device already has an SO-PIN and User PIN. Confirm detection, then initialize:

```
opensc-tool --list-readers

sc-hsm-tool --initialize \
  --so-pin <SO-PIN> \
  --pin <USER-PIN> \
  --label "CBOM-HSM" \
  --reader 0

pkcs11-tool --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so --list-slots
```

Note Store the SO-PIN in a secrets manager - losing it prevents re-initialization. The sensor only needs the User PIN. Record the token serial to pin the sensor to a specific device.

Step 2: Confirm the Read-Only User PIN and Slot

The device has a single User PIN; it grants enumeration without allowing external signing/decryption. Confirm it lists objects and note the slot index and library path:

```
pkcs11-tool \
  --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so \
  --login --pin <USER-PIN> --list-objects

pkcs11-tool --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so --list-slots
realpath /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
```

On RHEL/Fedora the library is typically /usr/lib64/opensc-pkcs11.so. If the sensor runs as a non-root account, add it to the pcscd group and re-verify slot visibility under that account.

Step 3: Pre-Check Key Metadata

```
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so --login --pin <USER-PIN> --
list-objects --type privkey
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so --login --pin <USER-PIN> --
list-objects --type cert
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so --list-mechanisms --slot 0
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: Discover_HSM
    type: pkcs11_hsm
    enabled: true
    connection:
      pkcs11_library: /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
      slot_index: 0
      token_label: CBOM-HSM
      token_serial: NKHS2XXXXXXXX
    credentials:
      user_pin: "${CBOM_HSM_USER_PIN}"
    discovery:
      include_private_keys: true       # metadata only; no key material exported
      include_certificates: true
      include_public_keys: true
      include_mechanisms: true
      read_only: true
    scan_schedule:
      cron: "0 2 * * *"
    output:
      tags: { device_type: nitrokey-hsm2, location: on-premise }
```

Inject CBOM_HSM_USER_PIN via a systemd EnvironmentFile (mode 0600, owned by the sensor account) or a secrets manager - never hard-code it.

Step 5: Validate

```
cbom-sensor scan --sensor Discover_HSM --dry-run --verbose
cbom-sensor scan --sensor Discover_HSM
```

Confirm the token connects (serial matches) and private keys, certificates, public keys, and mechanisms are discovered. Verify under Assets -> HSM Keys filtered by device_type: nitrokey-hsm2; the object count should match pkcs11-tool --list-objects and be unchanged after the scan (no writes).

Common Errors

CKR_TOKEN_NOT_PRESENT

Cause: The device is not detected by PC/SC - pcscd stopped, USB disconnected, or the account lacks socket access.

Resolution: Start/enable pcscd, confirm opensc-tool --list-readers, and add the sensor account to the pcscd group.

CKR_PIN_INCORRECT / CKR_PIN_LOCKED

Cause: The User PIN does not match; repeated failures lock the PIN.

Resolution: Check CBOM_HSM_USER_PIN (no whitespace). If locked, unblock with the SO-PIN (sc-hsm-tool --unblock-pin where supported).

Cannot load module / opensc-pkcs11.so not found

Cause: OpenSC is not installed or the library path is wrong for the OS/arch.

Resolution: find /usr /lib -name opensc-pkcs11.so, update pkcs11_library (RHEL: /usr/lib64/...), and ensure libpcsclite is installed.

Security Recommendations

- Never hard-code the User PIN; inject via env/secrets manager (secrets file mode 0600).
- Run the sensor as a dedicated non-root account with only pcscd group membership.
- Restrict physical USB access; log attach/detach via udev.
- Alert on repeated CKR_PIN_INCORRECT events in pcscd/OpenSC logs.
- Keep OpenSC updated and rotate the User PIN on schedule.

Conclusion

The HSM Sensor authenticates to the Nitrokey HSM 2 with the User PIN over the local PC/SC interface and enumerates private-key metadata, certificates, public keys, and mechanisms read-only - no key material leaves the device - keeping CBOM Secure's inventory of hardware-token keys current.