

SmartCard-HSM (Ultrasafe) Setup

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

Overview

This guide integrates a SmartCard-HSM (Ultrasafe) device with CBOM Secure. The HSM Sensor connects over the OpenSC PKCS#11 interface and performs read-only discovery of asymmetric and symmetric keys, X.509 certificates, data objects, and key attributes (algorithm, length, label, CKA_ID, usage flags, lifecycle state). It uses the Crypto User role and never writes to the device.

Prerequisites

- A SmartCard-HSM device attached and recognized (USB reader or integrated slot).
- OpenSC installed (opensc, opensc-pkcs11, libpcsclite-dev, pcscd) and pcscd running.
- The device visible to opensc-tool --list-readers.
- The Security Officer (SO) PIN (for initialization / creating a Crypto User PIN).
- sc-hsm-tool and pkcs11-tool available; the CBOM sensor agent installed on the host.

Step-by-Step Guide

Step 1: (First-Time) Initialize the Device

Skip if the device is already initialized with active SO and User PINs. Otherwise:

```
sc-hsm-tool --initialize \  
--so-pin <SO_PIN> --pin <USER_PIN> --label "CBOM-HSM"  
# optionally add --dkek-shares 1 for key backup capability
```

Step 2: Set a Read-Only Crypto User PIN

```
pkcs11-tool \  
--module /usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so \  
--change-pin --login --pin <CURRENT USER PIN> --new-pin <CBOM USER PIN>
```

Confirm the Crypto User can enumerate objects:

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

Step 3: Identify Slot and Library, Grant PC/SC Access

```
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so --list-slots  
# note the slot index and token serial (e.g. UTSC00000001)  
  
sudo usermod -aG plugdev cbom-agent  
sudo -u cbom-agent pkcs11-tool \  
--module /usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so --list-slots
```

Note On RHEL/CentOS the library is at /usr/lib64/pkcs11/opensc-pkcs11.so.

Step 4: Configure the CBOM Secure Sensor

```
sensors:
- name: Discover_HSM
  type: hsm
  enabled: true
  connection:
    pkcs11_module: /usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
    slot: 0
    token_label: CBOM-HSM
    token_serial: UTSC00000001
  auth:
    user_type: CKU_USER
    pin_env: CBOM_HSM_USER_PIN
  discovery:
    object_types: [private_keys, public_keys, symmetric_keys, certificates, data_objects]
    collect_attributes: [CKA_LABEL, CKA_ID, CKA_CLASS, CKA_KEY_TYPE,
CKA_VALUE_LEN,
    CKA_MODULUS_BITS, CKA_EC_PARAMS, CKA_SIGN, CKA_VERIFY,
CKA_EXTRACTABLE, CKA_SENSITIVE,
    CKA_START_DATE, CKA_END_DATE]
  schedule:
    interval: 24h
  output:
    tags: { device_type: smartcard-hsm, vendor: ultrasafe }
export CBOM_HSM_USER_PIN="<CBOM_USER_PIN>"
sudo -E systemctl restart cbom-agent
```

Step 5: Validate

```
cbom-agent sensor run --name Discover_HSM --dry-run
```

Confirm the module loads, the token connects, CKU_USER authenticates, and keys/certificates are discovered; verify under Assets → Cryptographic Keys filtered by Source: Discover_HSM.

Common Errors

CKR_PIN_INCORRECT

Cause: The PIN variable doesn't match the Crypto User PIN, or isn't exported into the agent's environment.

Resolution: Re-export CBOM_HSM_USER_PIN and restart with systemctl restart cbom-agent; verify it is set in the agent's environment.

PCSC error: No such device

Cause: pcscd is not running, the reader is disconnected, or the agent lacks reader access.

Resolution: Restart pcscd, confirm with opensc-tool --list-readers, and ensure cbom-agent is in the plugdev group.

CKR_SLOT_ID_INVALID

Cause: The slot index changed after a USB re-enumeration.

Resolution: Re-run `--list-slots`, or use `token_label` / `token_serial` for stable identification.

Security Recommendations

- Use the Crypto User PIN only — never the SO PIN, which can modify device configuration.
- Store the PIN in a secrets manager rather than a shell profile or unit file.
- Restrict the config to the agent account (`chmod 600`).
- Enable PIN lockout (5 or fewer attempts) and keep any DKEK share offline.
- Limit plugdev membership and review CBOM discovery logs for auth failures.

Conclusion

The HSM Sensor connects to the SmartCard-HSM via OpenSC PKCS#11, authenticates as a read-only Crypto User, and enumerates all key objects, certificates, and data objects — providing a continuously updated cryptographic inventory in CBOM Secure.