

Entrust nShield Setup

CBOM Secure · HSM Sensor (Discover_HSM)

Overview

This guide configures the CBOM Secure HSM sensor to connect to an Entrust nShield HSM over PKCS#11 and enumerate cryptographic objects in the nShield Security World, read-only:

- CKO_PRIVATE_KEY — private keys protected by the Security World
- CKO_PUBLIC_KEY — public keys associated with key pairs
- CKO_CERTIFICATE — X.509 certificates in the HSM token
- CKO_SECRET_KEY — symmetric keys (AES, DES, etc.)

For each object the sensor reads label, key type, key size, and object ID. It never extracts private-key or secret-key material.

Prerequisites

- An Entrust nShield HSM (Connect XC, Solo XC, or equivalent) installed and joined to a Security World.
- The nShield client software installed (default /opt/nfast/).
- The PKCS#11 library present at /opt/nfast/toolkits/pkcs11/libcknfast.so.
- Access to the nShield Management Console; the Security World created and distributed.
- CipherTools Manager available for creating operator credentials.
- The Discover_HSM sensor package installed, and connectivity to a network nShield on port 9004.

Step-by-Step Guide

Step 1: Create an Operator Card Set (OCS)

In the nShield Management Console, under Security World mgmt → Operator Card Sets → Create new OCS, set Name CBOM-Sensor-OCS, K of N 1 of 1, Persistent Yes, set a passphrase (store it in your vault), and write the card. Then verify on the host:

```
/opt/nfast/bin/enquiry  
/opt/nfast/bin/cardpp --check --cardset CBOM-Sensor-OCS  
/opt/nfast/bin/cardpp --auth --cardset CBOM-Sensor-OCS
```

Step 2: (Automated Deployments) Create a Softcard

For unattended sensor hosts, a softcard replaces physical card insertion:

```
/opt/nfast/bin/ppmk --new CBOM-Sensor-Softcard  
/opt/nfast/bin/nfkminfo --softcards  
# pre-load before starting the sensor:  
/opt/nfast/bin/preload --soft CBOM-Sensor-Softcard /opt/nfast/bin/enquiry
```

Step 3: Create a Minimal-Privilege Operator Credential

In CipherTools Manager → Manage Credentials → New Credential, create cbom-sensor-operator protected by the CBOM-Sensor-Softcard, granting only Enumerate and GetAttributeValue (never Decrypt, Sign, Unwrap, or Derive). Export the credential token to the sensor and restrict permissions:

```
cp /opt/nfast/kmdata/local/key_pkcs11_cbom-sensor-operator \
/etc/cbom/sensors/hsm/nshield/
chown cbom-service:cbom-service \
/etc/cbom/sensors/hsm/nshield/key_pkcs11_cbom-sensor-operator
chmod 600 /etc/cbom/sensors/hsm/nshield/key_pkcs11_cbom-sensor-operator
```

Step 4: Confirm the PKCS#11 Environment

```
export NFAST_PKCS11_LIB=/opt/nfast/toolkits/pkcs11/libcknfast.so
/opt/nfast/bin/cklist -L      # list slots / Security World label
/opt/nfast/bin/cklist -s 0    # list objects in slot 0
ls -lh /opt/nfast/toolkits/pkcs11/libcknfast.so
```

Step 5: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_HSM
  type: hsm
  vendor: entrust_nshield
  enabled: true
connection:
  pkcs11_library: /opt/nfast/toolkits/pkcs11/libcknfast.so
  slot_id: 0      # -1 to enumerate all slots
  token_label: "CipherTools Security World"
authentication:
  method: softcard
  softcard_name: CBOM-Sensor-Softcard
  passphrase_env: CBOM_NSCHILD_SOFTCARD_PASSPHRASE
discovery:
  enumerate_object_classes: [CKO_PRIVATE_KEY, CKO_PUBLIC_KEY, CKO_CERTIFICATE,
  CKO_SECRET_KEY]
  collect_attributes: [CKA_LABEL, CKA_KEY_TYPE, CKA_VALUE_LEN, CKA_ID, CKA_CLASS,
  CKA_TOKEN, CKA_SENSITIVE, CKA_EXTRACTABLE]
  read_only: true
  include_sensitive_flags: true
output:
  format: cbom_json
  destination: /var/cbom/output/nshield/
export CBOM_NSCHILD_SOFTCARD_PASSPHRASE="your-softcard-passphrase"
```

Step 6: Validate

```
cbom-sensor run --config /etc/cbom/sensors/hsm/nshield-sensor.yaml --dry-run
cbom-sensor run --config /etc/cbom/sensors/hsm/nshield-sensor.yaml
```

Confirm the library loads, the slot connects, softcard authentication succeeds, and objects are enumerated by class. Verify the output contains key metadata and no key values.

Common Errors

CKR_TOKEN_NOT_PRESENT

Cause: The Security World is not loaded, or slot_id does not match an active token.

Resolution: Check enquiry / nfkminfo, confirm port 9004 for network HSMs, and match slot_id to cklist -L.

CKR_USER_NOT_LOGGED_IN

Cause: The softcard/OCS was not loaded, or the passphrase variable is unset/incorrect.

Resolution: Verify the env var; test with ppmk --check; for OCS, ensure the card is loaded via preload.

libcknfast.so: cannot open shared object file

Cause: The nShield client is not installed, or installed to a non-default path.

Resolution: Verify /opt/nfast/toolkits/pkcs11/; reinstall the client or update pkcs11_library; ensure the cbom-service user can read/execute it.

Security Recommendations

- Grant the CipherTools credential only Enumerate and GetAttributeValue — never Decrypt/Sign/Unwrap/Derive.
- Store the softcard passphrase in a secrets manager and inject at runtime.
- Restrict the config, passphrase, and credential-token files to the cbom-service account at 600.
- Enable nShield audit logging for PKCS#11 sessions and object enumeration.
- Isolate the sensor host, limiting network access to the HSM port (9004) and the CBOM backend.

Conclusion

With an Operator Card Set or softcard, a minimal-privilege operator credential, and PKCS#11 connectivity, the Discover_HSM sensor provides full read-only visibility into keys, certificates, and tokens in the nShield Security World — feeding metadata into CBOM Secure for inventory, compliance, and risk analysis.