

Atos Trustway Proteccio NetHSM Setup

CBOM Secure · HSM Sensor (Discover_HSM)

Overview

This guide enables the CBOM Secure HSM Sensor to discover cryptographic assets in an Atos Trustway Proteccio NetHSM via the PKCS#11 interface (libnethsm.so), in read-only mode:

- Symmetric and asymmetric keys (RSA, EC, AES, 3DES) in virtual HSM slots
- X.509 certificates and associated key pairs
- Token and slot metadata (label, serial number, firmware version, mechanism support)

No keys are extracted, generated, or modified.

Prerequisites

- Trustway Administration Console access with the Security Officer (SO) role.
- The Proteccio NetHSM client software package (from Atos/Eviden).
- Network access from the sensor host to the appliance (default TCP 2348).
- A supported Linux distribution (RHEL 8+, Ubuntu 20.04+, or SLES 15+) with root/sudo.
- Proteccio firmware 4.x+ (PKCS#11 v2.40 support).
- The appliance IP/FQDN and the Security Officer PIN for the target virtual HSM.

Step-by-Step Guide

Step 1: Install the Proteccio Client

```
# RHEL/CentOS
sudo rpm -ivh proteccio-client-<version>.x86_64.rpm
# Ubuntu/Debian
sudo dpkg -i proteccio-client-<version>.amd64.deb

ls -lh /usr/lib/pkcs11/libnethsm.so
```

Configure the client daemon in /etc/proteccio/nethsm.conf:

```
[NetHSM]
HSM_IP = 192.168.10.50
HSM_PORT = 2348
TIMEOUT = 30
sudo systemctl enable proteccio-client
sudo systemctl start proteccio-client
sudo systemctl status proteccio-client
```

Step 2: Create a Dedicated Virtual HSM Slot

In the Trustway Administration Console (<https://<appliance>:8443/admin>), under Virtual HSMs → + New Virtual HSM, create a slot labelled CBOM_Discovery, set Max Sessions to 10, set the SO PIN, and Create. Then confirm visibility from the sensor host:

```
/usr/lib/pkcs11/tools/nethsm-tool --list-slots
# Note the Slot number (e.g. 0) and the CBOM_Discovery label
```

Step 3: Create a Read-Only Operator Credential

Under Virtual HSMs → CBOM_Discovery → Users → + Add User, create cbom_sensor_op with role Operator (CO) and set the PIN. Or via CLI:

```
/usr/lib/pkcs11/tools/nethsm-tool \
--slot 0 --init-user \
--so-pin <SO_PIN> --user-pin <OPERATOR_PIN>
```

Confirm read-only enumeration works:

```
/usr/lib/pkcs11/tools/nethsm-tool \
--slot 0 --user-pin <OPERATOR_PIN> --list-objects
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
- name: Discover_HSM
  type: hsm_pkcs11
  enabled: true
  description: "Atos Trustway Proteccio NetHSM - CBOM Discovery Slot"
  connection:
    library_path: /usr/lib/pkcs11/libnethsm.so
    slot: 0
    token_label: CBOM_Discovery
    hsm_host: 192.168.10.50
    hsm_port: 2348
  credentials:
    user_type: operator      # CKU_USER (Cryptographic Operator)
    pin: "${CBOM_HSM_PIN}"
  discovery:
    object_types: [keys, certificates, data_objects]
    include_sensitive_attributes: false
    session_type: read_only
  schedule:
    interval: 24h
  output:
    tags: { hsm_vendor: atos_trustway, hsm_model: proteccio_nethsm }
export CBOM_HSM_PIN="<OPERATOR_PIN>"
```

Step 5: Validate

```
cbom-sensor run --config /etc/cbom/sensors/atos-trustway.yaml --dry-run
```

Confirm output such as Objects found: 42 (18 keys, 12 certificates, 12 data objects), then run without --dry-run and verify assets appear under Assets → Sensor: Discover_HSM.

Common Errors

CKR_TOKEN_NOT_PRESENT

Cause: The client daemon cannot reach the appliance, or the slot number is wrong.

Resolution: Verify connectivity (telnet 192.168.10.50 2348), confirm proteccio-client is running, and re-check the slot index with --list-slots.

CKR_PIN_INCORRECT

Cause: The Operator PIN (or CBOM_HSM_PIN) does not match the initialized PIN.

Resolution: Reset the Operator PIN in the console (Reset PIN), update the variable, and retry.

CKR_LIBRARY_LOAD_FAILED / cannot open shared object file

Cause: The Proteccio client package is not installed, or the library is at a non-standard path.

Resolution: Install the client package and confirm /usr/lib/pkcs11/libnethsm.so; update library_path if it differs.

Security Recommendations

- Use a dedicated Operator account — never the Security Officer credential.
- Keep include_sensitive_attributes: false so the sensor never requests CKA_VALUE.
- Store the Operator PIN in a secrets manager; never hard-code or commit it.
- Restrict SSH access to the sensor host and monitor logins.
- Rotate the Operator PIN periodically and enable mutual TLS on the Proteccio client.

Conclusion

With the Proteccio client installed, a dedicated CBOM_Discovery slot, and a read-only Cryptographic Operator, the HSM Sensor enumerates cryptographic assets over PKCS#11 on a schedule — providing continuous visibility into key types, certificate lifetimes, and algorithm usage with no key material ever exposed.