OpenCryptoki (PKCS#11) Setup

CBOM Secure · HSM Sensor (Discover_HSM)

Overview

This guide configures OpenCryptoki so the CBOM Secure HSM Discovery Sensor can discover, read-only, over PKCS#11:

- PKCS#11 token slots and their attributes
- Key objects (symmetric, asymmetric) and associated metadata
- Certificate objects stored in token slots

The sensor connects with a user-level session and never extracts private key material - only metadata (type, size, label, key ID, usage flags).

Prerequisites

- A supported Linux distribution (Debian/Ubuntu or RHEL/CentOS/Rocky).
- sudo/root access on the host.
- The CBOM Collector installed on the host, or network access to the PKCS#11 socket.
- OpenCryptoki 3.17 or later recommended.

Step-by-Step Guide

Step 1: Install OpenCryptoki and Start the Daemon

```
sudo apt install -y opencryptoki      # or: sudo dnf install -y opencryptoki
sudo systemctl enable pkcsslotd && sudo systemctl start pkcsslotd
sudo systemctl status pkcsslotd
```

The main config is /etc/opencryptoki/opencryptoki.conf; a default install enables the software token (swtok). Add stdll entries for TPM/CCA/EP11 tokens per your hardware vendor.

Step 2: Create the Scan User and Grant pkcs11 Group Access

```
sudo useradd --system --no-create-home --shell /sbin/nologin cbom-scanner
sudo usermod -aG pkcs11 cbom-scanner       # OpenCryptoki restricts the socket to the pkcs11 group
groups cbom-scanner
sudo systemctl restart cbom-collector      # apply group change to the running service
```

Step 3: Initialize a Token Slot

```
pkcsconf -s                # list slots; note the target slot (e.g. 0)
sudo pkcsconf -I -c 0      # initialize the token; set SO-PIN and label (e.g. CBOM-SWTOK)
sudo pkcsconf -u -c 0      # set the User PIN (enter SO-PIN, then new User PIN)
pkcsconf -t -c 0           # verify TOKEN_INITIALIZED USER_PIN_INITIALIZED
```

Note Store both PINs in your credential vault. The sensor uses only the User PIN.

Step 4: Verify Slot Access with pkcs11-tool

```
sudo apt install -y opensc      # or: sudo dnf install -y opensc
pkcs11-tool --module /usr/lib/opencryptoki/libopencryptoki.so --list-slots
pkcs11-tool --module /usr/lib/opencryptoki/libopencryptoki.so \
  --slot 0 --login --pin <USER_PIN> --list-objects
```

If the library path differs, locate it with find /usr/lib -name libopencryptoki.so.

Step 5: Configure the CBOM Secure Sensor

```
pkcs11_library: "/usr/lib/opencryptoki/libopencryptoki.so"
slot: 0
user_pin: "<USER_PIN>"
token_label: "CBOM-SWTOK"
scan_name: Discover_HSM
```

token_label is an optional filter (blank scans all initialized slots). Duplicate the block per slot to scan multiple slots.

Step 6: Validate

```
# trigger the HSM discovery task from the CBOM dashboard, then:
journalctl -u cbom-collector --since "5 minutes ago" | grep -i pkcs11
```

Confirm the task completes with no CKR_PIN_INCORRECT or CKR_USER_NOT_LOGGED_IN errors and that key metadata objects appear in the CBOM inventory.

Common Errors

CKR_TOKEN_NOT_PRESENT

Cause: pkcsslotd is not running, or the slot number does not match an initialized slot.

Resolution: Start pkcsslotd, re-run pkcsconf -s, and update the slot field.

CKR_PIN_INCORRECT

Cause: The User PIN in the config is wrong.

Resolution: Reset it with pkcsconf -u -c <slot> using the SO-PIN and update the config.

CKR_USER_NOT_LOGGED_IN

Cause: Login failed, or cbom-scanner is not in the pkcs11 group.

Resolution: Confirm groups cbom-scanner and restart the Collector after adding the group.

Cannot open library libopencryptoki.so

Cause: OpenCryptoki is not installed or the library is at a different path.

Resolution: Install the package and update pkcs11_library to the path from find /usr/lib -name libopencryptoki.so.

Security Recommendations

- Store the User PIN in the CBOM credential vault (ECNE:{Base64}) - never plaintext YAML.
- Use a dedicated token slot for CBOM scanning; do not share slots with application workloads.
- Restrict opencryptoki.conf to root and the pkcs11 group (chmod 640).
- Never grant cbom-scanner SO-PIN access - a read-only user session is sufficient.
- Rotate the User PIN quarterly and audit token sessions with pkcsconf.

Conclusion

The HSM Discovery Sensor operates with a least-privilege, user-level PKCS#11 session over OpenCryptoki - enumerating slots and object attribute metadata read-only across software, TPM, CCA, and EP11 tokens, with no private key material ever extracted.