

Yubico YubiKey (PIV) Setup

CBOM Secure · HSM Sensor (Discover_HSM, PKCS#11 mode)

Overview

This guide configures a Yubico YubiKey (PIV / PKCS#11) as a cryptographic asset source for the CBOM Secure Discover_HSM sensor in PKCS#11 mode. The sensor connects read-only and discovers material stored in PIV slots:

- X.509 certificates in PIV slots (authentication, digital signature, key management, card authentication)
- RSA and EC public keys associated with on-device private keys
- PIV slot metadata: slot IDs, key algorithm, key size, and certificate subject/issuer/validity

Covered PIV slots: 9a (Authentication), 9c (Digital Signature), 9d (Key Management), 9e (Card Authentication), and 82-95 (retired key management). The sensor never reads private key material - both YKCS11 and ykman expose only public objects without a PIN when listing certificates.

Prerequisites

- A YubiKey 5 series (or later) with the PIV applet enabled, connected to the sensor host (or via USB passthrough).
- Linux (x86_64) or macOS host; Python 3.8+.
- opensc installed (provides pkcs11-tool).
- The Yubico YKCS11 library present (Linux: /usr/lib/x86_64-linux-gnu/libykcs11.so; macOS: /usr/local/lib/libykcs11.dylib).
- The sensor's OS account has read access to the USB HID/CCID device (Linux: plugdev group or a udev rule).
- At least one PIV slot contains a certificate.

Step-by-Step Guide

Step 1: Install YubiKey Manager (ykman) and Confirm the Device

```
python3 -m venv /opt/cbom/venv && source /opt/cbom/venv/bin/activate
pip install yubikey-manager && ykman --version
ykman list                # expect: YubiKey 5 ... Serial: 12345678
sudo systemctl enable --now pcscd # if no device is listed (Linux)
ykman info                # confirm: PIV Enabled
```

Step 2: Enumerate PIV Slots and Inspect a Certificate

```
ykman piv info            # lists populated slots, algorithm, subject, validity
ykman piv certificates export 9a /tmp/yubikey_9a_cert.pem
openssl x509 -in /tmp/yubikey_9a_cert.pem -text -noout && rm /tmp/yubikey_9a_cert.pem
```

Only slots containing certificates appear in discovery output - note which slots are populated.

Step 3: Verify PKCS#11 Library Access

```
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/libykcs11.so --list-objects
# macOS: --module /usr/local/lib/libykcs11.dylib
ls -la /usr/lib/x86_64-linux-gnu/libykcs11.so # record the confirmed path
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
- name: Discover_HSM
  enabled: true
  mode: pkcs11
  description: "YubiKey PIV / PKCS#11 identity token sensor"
  targets:
  - id: yubikey-primary
    label: "YubiKey 5 NFC - Serial 12345678"
    vendor: Yubico
    device_type: smart_card
    serial: "12345678"
    pkcs11:
      library: /usr/lib/x86_64-linux-gnu/libykcs11.so
      slot_index: 0
      pin_required: false # listing certs/public keys needs no PIN
    piv_slots:
      - { slot: "9a", label: Authentication, enabled: true }
      - { slot: "9c", label: Digital Signature, enabled: true }
      - { slot: "9d", label: Key Management, enabled: true }
      - { slot: "9e", label: Card Authentication, enabled: true }
    discovery:
      include_certificates: true
      include_public_keys: true
      include_private_key_metadata: false # private keys are not exportable
    schedule:
      interval_minutes: 60
```

Step 5: Validate

```
sudo systemctl restart cbom-sensor
sudo journalctl -u cbom-sensor -f # look for 'Discovery complete. N object(s) recorded'
cbom-sensor run --sensor Discover_HSM --target yubikey-primary --dry-run
```

Confirm the output lists at least one certificate with subject, issuer, serial, and expiry populated, and that assets appear in the inventory under Discover_HSM.

Common Errors

Cannot open library libykcs11.so

Cause: The YKCS11 library is not installed, or the configured path is wrong.

Resolution: Install libykcs11 (Linux) or yubico-piv-tool (macOS), locate with `find /usr /lib /opt -name 'libykcs11*'`, update the library path, and restart.

No token present / device not detected

Cause: The YubiKey is not inserted, CCID is disabled, or pcscd is not running.

Resolution: Confirm ykman list, start pcscd, enable CCID (ykman config usb --enable CCID), and add the sensor account to plugdev.

Slot is empty - no certificate discovered

Cause: The configured PIV slots hold no certificates (freshly provisioned or cleared).

Resolution: Run ykman piv info to see populated slots and limit piv_slots to those; provision certificates with ykman piv certificates import if needed.

Security Recommendations

- Restrict physical access to YubiKey devices and the sensor host.
- Run the sensor as a dedicated low-privilege account (plugdev only), never root.
- Do not configure a PIV PIN - certificate/public-key enumeration needs none; store any PIN in a secrets manager if ever required.
- Audit PIV PIN retry counters (ykman piv info) for unexpected decrements.
- Alert on certificates in slots 9a-9e expiring within 90 days to drive timely renewal.

Conclusion

With ykman confirming device readiness and the YKCS11 PKCS#11 library wired into Discover_HSM, the sensor enumerates X.509 certificates and public keys across YubiKey PIV slots entirely read-only - no PIN, no private key material - keeping managed YubiKeys in the CBOM Secure inventory for lifecycle and compliance tracking.