Feitian ePass Setup

CBOM Secure · HSM Sensor (PKCS#11 mode)

Overview

This guide configures the CBOM Secure Discover_HSM sensor (PKCS#11 mode) to connect to Feitian ePass hardware tokens (ePass2003, ePass3000, FIDO2). It discovers, read-only and without a PIN:

- X.509 certificates — end-entity and intermediate certificates on token slots
- RSA and EC public keys — asymmetric public key objects
- Key metadata — type, size, label, ID, and certificate linkage
- Slot and token inventory — manufacturer, firmware version, slot count, flags

Private key objects are skipped during discovery; no PIN is required and no private-key operations are performed.

Prerequisites

- A Linux host (Ubuntu 20.04+ or RHEL 8+) with the CBOM sensor agent installed.
- One or more Feitian ePass tokens connected via USB or a smart card reader.
- The Feitian ePass middleware installed (provides the PKCS#11 library).
- The PKCS#11 library present (/usr/lib/libePass2003.so, or /usr/lib/libgtop11dotnet.so).
- The opensc and pcsc-lite packages installed for PCSC daemon support.
- The sensor user has access to USB device nodes via pcscd (no root at runtime).

Step-by-Step Guide

Step 1: Install PC/SC and Feitian Middleware

```
sudo apt-get update
sudo apt-get install -y pcscd pcsc-tools opensc libpcsclite-dev
sudo systemctl enable pcscd && sudo systemctl start pcscd


# install the Feitian PKCS#11 middleware package:
sudo dpkg -i ePass2003-pkcs11-linux-x86_64.deb
ls -lh /usr/lib/libePass2003.so
```

Step 2: Verify Token Detection

Insert the token and list slots and public objects (no PIN required):

```
pkcs11-tool --module /usr/lib/libePass2003.so --list-slots
pkcs11-tool --module /usr/lib/libePass2003.so --list-objects
# inspect a certificate object:
pkcs11-tool --module /usr/lib/libePass2003.so --read-object --type cert --id 01 \
  | openssl x509 -inform DER -text -noout
```

Note the slot number and token label for the sensor configuration.

Step 3: Configure Host Permissions

```
id cbom-agent
sudo usermod -aG pcscd cbom-agent
sudo systemctl restart cbom-agent
```

Step 4: Configure the CBOM Secure Sensor

```
sensors:
  - name: feitian-epass-pkcs11
    type: Discover_HSM
    mode: pkcs11
    enabled: true
    pkcs11:
      library_path: /usr/lib/libePass2003.so
      slot_id: 0
      token_label: "MyTokenLabel"
      user_pin: ""                # leave blank — public objects only
      discover_objects: [certificates, public_keys]
      skip_private_keys: true
    schedule:
      interval: 6h
    output:
      endpoint: https://cbom.example.internal/api/v1/ingest
      tls_verify: true
    tags: { token_vendor: feitian, token_model: ePass2003 }
sudo systemctl reload cbom-agent
```

Step 5: Validate

```
cbom-agent discover --sensor feitian-epass-pkcs11 --verbose
sudo journalctl -u cbom-agent -f | grep feitian-epass-pkcs11
```

Confirm the slot connects and certificates/public keys are discovered. The asset list for this sensor should contain only Certificate and PublicKey object types — no private keys.

Common Errors

PKCS#11 library not found

Cause: The Feitian middleware is not installed, or the library is at a non-standard path.

Resolution: Locate it (find /usr /lib /opt -name libePass2003.so) and update library_path, or reinstall the middleware.

No slots available / token not detected

Cause: pcscd is not running, the token is not connected, or a driver is missing.

Resolution: Restart pcscd, confirm with lsusb | grep -i feitian, try another USB port, and re-run --list-slots.

CKR_TOKEN_NOT_RECOGNIZED

Cause: The token model needs a different library (e.g. ePass3000 → libgtop11dotnet.so), or the token is locked.

Resolution: Try the alternative library path and update library_path; unlock the token with the SO PIN if locked.

Security Recommendations

- Never configure a User PIN in the sensor YAML — only public objects are needed.
- Restrict the sensor config to 0600, owned by cbom-agent, to protect the API key.
- Enable TLS verification (tls_verify: true) for all platform connections.
- Physically secure the token host and audit pcscd group membership.
- Rotate the CBOM API key on schedule and store it in a secrets manager where possible.

Conclusion

In PKCS#11 mode the Discover_HSM sensor provides continuous, read-only visibility into certificates and public keys on Feitian ePass tokens — covering PKI and identity-token infrastructure without ever touching private-key material — and submits discovered assets to CBOM Secure on schedule.