IBM Crypto Express (CEX) Setup

CBOM Secure · HSM Sensor (PKCS#11 / EP11)

Overview

This guide configures an IBM Crypto Express (CEX) adapter in EP11 mode so the CBOM Secure HSM Sensor can discover cryptographic material over the EP11 PKCS#11 library on IBM Z (s390x):

- EP11 symmetric and asymmetric keys managed by the Crypto Express card
- PKCS#11 token objects: private keys, public keys, secret keys, and X.509 certificates
- Key metadata: label, key type, size, CKA_ID, CKA_EXTRACTABLE, CKA_SENSITIVE, and slot assignment

Prerequisites

- Administrator access to the IBM Hardware Management Console (HMC) for the IBM Z / LinuxONE system.
- A CEX adapter (CEX7S, CEX8S, or later) installed and recognized.
- SSH access to the LPAR / z/VM guest that will run the sensor.
- opencryptoki (3.19+), the EP11 host library, and the pkcsep11 slot plug-in installed on the LPAR.
- The Security Administrator role in the HMC.

Step-by-Step Guide

Step 1: Set the Adapter to EP11 Mode and Assign a Domain

In the HMC, open the IBM Z system → Crypto tab, set the CEX adapter to EP11 Coprocessor, and Apply. Assign the adapter domain to the target LPAR (Partitions → LPAR → Crypto → Add Crypto Adapter), choosing a Usage domain (e.g. domain 0). CLI alternative on the Support Element:

```
chzcrypt -e EP11 -a 04
lszcrypt        # verify adapter/domain visible to the LPAR
```

Step 2: Install and Start opencryptoki

```
sudo dnf install -y opencryptoki opencryptoki-ep11tok   # or apt: opencryptoki pkcsep11
sudo usermod -aG pkcs11 cbom-sensor
sudo systemctl enable pkcsslotd && sudo systemctl start pkcsslotd
```

Step 3: Configure and Initialize the EP11 Token

Set the assigned adapter/domain in the EP11 token config, then restart the slot manager and initialize the token:

```
# /etc/opencryptoki/ep11tok.conf
APQN_WHITELIST 04.0000        # adapter 4, domain 0
```

```
sudo systemctl restart pkcsslotd
pkcsconf -i                 # confirm slot 0 and token label
pkcsconf -I -c 0 -S           # initialize token, set SO PIN, set label CBOM_EP11_SLOT0
```

Step 4: Create a Read-Only Crypto User (CKU_USER)

```
pkcsconf -P -c 0 -S    # set the User PIN (the sensor credential)
pkcsconf -t -c 0 -u    # verify read-only session and object enumeration
```

Step 5: Confirm the Library Path and Slot

```
ls -l /usr/lib/s390x-linux-gnu/pkcs11/PKCS11_API.so
pkcsconf -i            # note the Slot # for the EP11 token
```

Step 6: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_HSM
  type: pkcs11
connection:
  library_path: /usr/lib/s390x-linux-gnu/pkcs11/PKCS11_API.so
  slot: 0
  token_label: CBOM_EP11_SLOT0
  user_pin: "<CRYPTO_USER_PIN>"
  user_type: CKU_USER
discovery:
  include_object_types: [CKO_PRIVATE_KEY, CKO_PUBLIC_KEY, CKO_SECRET_KEY,
CKO_CERTIFICATE]
  include_attributes: [CKA_LABEL, CKA_KEY_TYPE, CKA_VALUE_LEN, CKA_ID,
CKA_EXTRACTABLE, CKA_SENSITIVE, CKA_TOKEN]
  read_only: true
output:
  collector_url: https://<cbom-collector-host>:5001/collector/collect
  scan_name: IBM_CEX_EP11_Discovery
```

Step 7: Validate

Run the CBOM HSM discovery task and confirm a success status with no auth errors. Verify discovered objects appear in the CryptoMaterial inventory with the correct token label, object types, and metadata (CKA_LABEL, CKA_KEY_TYPE, CKA_EXTRACTABLE). On the LPAR, confirm the session with pkcsconf -t -c 0.

Common Errors

CKR_TOKEN_NOT_PRESENT

Cause: pkcsslotd is not running, or the EP11 domain is not visible to the LPAR.

Resolution: Run lszcrypt to confirm adapter/domain, restart pkcsslotd, and re-check pkcsconf -i.

CKR_PIN_INCORRECT

Cause: The User PIN does not match, or the PIN is locked after failed attempts.

Resolution: Verify with pkcsconf -t -c 0 -u; reset via the SO PIN (pkcsconf -P -c 0 -S) and update the YAML.

dlopen PKCS11_API.so: No such file

Cause: The EP11 host library is missing, or the sensor runs on x86 rather than s390x.

Resolution: Confirm uname -m is s390x, install the EP11 host library, and verify the library path.

Security Recommendations

- Use only CKU_USER for the sensor — never the Security Officer PIN.
- Store the Crypto User PIN in a secrets manager rather than plaintext YAML.
- Assign only the specific EP11 domain indices the sensor needs.
- Access the PKCS#11 library via the local adapter, not a network proxy.
- Enable CEX adapter audit logging and verify the PKCS11_API.so checksum after updates.

Conclusion

With the CEX adapter in EP11 mode, a domain assigned to the LPAR, and a read-only Crypto User, the HSM Sensor discovers IBM Crypto Express key material over the EP11 PKCS#11 library — capturing type, size, label, and sensitivity attributes with no ability to modify objects.