

Utimaco SecurityServer (CryptoServer) Setup

CBOM Secure · HSM Sensor (Discover_HSM)

Overview

This guide configures the Utimaco SecurityServer (CryptoServer) HSM for the CBOM Secure Discover_HSM sensor, which connects over PKCS#11 and discovers cryptographic material read-only:

- Symmetric keys (AES, 3DES, HMAC)
- Asymmetric key pairs (RSA, ECC, DSA)
- X.509 certificates stored on the HSM
- Key attributes: algorithm, key length, usage flags, label, CKA_ID, and expiry

Prerequisites

- Utimaco SecurityServer (CryptoServer) installed, initialized, and network-reachable.
- Access to the SSCA GUI or the csadm CLI with administrator privileges.
- The CryptoServer software on the sensor host providing the PKCS#11 library (/opt/utimaco/lib/libcs_pkcs11_R2.so), p11tool2, and csadm.
- At least one initialized partition (slot/token).
- Network reachability to the device (default TCP 3001, or 2345 for the simulator).
- The PKCS#11 config file cs_pkcs11_R2.cfg on the sensor host.

Step-by-Step Guide

Step 1: Create a Read-Only CryptoServer User

Create a dedicated cbom-readonly account via the Admin Console (<https://<host>:2223> > User Management) or CLI:

```
csadm Dev=<host>:3001 AddUser User=cbom-readonly AuthMethod=Password  
Password=<strong-password>  
csadm Dev=<host>:3001 AssignRole User=cbom-readonly Role=CS_ADMIN \  
Permissions=KEY_LIST,CERT_READ,OBJECT_READ
```

Assign the CS_ADMIN role at read-only scope. Do NOT grant KEY_GENERATE, KEY_DELETE, KEY_IMPORT, or KEY_EXPORT. Optionally restrict the user to specific slots:

```
csadm Dev=<host>:3001 SetSlotUser Slot=0 User=cbom-readonly Access=Read
```

Step 2: Configure the PKCS#11 Client on the Sensor Host

```
ls -l /opt/utimaco/lib/libcs_pkcs11_R2.so      # confirm the library exists
```

Create /etc/utimaco/cs_pkcs11_R2.cfg and export the config path:

```
# /etc/utimaco/cs_pkcs11_R2.cfg
```

```
[Global]
Logpath = /var/log/utimaco/
Logging = 0
[CryptoServer]
Device = 3001@<cryptoserver-host>
Timeout = 10000

export CS_PKCS11_R2_CFG=/etc/utimaco/cs_pkcs11_R2.cfg
```

Step 3: Verify Slot Visibility with p11tool2

```
p11tool2 Module=/opt/utimaco/lib/libcs_pkcs11_R2.so ListSlots
p11tool2 Module=/opt/utimaco/lib/libcs_pkcs11_R2.so Slot=0 \
  UserPIN=<strong-password> ListObjects
```

Confirm key labels, types, and attributes are returned without error.

Step 4: Configure the CBOM Secure Sensor

```
sensors:
- name: Discover_HSM
  type: pkcs11_hsm
  enabled: true
  description: "Utimaco SecurityServer CryptoServer HSM - Production"
  connection:
    pkcs11_library: /opt/utimaco/lib/libcs_pkcs11_R2.so
    config_file: /etc/utimaco/cs_pkcs11_R2.cfg
    device: "3001@cryptoserver.prod.example.com"
    slot: 0
  auth:
    user_type: user          # CKU_USER (read-only)
    username: cbom-readonly
    pin_secret_ref: "vault://secret/cbom/utimaco/pin"
  discovery:
    include_object_types: [CKO_PRIVATE_KEY, CKO_PUBLIC_KEY, CKO_SECRET_KEY,
      CKO_CERTIFICATE]
    collect_attributes: [CKA_LABEL, CKA_ID, CKA_KEY_TYPE, CKA_KEY_BITS,
      CKA_SIGN, CKA_VERIFY, CKA_EXTRACTABLE, CKA_SENSITIVE, CKA_START_DATE,
      CKA_END_DATE]
    skip_sensitive_attributes: true # never extract key material
  schedule:
    interval hours: 24
```

Step 5: Validate

```
cbom-sensor validate --config cbom-sensors.yaml --sensor Discover_HSM
cbom-sensor run --config cbom-sensors.yaml --sensor Discover_HSM --output ./cbom-
output.json
```

A successful validate authenticates as CKU_USER (cbom-readonly), opens the slot, and reports the discovered object counts with no errors.

Common Errors

CKR_TOKEN_NOT_PRESENT on slot open

Cause: The slot value does not match an initialized token, or the device is unreachable.

Resolution: Confirm the slot index with p11tool2 ListSlots, verify the device address in cs_pkcs11_R2.cfg, and open TCP 3001.

CKR_PIN_INCORRECT on login

Cause: The PIN for cbom-readonly is wrong or the account is locked.

Resolution: Confirm the secret at the pin_secret_ref, check the account is not locked, and reset with csadm SetUserPIN if needed.

CS_PKCS11_R2_CFG not found / C_Initialize CKR_GENERAL_ERROR

Cause: The library cannot find its config because CS_PKCS11_R2_CFG is not set for the service process.

Resolution: Confirm echo \$CS_PKCS11_R2_CFG, add Environment=CS_PKCS11_R2_CFG=... to the systemd unit, and restart the service.

Security Recommendations

- Use a dedicated read-only account - never the Security Officer or a key-generation account.
- Store the CryptoServer PIN in a secrets manager via pin_secret_ref, not plaintext YAML.
- Restrict cs_pkcs11_R2.cfg to the sensor OS user (chmod 640, chown cbom-svc).
- Limit the user to only the slots that need inventorying.
- Enable CryptoServer audit logging, rotate the PIN every 90 days, and keep skip_sensitive_attributes: true.

Conclusion

The cbom-readonly account, scoped to CS_ADMIN read-only permissions, lets the Discover_HSM sensor enumerate all key objects, certificates, and metadata across the configured CryptoServer slot with no risk of key exposure or modification - giving CBOM Secure continuous, least-privilege visibility into your Utimaco HSM estate.