Trustica Cryptoucan Setup

CBOM Secure · OpenPGP Sensor (Discover_PGP)

Overview

This guide configures the CBOM Secure Discover_PGP sensor to discover cryptographic assets managed by a Trustica Cryptoucan OpenPGP smart card. The Cryptoucan implements the OpenPGP card standard - private keys are generated and held on-device and are never extractable - while GnuPG keeps public key stubs in the local keyring. The sensor reads the keyring read-only and discovers:

- The primary OpenPGP key and its sign/encrypt/authenticate subkeys
- Algorithm and key size for each key slot
- Key creation and expiry dates
- Key fingerprints and long key IDs
- Card serial-number association (via the GnuPG trust database, where available)

Prerequisites

- A Trustica Cryptoucan connected via USB.
- GnuPG 2.2 or later installed on the sensor host.
- pcscd (PC/SC daemon) or scdaemon running and able to reach the reader.
- Functional gpg-agent and scdaemon.
- The Cryptoucan initialized with at least one populated key slot.
- A public-key URL on the card, or the public key imported manually into the keyring.
- The CBOM sensor installed on the host with read access to the target GnuPG home (~/.gnupg by default).

Step-by-Step Guide

Step 1: Verify Cryptoucan Detection

```
sudo systemctl status pcscd        # start + enable if not running
gpg --card-status                  # expect serial number + key attributes
```

If the card is not detected, reset scdaemon and confirm the USB device:

```
gpgconf --kill scdaemon && gpg --card-status
lsusb | grep -i trustica
```

Step 2: Import the Card Public Key into the Keyring

Fetch from the URL stored on the card:

```
gpg --edit-card
```

```
gpg/card> fetch
gpg/card> quit
```

If no URL is stored, import the public key file out-of-band:

```
gpg --import /path/to/jane-public-key.asc
```

Step 3: Verify Key Stubs

```
gpg --list-keys --with-fingerprint          # primary + subkeys, algorithms, capabilities
gpg --list-secret-keys --with-fingerprint    # sec>/ssb> and 'Card serial no.' = on-card stub
```

The > after sec and ssb confirms the private key resides on the card, not on disk.

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_PGP
  enabled: true
  description: "OpenPGP keys via GnuPG, including Cryptoucan card stubs"
connection:
  gpg_home_dir: "/home/jane/.gnupg"
  gpg_binary: "/usr/bin/gpg"
  gpg_version: "2"
discovery:
  include_expired_keys: false
  include_revoked_keys: false
  include_subkeys: true
  key_uid_filter: ""
output:
  cbom_endpoint: "https://cbom.example.com/api/v1/ingest"
  api_key: "${CBOM_API_KEY}"
schedule:
  interval_minutes: 60
```

gpg_home_dir must point to the keyring holding the Cryptoucan stubs, readable by the sensor's OS user.

Step 5: Validate

```
cbom-sensor run --config /etc/cbom/discover_pgp.yaml --dry-run
cbom-sensor run --config /etc/cbom/discover_pgp.yaml
```

The dry run lists the primary key and subkeys with algorithms and creation dates. Confirm fingerprints and expiry in the CBOM inventory, and verify no private key material appears in any record.

Common Errors

gpg: error reading key: No public key

Cause: The public key has not been imported into the keyring.

Resolution: Confirm gpg --card-status, then fetch via gpg --edit-card, or import the .asc manually; re-run after verifying with gpg --list-keys.

GPG home directory not found

Cause: gpg_home_dir points to a missing or inaccessible path for the sensor's OS user.

Resolution: Confirm the directory exists, grant read/execute (chmod o+rx ~/.gnupg, o+r pubring.kbx), and correct the path.

scdaemon: card reader not available

Cause: The card is unplugged or another process holds the reader lock.

Resolution: Confirm lsusb, run gpgconf --kill scdaemon, restart pcscd; note the card need not remain plugged in for scheduled runs once stubs are imported.

Security Recommendations

- Grant the sensor service account read-only access to the GnuPG home - never write.
- Run the sensor as a dedicated low-privilege user, not root or the keyring owner.
- Store the CBOM API key in a secrets manager / environment variable, not the YAML.
- Rotate the CBOM API key on a schedule and update the sensor config.
- Keep GnuPG and Cryptoucan firmware patched for scdaemon compatibility and security fixes.

Conclusion

Once the Cryptoucan public-key stubs are imported and the sensor is pointed at the correct GnuPG home, the Discover_PGP sensor inventories primary keys, subkeys, algorithms, sizes, and expiry dates on schedule - without ever accessing or transmitting private key material - keeping Cryptoucan-managed keys visible in your cryptographic posture.