Nitrokey Pro / Start / Storage Setup

CBOM Secure · PGP Sensor (Discover_PGP)

Overview

This guide configures the CBOM Secure Discover_PGP sensor to discover cryptographic assets on Nitrokey Pro, Start, or Storage devices. These implement the OpenPGP card standard; private keys reside on the device and are never exportable, while GnuPG stores public key stubs in the local keyring. The sensor reads those stubs read-only:

- OpenPGP public key stubs cached in the GnuPG keyring (~/.gnupg or a custom GNUPGHOME)
- Key metadata: key ID, fingerprint, algorithm, key length, creation/expiry dates, user IDs
- Subkey entries for signing, encryption, and authentication slots
- (Nitrokey HSM / PKCS#11 mode only) certificates, public keys, and private-key handles via opensc-pkcs11.so

Prerequisites

- A supported Nitrokey (Pro 2, Start, or Storage) connected via USB.
- GnuPG 2.2 or later on the sensor host, with the scdaemon component present.
- The PC/SC daemon (pcscd) running.
- For Nitrokey HSM (PKCS#11) mode only: opensc and opensc-pkcs11 installed.
- The CBOM agent installed and reachable; read access to the GnuPG home directory.
- No PIN lock-out condition on the device.

Step-by-Step Guide

Step 1: Verify Device Detection

```
systemctl status pcscd      # start with: sudo systemctl enable --now pcscd
gpg --card-status           # confirm Reader / Application ID / Nitrokey serial
```

Step 2: Confirm Keyring Stub Entries

Card-backed keys appear with a > prefix on the sec/ssb line, indicating the private key resides on the hardware. If no stubs are present, gpg --card-status creates them automatically:

```
gpg --list-keys
gpg --list-secret-keys     # look for sec> / ssb> (key on card)
```

Step 3: (HSM Mode Only) Enumerate PKCS#11 Objects

Applies only when the device is used as a Nitrokey HSM with PKCS#11 access; skip for standard OpenPGP card mode.

```
ls -l /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so    # RHEL: /usr/lib64/opensc-pkcs11.so
```

```
pkcs11-tool --module /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so --list-objects
```

Step 4: Configure the CBOM Secure Sensor

```
sensor:
  name: Discover_PGP
  enabled: true
  pgp:
    gpg_home: "/home/cbom-agent/.gnupg"
    gpg_binary: "/usr/bin/gpg"
    list_secret_stubs: true
    list_public_keys: true
    include_subkeys: true
    include_expired: false
  device:
    vendor: "Nitrokey"
    model: "Pro 2"            # Pro 2 | Start | Storage | HSM 2
    serial_number: "00000XXX"  # from gpg --card-status
  pkcs11:
    enabled: false            # true only for Nitrokey HSM mode
    module_path: "/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so"
    slot: 0
    list_private_key_handles: true   # handles only; key material never read
  output:
    format: "json"
    cbom_server_url: "https://cbom.example.com/api/v1/ingest"
    api_key: "${CBOM_API_KEY}"
  schedule:
    interval_minutes: 60
```

Save at /etc/cbom/sensors/nitrokey-pgp.yaml and reload the agent. Inject CBOM_API_KEY via env/secrets manager.

Step 5: Validate

```
cbom-cli sensor run --name Discover_PGP --config /etc/cbom/sensors/nitrokey-pgp.yaml --dry-run
gpg --fingerprint --with-colons      # cross-reference fpr fields against the scan
```

Confirm the scan reports key fingerprints, algorithms, and expiry dates matching the GnuPG stubs, tagged with the Nitrokey serial as the source. Confirm no private key material appears (private_key_exported: false on all entries).

Common Errors

gpg: selecting card failed: No such device

Cause: pcscd is not running, or the device is not detected by USB.

Resolution: Confirm lsusb | grep -i nitrokey, start pcscd, restart the agent (gpgconf --kill gpg-agent), and pass the USB device through if in a VM.

pkcs11-tool: PKCS#11 module load failed

Cause: The opensc-pkcs11.so path is wrong or OpenSC is not installed.

Resolution: find /usr/lib -name opensc-pkcs11.so, update module_path, and install opensc if missing.

scdaemon is older than us

Cause: A version mismatch between gpg and scdaemon from a partial upgrade.

Resolution: Upgrade gnupg2 and scdaemon together, kill the agent (gpgconf --kill gpg-agent), and re-run gpg --card-status.

Security Recommendations

- Run the sensor as a dedicated low-privilege account with read-only access to the GnuPG home.
- Never store device PINs in the config - the PGP sensor reads public stubs and metadata only.
- Restrict the GnuPG home directory (chmod 700) to the owning user and the sensor account.
- Rotate CBOM_API_KEY periodically and inject it via env/secrets manager.
- Audit Nitrokey PIN retry counters via gpg --card-status to detect unauthorized attempts.

Conclusion

The Discover_PGP sensor provides passive, read-only discovery of OpenPGP key stubs (and optional PKCS#11 objects) anchored to Nitrokey devices - without exposing or exporting private key material - giving CBOM Secure continuous visibility into hardware-token key expiry, algorithms, and lifecycle.