strongSwan - Issue #3460

p11kit with NSS soft token unusable

22.05.2020 17:04 - Yuri B

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	libstrongswan		
Affected version:	5.8.4	**Resolution:**	No feedback

Description

You'll have to try reproducing this locally, it should be easy.

You'd usually use softhsm to test the pkcs11 stuff, but someone might realize that there's no need to install extra software when your distro (fedora) already bundles NSS, which in fact provides a pkcs11 interface to NSS software token (firefox is/was actively using that to store their certs).

So you go to https://p11-glue.github.io/p11-glue/p11-kit/manual/config-example.html , bottom module example, and decide to use that.

```
[root@test ~]# cat /etc/pkcs11/modules/nss.module
# Load the NSS libsoftokn.so.3 PKCS#11 library as a module. Note that we pass some custom non-stan
dard initialization arguments, as NSS expects.
module: /usr/lib64/libsoftokn3.so

x-init-reserved: configdir='sql:/var/lib/nss' certPrefix='' keyPrefix='' secmod=secmod.db flags= u
pdatedir='' updateCertPrefix='' updateKeyPrefix='' updateid='' updateTokenDescription=''
critical: yes

[root@test ~]# pkcs11-dump slotlist  /lib64/libp11-kit.so.0

16 NSS Internal Cryptographic Services
17 NSS User Private Key and Certificate Services

[root@test ~]# p11-kit list-modules
p11-kit-trust: p11-kit-trust.so
    library-description: PKCS#11 Kit Trust Module
    library-manufacturer: PKCS#11 Kit
    library-version: 0.23
    token: System Trust
        manufacturer: PKCS#11 Kit
        model: p11-kit-trust
        serial-number: 1
        hardware-version: 0.23
        flags:
               token-initialized
    token: Default Trust
        manufacturer: PKCS#11 Kit
        model: p11-kit-trust
        serial-number: 1
        hardware-version: 0.23
        flags:
               write-protected
               token-initialized
nss: /usr/lib64/libsoftokn3.so
    library-description: NSS Internal Crypto Services
    library-manufacturer: Mozilla Foundation
    library-version: 3.51
    token: NSS Generic Crypto Services
        manufacturer: Mozilla Foundation
        model: NSS 3
        serial-number: 0000000000000000
        hardware-version: 4.0
```

```
        flags:
               rng
               write-protected
               dual-crypto-operations
               token-initialized
    token: NSS Certificate DB
        manufacturer: Mozilla Foundation
        model: NSS 3
        serial-number: 0000000000000000
        flags:
               rng
               login-required
               user-pin-initialized
               dual-crypto-operations
               token-initialized
[root@test ~]#
```

p11-kit-trust.so is not shown in pkcs11-dump, I don't know why. I also don't know why slot 17 with "NSS User Private Key and Certificate Services" is not visible in p11-kit list-modules .
All certs imported with NSS's certutil -d sql:/var/lib/nss -A -a -i cert.pem -t P,P,P end up in "NSS Certificate DB" token.

And here's the error that prevents it from working and sourcing the certs:

```
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG] loaded PKCS#11 v2.40 library 'p11kit' (/usr/l
ib64/p11-kit-proxy.so)
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG]   PKCS#11 Kit: PKCS#11 Kit Proxy Module v1.1
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG]   found token in slot 'p11kit':16 (NSS Intern
al Cryptographic Services)
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG]     NSS Generic Crypto Services (Mozilla Foun
dation: NSS 3)
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG]   found token in slot 'p11kit':17 (NSS User P
rivate Key and Certificate Services)
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG]     NSS Certificate DB (Mozilla Foundation: N
SS 3)
May 21 09:29:22 test.local charon-nm[13013]: 00[LIB] openssl FIPS mode(2) - enabled
May 21 09:29:22 test.local charon-nm[13013]: 00[CFG] C_GetAttributeValue(NULL) error: ATTRIBUTE_TY
PE_INVALID
May 21 09:29:22 test.local charon-nm[13013]: 00[LIB] loaded plugins: nm-backend charon-nm pkcs11 t
pm aesni aes des rc2 sha2 sha1 md4 md5 mgf1 random nonce x509 revocation constraints pkcs1 pkcs7 p
kcs8 sshkey pem openssl gcrypt fips-prf >
May 21 09:29:22 test.local charon-nm[13013]: 00[JOB] spawning 16 worker threads
May 21 09:29:22 test.local charon-nm[13013]: 02[CFG] module 'p11kit' does not support hot-plugging
, cancelled
```

if debugging (default = 3) is enabled, this is happening around:

```
00[LIB]         loop detected while loading CERT_DECODE:X509 in plugin 'pem'
00[LIB]         loading feature CERT_DECODE:X509 in plugin 'openssl'
00[LIB]           feature CERT_DECODE:X509 in plugin 'openssl' has unmet soft dependency: PUBKEY:D
SA
00[LIB]     loading feature CERT_DECODE:PGP in plugin 'pem'
00[LIB] feature CERT_DECODE:PGP in plugin 'pem' has unmet dependency: CERT_DECODE:PGP
00[LIB]     feature CERT_DECODE:ANY in plugin 'pem' has unmet soft dependency: CERT_DECODE:PGP
00[LIB] loading feature CUSTOM:pkcs11-certs in plugin 'pkcs11'
00[CFG] C_GetAttributeValue(NULL) error: ATTRIBUTE_TYPE_INVALID
00[LIB] loading feature PRIVKEY:ANY in plugin 'pkcs11'
00[LIB] loading feature PRIVKEY:ANY in plugin 'tpm'
00[LIB] loading feature CRYPTER:AES_CBC-16 in plugin 'aesni'
00[LIB] loading feature CRYPTER:AES_CBC-24 in plugin 'aesni'
00[LIB] loading feature CRYPTER:AES_CBC-32 in plugin 'aesni'
00[LIB] loading feature CRYPTER:AES_ECB-16 in plugin 'aesni'
```

```
# rpm -qa |grep -i strongs
strongswan-charon-nm-5.8.4-2.fc32.x86_64
strongswan-5.8.4-2.fc32.x86_64
NetworkManager-strongswan-1.5.0-1.fc33.x86_64
```

```
NetworkManager-strongswan-gnome-1.5.0-1.fc33.x86_64
```

Thanks.

History

#1 - 22.05.2020 17:05 - Yuri B

Don't forget to setenforce 0, chmod -R a+rwx /var/lib/nss.

#2 - 25.05.2020 11:32 - Tobias Brunner

- Tracker changed from Bug to Issue

- Status changed from New to Feedback

- Start date deleted (22.05.2020)

When loading certificates, three attributes are requested: CKA_VALUE, CKA_LABEL, CKA_TRUSTED. Which of them is invalid for this module?

#3 - 30.09.2020 13:42 - Tobias Brunner

- Category set to libstrongswan

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback