strongSwan - Feature #490

charon-nm fails to find private key if CKA_ID doesn't match the x509 subject key id

16.01.2014 17:01 - Raphael Geissert

Status:	Closed	**Start date:**	16.01.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.5.1		
Resolution:	Fixed		

Description

When using the smartcard authentication method in the NetworkManager plugin, charon-nm fails to find the private key for the x509 certificate if the CKA_ID of the privkey doesn't match the subject key identifier of the certificate.

I sent a mail with a proposed patch to the -dev list a few months ago with no replies. The proposal was that in case of no privkey being found, the charon-nm plugin would workaround the issue by restarting the search with the CKA_ID of the first token with an object of class CKO_PUBLIC_KEY or CKO_CERTIFICATE, in that order.

The real problem is charon-nm not being told the CKA_ID of the certificate it is going to use to authenticate, but later having to tell credentials manager the keyid it wants to load.

Noticed it in 4.5.2 but I believe 5.x to still be affected.

Related issues:

Related to Issue #845: Problem with StrongSwan (5.1.2) and USB eToken Aladdin	**Closed**	**08.02.2015**
Related to Issue #2671: Passing user-supplied cerificate file names to charon...	**New**	

Associated revisions

Revision 9a704963 - 04.10.2016 12:09 - Raphael Geissert

pkcs11: Look for the CKA_ID of the cert if it doesn't match the subjectKeyId

charon-nm fails to find the private key when its CKA_ID doesn't match the
subjectKeyIdentifier of the X.509 certificate. In such cases, the private
key builder now falls back to enumerating all the certificates, looking for
one that matches the supplied subjectKeyIdentifier. It then uses the CKA_ID
of that certificate to find the corresponding private key.

It effectively means that PKCS#11 tokens where the only identifier to relate
the certificate, the public key, and the private key is the CKA_ID are now
supported by charon-nm.

Fixes #490.

History

#1 - 01.08.2016 16:36 - Raphael Geissert

- File keyid-alias.patch added

- File login-refactor.patch added

Attached patches are a revisited version of the ones I sent back then. They apply against 5.2.1.

Note that *login-refactor.patch* is entirely optional.

#2 - 25.08.2016 15:30 - Raphael Geissert

After discussing with Tobias Brunner, the plan would be to:

1. add a fallback case to find_key where it would enumerate the certificates, find the one that corresponds to the identifier and obtain the CKA_ID
2. at a later point make charon-nm parse PKCS11 URIs (cf. https://p11-glue.freedesktop.org/p11-kit.html)
3. at a later point make the certificate configurable via the GUI. Cf. https://bugzilla.gnome.org/show_bug.cgi?id=679860

#3 - 25.08.2016 15:38 - Tobias Brunner

- Related to Issue #845: Problem with StrongSwan (5.1.2) and USB eToken Aladdin added

#4 - 31.08.2016 13:38 - Raphael Geissert

- File 0001-pkcs11-look-for-the-CKA_ID-of-the-cert-if-it-doesn-t.patch added

Raphael Geissert wrote:

> After discussing with Tobias Brunner, the plan would be to:
>
> 1. add a fallback case to find_key where it would enumerate the certificates, find the one that corresponds to the identifier and obtain the CKA_ID

Attached patch implements that. Tested against 5.2.1 but the only two commits since then should have no effect on it.

#5 - 04.10.2016 12:12 - Tobias Brunner

- Tracker changed from Issue to Feature

- Category set to libstrongswan

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.5.1

- Resolution set to Fixed

I'm closing this for now. Extending charon-nm and the GUI should be tracked in a new ticket, if that's required sometime in the future.

#6 - 24.05.2018 09:32 - Tobias Brunner

- Related to Issue #2671: Passing user-supplied cerificate file names to charon-nm is problematic added

Files

keyid-alias.patch	6.13 KB	01.08.2016	Raphael Geissert
login-refactor.patch	3.77 KB	01.08.2016	Raphael Geissert
0001-pkcs11-look-for-the-CKA_ID-of-the-cert-if-it-doesn-t.patch	5.74 KB	31.08.2016	Raphael Geissert