strongSwan - Feature #3457

user-friendly pkcs11 certificate selection

22.05.2020 12:52 - Yuri B

Status:	New	**Start date:**	22.05.2020
Priority:	Low	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:			
Target version:			
Resolution:			

Description

I see there've been a lot of open issues and questions about this, with a lot of people (end-users) including me that are having problems with specifying / picking the right certificate off their pkcs11 token/smartcard.

It's 2020, the current trend is to use p11kit that acts as an umbrella for various pkcs11 vendor drivers. My suggestion is going that route, which will eliminate the need to learn what slot to use, what HEX to write in order to select proper cert.

openvpn has already implemented and provided this via `--show-pkcs11-ids` option that end-user just invokes to see the available certs, then picks the right one, then puts the URI into `pkcs11-id` and he's done. p11kit URIs are essentially a query language that can select multiple certs, so in case more broad selection is needed, you could just go that route.

Same with https://www.infradead.org/openconnect/pkcs11.html , it's just very easy for end user to work with that.

Now regarding the networkmanager. Thanks for finally providing a way to make smartcards/tokens work via gnome UI. Now if you implement the above, you might want to modify the UI so that there's a certificate picker that would allow user to select the necessary certificate. You can even ask him to first login to all tokens, then present with a list of certs, then allow him to pick the necessary cert, then under the hood check whether that cert would actually be ready to use in normal connection mode. That is, do preliminary checks finding the key and checking the cert validity before saving the URI in the config.

Just a couple of thoughts... Thanks.

Related issues:

Is duplicate of Issue #2671: Passing user-supplied cerificate file names to c...	**New**

History

#1 - 25.05.2020 11:13 - Tobias Brunner

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