Smuxi Issues [FROZEN ARCHIVE] - Feature # 96: SSL+CertFP support

Status:	Closed	Priority:	Urgent	
Author:	Mirco Bauer	Category:	Engine	
Created:	08/03/2008	Assigned to:	Mirco Bauer	
Updated:	10/02/2015	Due date:		
Complexity:	Medium	•		
Subject:	SSL+CertFP support			
Description:	Implement SSL+CertFP support see: http://www.oftc.net/oftc/NickServ/CertFP			

Associated revisions

11/21/2011 02:40 AM - Mirco Bauer

[Engine/Engine-*] Refactored IProtocolManager.Connect() to use ServerModel

Cleanly pass all connection parameters to the protocol manager using the ServerModel class. This way it is no longer needed to add and save a server before making use of SSL options.

Also it will make it easier to add multi-identity support (references: #428), different encoding per server (references: #27), client certificates (references: #96) and SASL support (references: #98).

10/02/2015 04:29 PM - Mirco Bauer

Engine(-IRC), Frontend-GNOME: support CertFP (closes: #96)

[CertFP][] is a NickServ authentication feature supported by modern IRC networks as an more secure alternative to the famous "/msg NickServ IDENTIFY my_password" command.

[CertFP]: https://freenode.net/certfp/

As this is an internal setting only (for now) you need to configure it using the /config command like this:

/config Servers/IRC/\$SERVER_ID/ClientCertificateFilename = mycert.pfx /config save

The client certificate can be generated using makecert like this:

makecert -eku 1.3.6.1.5.5.7.3.2 -r -cy end -n "CN=\$USER" -p12 mycert.pfx ""

The certificate must not use a passphrase, else it can't be loaded. Thus secure the file against access by other users with:

chmod 400 mycert.pfx

Place the certificate in ~/.config/smuxi/certs/ otherwise specify the full path in ClientCertificateFilename.

On most IRC networks that support CertFP you can verify if the certificate was used using /whois on your own nickname. A line like this should show up in the whois reply:

12/05/2025 1/2

Special thanks goes to An-Ivoz for finding out how client certificate selection works!

History

08/28/2010 11:43 PM - Mirco Bauer

- Target version changed from 0.8 to TBD

CA certs need to be imported into Smuxi and the CA store needs to be populated at runtime somehow... SslStream doesn't need to offer a simple API for this:/

08/29/2010 12:48 PM - Mirco Bauer

Also see http://freenode.net/faq.shtml#sslaccess

01/09/2014 08:55 PM - Mirco Bauer

- Priority changed from Normal to Urgent
- Complexity set to Medium

Cert validation is NOT required as the client only needs to supply a client certificate and the _server_ validates that cert for authentication.

01/22/2014 07:40 PM - Mirco Bauer

- % Done changed from 0 to 90

I have implemented a PoC of this feature here:

https://github.com/meebey/smuxi/tree/experiments/certfp

But it seems like Mono has a bug in its SSL implementation which does not send a client supplied certificate to the server :/

10/02/2015 07:38 PM - Mirco Bauer

- Target version changed from TBD to 1.1

10/02/2015 07:38 PM - Mirco Bauer

- Status changed from New to Closed
- % Done changed from 90 to 100

Applied in changeset commit: "83a2ab1c3e64ef4438b8e901891270f65566ea95".

10/02/2015 07:40 PM - Mirco Bauer

That was because the client certificate selection callback wasn't provided, thus the supplied cert was never sent.

12/05/2025 2/2