Quassel IRC - Feature #463

GUI for verifying SSL Certificates

01/04/2009 05:51 PM - xAFFE

Status:	Feedback	**Start date:**	01/04/2009
Priority:	Normal	**Due date:**	
Assignee:	EgS	**% Done:**	0%
Category:	Quassel Client	**Estimated time:**	0.00 hour
Target version:			
OS:	Any		

Description

There should be a gui where the fingerprint of the SSL-Certificate is printed, so I can verify the cert.

Related issues:

Related to Quassel IRC - Feature #464: Ability to specify a "Certificate Auth...	**Feedback**	**01/04/2009**

History

#1 - 01/04/2009 06:00 PM - xAFFE

As mentioned on IRC:

This dialog should be to check the the IRC-Server certificate.

#2 - 01/13/2009 09:29 PM - EgS

- Status changed from New to Feedback

- Assignee set to EgS

As this is obviously related to the CA cert feature request:
wouldn't it suffice, if the CA cert verified the servers authenticity? Also I can think of an option to enforce CA verification, so if it fails that quassel will not continue to connect to the server.

#3 - 01/16/2009 06:50 PM - Sputnick

It would also be nice to show a different icon ("security-medium" exists for that purpose) in the statusbar in case there were problems with the cert, and maybe a way (tooltip? popup?) to display the warnings generated by cert validation.

Also we should at least warn or outright refuse connection if the core cert's fingerprint has changed; similar to what SSL does. This prevents MITM attacks after the initial connection.

#4 - 01/16/2009 07:49 PM - Sputnick

One more thing: We need to find a way to make SSL connections by default. Right now, if the core doesn't support SSL, we fail and tell the user to uncheck the box. This is OK, though it would be smoother to just change that directly if the user accepts rather than requiring extra clicks. Need to make sure it works with the mono client too.

#5 - 01/17/2009 01:00 AM - EgS

Please open another BR as this issue is to ensure that the connected *IRC* server is trusted.

#6 - 01/17/2009 04:23 AM - xAFFE

EgS wrote:

> As this is obviously related to the CA cert feature request:
> wouldn't it suffice, if the CA cert verified the servers authenticity? Also I can think of an option to enforce CA verification, so if it fails that quassel will not continue to connect to the server.

This dialog would only be for manual verification. It should only contain the fingerprint of the server I'm connecting to, maybe this could just printed on the status buffer.