Quassel IRC - Feature #1564

TLS-SRP support

04/18/2020 04:39 PM - SoniEx2

Status:	New	Start date:	04/18/2020
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:			
os:	Any		

Description

you can't write passwords to a server log if you're using TLS-SRP, as you never see the passwords.

it also solves the server cert problem (you can still have server certs with TLS-SRP, but it's not strictly necessary). it'd just improve things all around.

History

#1 - 04/18/2020 04:42 PM - SoniEx2

(might want to mark a server as using SRP after the first connection, and enforce that for future sessions. let's just put an end to the plaintext passwords already, okay?)

#2 - 05/24/2021 10:15 PM - SoniEx2

Sadly the main blocker for this is that Qt doesn't support TLS-SRP... sigh

04/28/2024 1/1