Quassel IRC - Feature #911

DH1080 Key exchange for Blowfish encryption

02/11/2010 10:31 PM - johu

Status:	Resolved	**Start date:**	02/11/2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Quassel Core	**Estimated time:**	0.00 hour
Target version:	0.9.0		
OS:	Any		

Description

After stabilisation of #689 include key exchange. More Information about that can be found here

http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://blog.bjrn.se/2009/01/proposal-for-better-irc-encryption.html

Related issues:

Blocked by Quassel IRC - Feature #689: Blowfish Support	**Resolved**	**05/08/2009**

History

#1 - 02/26/2010 12:50 AM - johu

- Target version set to 0.7.0

#2 - 03/09/2010 07:54 PM - johu

- Target version deleted (0.7.0)

#3 - 07/29/2010 04:47 AM - johu

- Category changed from General / Unspecified to Quassel Core

- Status changed from New to Assigned

#4 - 08/26/2010 06:09 PM - johu

- Target version set to 0.8.0

#5 - 01/20/2012 07:40 PM - johu

- Target version deleted (0.8.0)

#6 - 01/31/2013 07:26 PM - Anonymous

- Assignee changed from johu to Anonymous

- Target version set to Some future release

PR 5

#7 - 02/20/2013 07:59 PM - Anonymous

- Status changed from Assigned to Resolved

- Target version changed from Some future release to 0.9.0

Merged in 04315f46a16fc3627218377071e008b6b9744992

#8 - 08/25/2013 02:13 AM - sjefen6

Might I suggest the following improvements:

- Implement CBC http://www.donationcoder.com/Software/Mouser/mircryption/extra_cbcinfo.php
- Disable keyx for channels
- Work on some indication that a key is set in the client, and some indication that the message received was decrypted from blowfish