Smuxi - Feature # 651: OTR support

Status:	New	**Priority:**	Normal
Author:	Mirco Bauer	**Category:**	Engine
Created:	11/22/2011	**Assigned to:**	Mirco Bauer
Updated:	08/25/2015	**Due date:**	
Complexity:	High		
Subject:	OTR support		
Description:	Smuxi should have OTR support, I wanted something like that for a long time but all the existing protocols for IRC simply sucked. The specification can be found at http://www.cypherpunks.ca/otr/		

History

11/27/2013 06:32 PM - Mirco Bauer

- Category set to Engine

- Target version set to TBD

I will look into making a otr-sharp binding for the libotr library. This could be some good hack candidate for the 30C3.

01/05/2015 08:58 PM - Mirco Bauer

Smuxi should use libotr but that needs a C# binding. not sure if it has create/delete function for management memory.

01/05/2015 08:59 PM - Silvan Gebhardt

+1 (and where is the like button?)

01/05/2015 09:00 PM - Mirco Bauer

For inspiration https://github.com/mmb/weechat-otr/blob/master/weechat_otr.py can be used

04/14/2015 05:17 PM - Alexander E. Fischer

If you see a chance, please do not store the OTR keys on the (possibly remote) engine. A lot of people will run Smuxi engines on rented hardware in off-site centers or even on cloud instances which will always offer only limited security. If I interpret it correctly, OTR only needs the keys to authenticate the first DH(Diffie Hellman) key exchange in each chat session. If that is true, you could store the keys where the frontend is and only initiate sessions while the frontend is connected, but already running connections could possibly continue to work when the main part of the protocol handling happens in the engine.

Also, please store and read OTR keys in the default LibOTR format. Far too many clients have their own storage format resultung in converter projects like "Keysync":https://github.com/guardianproject/keysync .

04/16/2015 05:35 AM - Mirco Bauer

Perl (binding?):
https://metacpan.org/release/Protocol-OTR

Objective C binding:
https://github.com/chatsecure/otrkit

04/16/2015 05:35 AM - Mirco Bauer

- Assigned to set to Mirco Bauer

- Target version changed from TBD to 1.1