Bip - Bug #500

bip 0.8.9 and 0.9.0 often fail on SSL/TLS connection to Freenode

2016-11-24 21:22 - Adam Williamson

Status:	New	**Start date:**	2016-11-24
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:			
Patch Available:		**Branch:**	
Found in Versions:		**Security:**	
Confirmed:	No	**Help Needed:**	

Description

After rebooting my Bip server today, I noticed it frequently fails on attempts to connect to Freenode via SSL/TLS, like this:

```
Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 [freenode] Connecting user 'adamw' using server chat.freenode.net:7000
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 No SSL certificate check store configured. Default store will be used.
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 WARNING: mySSL_get_cert() SSL server supplied no certificate !
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 ERROR: No certificate in SSL write_socket
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 WARNING: mySSL_get_cert() SSL server supplied no certificate !
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 ERROR: No certificate in SSL write_socket
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 WARNING: mySSL_get_cert() SSL server supplied no certificate !
    Nov 24 12:14:20 ircproxy.happyassassin.net bip[1342]: 24-11-2016 12:14:20 ERROR: No certificate in SSL write_socket
```

It's rather strange, because it suggests that `SSL_get_peer_certificate()` is failing, and I don't know why it would do that (and it doesn't seem very easy to debug. Man I hate openssl.) I can only think there must, somehow, be something wrong with the SSL context.

I don't think there is a server issue here, as HexChat seems to always work when I try it (with SSL). I do note that Hexchat seems to wait for `SSL_is_init_finished` to be true before doing `SSL_get_cert_info`...