Smuxi - Bug # 977: Connection to XMPP server with SHA2 certificate signature fails on mono 2.6 even when

Status:	New	**Priority:**	Normal
Author:	Jan Krajdl	**Category:**	Other
Created:	08/10/2014	**Assigned to:**	
Updated:	05/24/2015	**Due date:**	
Complexity:			
Found in Version:			
Subject:	Connection to XMPP server with SHA2 certificate signature fails on mono 2.6 even when certificate verify is disabled		
Description:	I have problem with connection to my XMPP server. XMPP server has TLS enabled and using certificate with SHA2 signature (SHA 256 or SHA 512). Also I'm using mono 2.6 for compatibility with native windows frontend and mono 2.6 can't recognize SHA2. But even when I have disabled certificate verification in XMPP account settings it still fails with exception on engine side and I am unable to connect to server. XMPP server still can handle unencrypted connection. I'm attaching engine console out when this error occurres.		

History

08/12/2014 11:30 PM - Mirco Bauer

Looks like Mono requires that it understands the certificate regardless of the validation part. This won't fix this issue but you could workaround it by using stunnel.

05/24/2015 11:34 AM - Mirco Bauer

- Category changed from Engine XMPP (Jabber) to Other

- Assigned to deleted (Oliver Schneider)

This issue isn't XMPP specific actually, but an issue with Smuxi in general, but really Mono.

05/24/2015 11:35 AM - Mirco Bauer

You can upgrade your Mono to a newer version if you use Mono on Windows as well.

05/24/2015 07:13 PM - Jan Krajdl

Yeah, but mono in Windows has some issues too... don't remember exactly what it was but remember something that I couldn't quit it (always needed kill from OS) and it also wouldn't reconnect automatically (this combination I hated because I usually has smuxi running all the time and just suspend computer). I finally forced XMPP server to listen on another port with unencrypted connections and connect smuxi without encryption - as both are running on same server it's not security issue and it's working fine. But maybe for someone else who has to have Windows (:-)) and doesn't have own XMPP server it can be really anoying...

Files

x509_error.txt	5.6 KB	08/10/2014	Jan Krajdl