Smuxi - Task # 1070: Replace Mono's System.Security library with something better

Status:	New	**Priority:**	Normal
Author:	Mirco Bauer	**Category:**	Engine
Created:	06/14/2015	**Assigned to:**	Mirco Bauer
Updated:	01/09/2017	**Due date:**	
Complexity:	High		
Subject:	Replace Mono's System.Security library with something better		
Description:	IRCS used by Engine-IRC and HTTPS used by Engine-Twitter, Engine-Campfire and Engine-JabbR rely on the X.509 implemented by the CLR. There are many certificate validation issues with Mono's implementation, some of them are documented with known workarounds here: https://smuxi.im/faq/troubleshooting/linux-tls/ Since the .NET Core will not improve the situation with X.509 validation. It relies on the crypto library provided by the operating system, thus Smuxi should seek out into using OpenSSL, GnuTLS, PolarSSL, WolfSSL and the like.		

History

06/14/2015 02:57 PM - Mirco Bauer

- Subject changed from Replace Mono's System.Security.Cryptography.X509Certificates with something better to Replace Mono's System.Security library with s

06/14/2015 03:25 PM - Mirco Bauer

PoC for certificate validation using PolarSSL in Smuxi: https://github.com/meebey/smuxi/tree/experiments/polarssl_cert_validation

01/09/2017 09:20 AM - Mirco Bauer

As a short term workaround you can use stunnel with Smuxi to connect to SSL/TLS enabled servers, see: https://smuxi.im/faq/usage/stunnel/