strongSwan - Issue #1540

No trusted RSA public key found for

28.06.2016 10:02 - Yassine Imounachen

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.4.0	**Resolution:**	No change required

Description

Hello,

I get "No trusted RSA public key found for [domain]" in strongSwan client on Arch Linux unless I add (Let's Encrypt issued) server's certificate in /etc/ipsec.d/certs and specify that certificate in ipsec.conf using rightcert=cert.pem. I'm using IKEv2 with MS-CHAPv2. OS X 10.11, Windows 10, iOS 9 and Android (with stronSwan app) clients work fine without adding any certificates.

History

#1 - 28.06.2016 11:38 - Tobias Brunner

- Category changed from charon to configuration

- Status changed from New to Feedback

You obviously need to install the CA certificate on the client in /etc/ipsec.d/cacerts (or as you did the server certificate), or reference the CA certificate that might already be on the system (e.g. in /etc/ssl/certs/DST_Root_CA_X3.pem on Ubuntu) in a ca section (you can also copy or symlink it to the cacerts directory). strongSwan does not automatically use the CA certificates installed on the system (the NM plugin being an exception).

#2 - 28.06.2016 12:41 - Yassine Imounachen

I've tried adding CA certificates from https://letsencrypt.org/certificates/ before, but I was adding the wrong one (isrgrootx1.pem). I added the certificate you mentioned (DST_Root_CA_X3.pem) in /etc/ipsec.d/cacerts/ and now the client connects successfully. Thank you!

#3 - 28.06.2016 16:51 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required

> I've tried adding CA certificates from https://letsencrypt.org/certificates/ before, but I was adding the wrong one (isrgrootx1.pem).

Yes, Let's Encrypt currently issues certificates from the "Let’s Encrypt Authority X3" intermediate CA, for which there is no certificate published that's signed by ISRG Root X1. The one published is signed by the aforementioned CA "DST Root CA X3".