strongSwan - Bug #252

scep client - invalid flags?

11.11.2012 20:46 - Norbert Wegener

Status:	Closed	**Start date:**	11.11.2012
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.0.2		
Affected version:	5.0.1	**Resolution:**	Fixed

Description

Hello,
I use strongswan 5.0.1 and want to request certificates from a windows 2008 server via scep.
The first part of the action is working fine:
sudo ipsec scepclient --out caCert --url http://192.168.1.18/certsrv/mscep/mscep.dll -f

loaded plugins: curl aes des sha1 sha2 md5 random x509 pkcs1 pkcs8 pem gmp
written ra cert file '/usr/local/etc/ipsec.d/cacerts/caCert-ra-1.der' (1383 bytes)
written ra cert file '/usr/local/etc/ipsec.d/cacerts/caCert-ra-2.der' (1365 bytes)
written ca cert file '/usr/local/etc/ipsec.d/cacerts/caCert.der' (901 bytes)

Unfortunately the next part fails:
sudo ipsec scepclient --out pkcs1=joeKey.der --out cert==joeCert.der \
--dn "C=CH, CN=John Doe" \
--url http://192.168.1.18/certsrv/mscep/mscep.dll \
--in cacert-enc=caCert-ra-2.der --in cacert-sig=caCert-ra-1.der
loaded plugins: curl aes des sha1 sha2 md5 random x509 pkcs1 pkcs8 pem gmp
fingerprint: c51cc00908f023a0365c93562cf022f3
written pkcs1 file '/usr/local/etc/ipsec.d/private/joeKey.der' (1191 bytes)
transaction ID: B269BB0F93A7A4D7E5291B9C3A4C98C3
failInfo: badMessageCheck - integrity check failed
error: reply status is not 'SUCCESS'

Der Windows Server reports:
The Network Device Enrollment Service cannot decrypt the client's PKCS7 message (0x80090009). Invalid flags specified.

Norbert

History

#1 - 12.11.2012 09:15 - Martin Willi

- Status changed from New to Assigned

- Assignee set to Martin Willi

- Target version set to 5.0.2

There is a bug in 5.0.1 with RSA encryption in the gmp plugin. Please try to apply the patch at:

http://git.strongswan.org/?p=strongswan.git;a=commitdiff;h=828cefc3

I think it should fix this issue.

#2 - 12.11.2012 10:37 - Norbert Wegener

The patch fixes the problem. I do get certificates from the Windows 2008 server now.
Thank you.

Norbert

#3 - 12.11.2012 11:17 - Martin Willi

- Status changed from Assigned to Closed

- Resolution set to Fixed