strongSwan - Issue #2858

NetworkManager : no trusted RSA public key found

12.12.2018 18:04 - smina would

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	networkmanager (charon-nm)		
Affected version:	5.7.1	**Resolution:**	No change required

Description

after successfully configuring network-manager on my ubuntu 18.10 (https://wiki.strongswan.org/issues/2822), i tried to configure a second ubuntu 18.10. Unfortunately, I get the error message: no trusted RSA public key found for ... However I use the same network-manager configuration for both.
I certainly did something special on the first, but I do not know what. I copied the ca certificate in /etc/ssl/certs, the problem remains the same.

have I forgotten something?

History

#1 - 13.12.2018 10:36 - Tobias Brunner

- Category changed from configuration to networkmanager (charon-nm)

- Status changed from New to Feedback

> I copied the ca certificate in /etc/ssl/certs, the problem remains the same.

The error does not refer to the CA certificate, but the client's private key. So make sure the client's certificate and private key is loaded properly (also check the log for errors during that process).

#2 - 14.12.2018 09:25 - smina would

I don't understand. On first computer (working), I set the network-manager like this :

bd4IajvsqjPT.png?width=450

no certificate and private key, and nothing into /etc/ipsec.d/private/ and /etc/ipsec.d/certs/

#3 - 14.12.2018 09:30 - Tobias Brunner

> no certificate and private key, and nothing into /etc/ipsec.d/private/ and /etc/ipsec.d/certs/

No files are needed in those directories because the *charon-nm* daemon does not use them. But if it complains about not finding a private key that

means you configured the GUI on the second client incorrectly (i.e. you didn't configure "EAP" as authentication method).

#4 - 14.12.2018 09:31 - smina would

syslog of first computer :

```
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.3289] audit: op="connection-activate" uuid="543678c4-bcd0-4bd6-aa8e-29767925f077" name="VPN 1" pid=7755 uid=1000 result="success"
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.3443] vpn-connection[0x5603f6d7e360,543678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Saw the service appear; activating connection
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.3587] vpn-connection[0x5603f6d7e360,543678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: VPN connection: (ConnectInteractive) reply received
Dec 14 09:26:23 cri-port3-sabe charon-nm: 05[CFG] received initiate for NetworkManager connection VPN 1
Dec 14 09:26:23 cri-port3-sabe charon-nm: 05[CFG] using CA certificate, gateway identity 'svpn.domaine.fr'
Dec 14 09:26:23 cri-port3-sabe charon-nm: 05[IKE] initiating IKE_SA VPN 1[34] to 192.168.244.107
Dec 14 09:26:23 cri-port3-sabe charon-nm: 05[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 05[NET] sending packet: from 172.18.239.138[46619] to 192.168.244.107[500] (1112 bytes)
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.3690] vpn-connection[0x5603f6d7e360,543678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: VPN plugin: state changed: starting (3)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 01[NET] received packet: from 192.168.244.107[500] to 172.18.239.138[46619] (38 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 01[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 01[IKE] peer didn't accept DH group ECP_256, it requested MODP_2048
Dec 14 09:26:23 cri-port3-sabe charon-nm: 01[IKE] initiating IKE_SA VPN 1[34] to 192.168.244.107
Dec 14 09:26:23 cri-port3-sabe charon-nm: 01[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 01[NET] sending packet: from 172.18.239.138[46619] to 192.168.244.107[500] (1304 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[NET] received packet: from 192.168.244.107[500] to 172.18.239.138[46619] (464 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[IKE] remote host is behind NAT
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[IKE] sending cert request for "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[IKE] establishing CHILD_SA VPN 1{34}
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ CPRQ(ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 13[NET] sending packet: from 172.18.239.138[55846] to 192.168.244.107[4500] (336 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 12[NET] received packet: from 192.168.244.107[4500] to 172.18.239.138[55846] (1236 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 12[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 12[ENC] received fragment #1 of 2, waiting for complete IKE message
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[NET] received packet: from 192.168.244.107[4500] to 172.18.239.138[55846] (1060 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[ENC] received fragment #2 of 2, reassembling fragmented IKE message
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[IKE] received end entity cert "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=dsi-assistance@domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG]   using certificate "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=dsi-assistance@domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG] no issuer certificate found for "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=dsi-assistance@domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG]   issuer is "C=FR, ST=France, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG]   using certificate "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG]   using trusted ca certificate "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG] checking certificate status of "C=FR, ST=FRANCE, L=PARIS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG] certificate status is not available
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[CFG]   reached self-signed root ca with a path length of 0
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[IKE] authentication of 'svpn.domaine.fr' with RSA_EMSA_PKCS1_SHA2_384 successful
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[IKE] server requested EAP_IDENTITY (id 0x00), sending 'username'
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[ENC] generating IKE_AUTH request 2 [ EAP/RES/ID ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 11[NET] sending packet: from 172.18.239.138[55846] to 192.168.244.107[4500] (96 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 08[NET] received packet: from 192.168.244.107[4500] to 172.18.239.13
```

```
8[55846] (112 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 08[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 08[IKE] server requested EAP_MSCHAPV2 authentication (id 0xFF)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 08[ENC] generating IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 08[NET] sending packet: from 172.18.239.138[55846] to 192.168.244.10
7[4500] (144 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 06[NET] received packet: from 192.168.244.107[4500] to 172.18.239.13
8[55846] (144 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 06[ENC] parsed IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 06[IKE] EAP-MS-CHAPv2 succeeded: 'Welcome2strongSwan'
Dec 14 09:26:23 cri-port3-sabe charon-nm: 06[ENC] generating IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 06[NET] sending packet: from 172.18.239.138[55846] to 192.168.244.10
7[4500] (80 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 07[NET] received packet: from 192.168.244.107[4500] to 172.18.239.13
8[55846] (80 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 07[ENC] parsed IKE_AUTH response 4 [ EAP/SUCC ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 07[IKE] EAP method EAP_MSCHAPV2 succeeded, MSK established
Dec 14 09:26:23 cri-port3-sabe charon-nm: 07[IKE] authentication of 'username' (myself) with EAP
Dec 14 09:26:23 cri-port3-sabe charon-nm: 07[ENC] generating IKE_AUTH request 5 [ AUTH ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 07[NET] sending packet: from 172.18.239.138[55846] to 192.168.244.10
7[4500] (112 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[NET] received packet: from 192.168.244.107[4500] to 172.18.239.13
8[55846] (256 bytes)
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[ENC] parsed IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS DNS) SA TSi
TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) ]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] authentication of 'svpn.domaine.fr' with EAP successful
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] IKE_SA VPN 1[34] established between 172.18.239.138[username
]...192.168.244.107[svpn.domaine.fr]
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] scheduling rekeying in 35553s
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] maximum IKE_SA lifetime 36153s
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] installing new virtual IP 192.168.90.1
Dec 14 09:26:23 cri-port3-sabe charon: 01[KNL] 192.168.90.1 appeared on wlp2s0
Dec 14 09:26:23 cri-port3-sabe avahi-daemon[831]: Registering new address record for 192.168.90.1 on wlp2s0.IP
v4.
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] CHILD_SA VPN 1{34} established with SPIs c1a7242d_i c59462de
_o and TS 192.168.90.1/32 === 0.0.0.0/0
Dec 14 09:26:23 cri-port3-sabe charon-nm: 10[IKE] peer supports MOBIKE
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4380] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: VPN connection: (IP4 Config Get) reply received from old-style
plugin
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4385] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data: VPN Gateway: 192.168.244.107
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4385] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data: Tunnel Device: (null)
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4385] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data: IPv4 configuration:
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   Internal Address: 192.168.90.1
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   Internal Prefix: 32
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   Internal Point-to-Point Address: 192.168.90.1
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   Static Route: 192.168.90.1/32   Next Hop: 0.0.0.0
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   Internal DNS: 192.168.244.104
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   Internal DNS: 192.168.244.106
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data:   DNS Domain: '(none)'
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4386] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: Data: No IPv6 configuration
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4400] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: VPN connection: (IP Config Get) complete
Dec 14 09:26:23 cri-port3-sabe NetworkManager[847]: <info>  [1544775983.4401] vpn-connection[0x5603f6d7e360,54
3678c4-bcd0-4bd6-aa8e-29767925f077,"VPN 1",0]: VPN plugin: state changed: started (4)
Dec 14 09:26:23 cri-port3-sabe dbus-daemon[832]: [system] Activating via systemd: service name='org.freedeskto
p.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.16' (uid=0 pid=847 comm="/
usr/sbin/NetworkManager --no-daemon " label="unconfined")
Dec 14 09:26:23 cri-port3-sabe systemd[1]: Starting Network Manager Script Dispatcher Service...
Dec 14 09:26:23 cri-port3-sabe dbus-daemon[832]: [system] Successfully activated service 'org.freedesktop.nm_d
ispatcher'
Dec 14 09:26:23 cri-port3-sabe systemd[1]: Started Network Manager Script Dispatcher Service.
Dec 14 09:26:23 cri-port3-sabe nm-dispatcher: req:1 'vpn-up' [wlp2s0]: new request (1 scripts)
Dec 14 09:26:23 cri-port3-sabe nm-dispatcher: req:1 'vpn-up' [wlp2s0]: start running ordered scripts...
```

I will send logs of second computer later...

#5 - 14.12.2018 15:27 - smina would

Logs from an ubuntu fresh install (with network-manager-strongswan, libcharon-extra-plugins and libcharon-standard-plugins installed) :

```
Dec 14 15:14:03 username-VirtualBox charon-nm: 05[CFG] received initiate for NetworkManager connection VPN 1
Dec 14 15:14:03 username-VirtualBox charon-nm: 05[CFG] using CA certificate, gateway identity 'svpn.domaine.fr
'
Dec 14 15:14:03 username-VirtualBox charon-nm: 05[IKE] initiating IKE_SA VPN 1[2] to 192.168.244.107
Dec 14 15:14:03 username-VirtualBox charon-nm: 05[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP
) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 05[NET] sending packet: from 10.0.2.15[37812] to 192.168.244.10
7[500] (1112 bytes)
Dec 14 15:14:03 username-VirtualBox NetworkManager[369]: <info>  [1544796843.5162] vpn-connection[0x55f5162c43
80,b40a7577-3cd9-4a3e-9608-7b472e46bcf0,"VPN 1",0]: VPN plugin: state changed: starting (3)
Dec 14 15:14:03 username-VirtualBox charon-nm: 16[NET] received packet: from 192.168.244.107[500] to 10.0.2.15
[37812] (38 bytes)
Dec 14 15:14:03 username-VirtualBox charon-nm: 16[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 16[IKE] peer didn't accept DH group ECP_256, it requested MODP_
2048
Dec 14 15:14:03 username-VirtualBox charon-nm: 16[IKE] initiating IKE_SA VPN 1[2] to 192.168.244.107
Dec 14 15:14:03 username-VirtualBox charon-nm: 16[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP
) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 16[NET] sending packet: from 10.0.2.15[37812] to 192.168.244.10
7[500] (1304 bytes)
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[NET] received packet: from 192.168.244.107[500] to 10.0.2.15
[37812] (464 bytes)
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N
(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[IKE] local host is behind NAT, sending keep alives
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[IKE] remote host is behind NAT
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[IKE] sending cert request for "C=FR, ST=FRANCE, L=PARIS, O=s
vpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[IKE] establishing CHILD_SA VPN 1{2}
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CER
TREQ CPRQ(ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 06[NET] sending packet: from 10.0.2.15[43503] to 192.168.244.10
7[4500] (336 bytes)
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[NET] received packet: from 192.168.244.107[4500] to 10.0.2.1
5[43503] (1236 bytes)
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[ENC] received fragment #1 of 2, waiting for complete IKE mes
sage
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[NET] received packet: from 192.168.244.107[4500] to 10.0.2.1
5[43503] (1060 bytes)
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[ENC] received fragment #2 of 2, reassembling fragmented IKE
message
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[IKE] received end entity cert "C=FR, ST=FRANCE, L=PARIS, O=s
vpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=dsi-assistance@domaine.fr"
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[CFG]   using certificate "C=FR, ST=FRANCE, L=PARIS, O=svpn.d
omaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=dsi-assistance@domaine.fr"
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[CFG] no issuer certificate found for "C=FR, ST=FRANCE, L=PAR
IS, O=svpn.domaine.fr, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=dsi-assistance@domaine.fr"
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[CFG]   issuer is "C=FR, ST=France, L=PARIS, O=svpn.domaine.f
r, OU=svpn.domaine.fr, CN=svpn.domaine.fr, E=svpn.domaine.fr"
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[IKE] no trusted RSA public key found for 'svpn.domaine.fr'
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[ENC] generating INFORMATIONAL request 2 [ N(AUTH_FAILED) ]
Dec 14 15:14:03 username-VirtualBox charon-nm: 08[NET] sending packet: from 10.0.2.15[43503] to 192.168.244.10
7[4500] (80 bytes)
Dec 14 15:14:03 username-VirtualBox NetworkManager[369]: <warn>  [1544796843.5708] vpn-connection[0x55f5162c43
80,b40a7577-3cd9-4a3e-9608-7b472e46bcf0,"VPN 1",0]: VPN plugin: failed: connect-failed (1)
```

configuration screenshot :
wIFl2Mo9TuUa.png

> But if it complains about not finding a private key that means you configured the GUI on the second client incorrectly (i.e. you didn't configure "EAP" as authentication method).

as you can see, it's the same configuration as the first client.

#6 - 14.12.2018 16:10 - Tobias Brunner

Yeah, sorry, didn't read the error message properly. According to the log no issuer certificate was found. Even though a certificate with the proper subject DN was apparently loaded, but maybe the certificate you loaded is based on a different key (check keyids and other properties with e.g. pki --print). It's also interesting that the same error is seen on the other host, but it somehow managed to continue (perhaps you messed up your PKI somehow, same IDs or keys for multiple certificates).

#7 - 14.12.2018 23:24 - smina would

> but maybe the certificate you loaded is based on a different key

it's the same file on both. And pki --print --in caCert.der return the same values.

> perhaps you messed up your PKI somehow, same IDs or keys for multiple certificates

Server side, I placed two CA certificates into /etc/ipsec.d/cacerts/ issued from the same private key. did I make a mistake?

#8 - 17.12.2018 09:19 - Tobias Brunner

> > but maybe the certificate you loaded is based on a different key
>
> it's the same file on both. And pki --print --in caCert.der return the same values.

Rally? That's strange.

> perhaps you messed up your PKI somehow, same IDs or keys for multiple certificates

> Server side, I placed two CA certificates into /etc/ipsec.d/cacerts/ issued from the same private key. did I make a mistake?

Maybe. The behavior of the first client is actually a bit weird. It complains that it doesn't find an issuer certificate for the server certificate but it then still continues with the CA certificate. This could indicate an issue with the PKI (as I mentioned perhaps the same identity and key for CA certificate and server certificate, that both DNs list the same CN is already a bit weird, maybe they also contain the same SANs). But why the second client doesn't behave the same I don't know.

#9 - 20.12.2018 10:43 - smina would

I create new certificates and replace olds, now all Ubuntu clients work... but the Windows clients does not work anymore :'(returning error 13801

I follow SimpleCA and Win7CertReq to generate certificate:

```
ipsec pki --self --in ca.key --dn "C=FR, O=xxxxx, CN=yyyyy" --ca > caCert.der
```

```
ipsec pki --pub --in server.new.key| ipsec pki --issue --cacert caCert.der --cakey ca.key --dn "C=FR, O=xxxxx,
 CN=svpn.domaine.fr" --san svpn.domaine.fr --flag serverAuth --flag ikeIntermediate > peerCert.der
```

- ca.key and server.new.key are RSA key generated from openssl command line.
- caCert.der successfully imported into Windows certificates store (certmgr.msc)

have I forgotten something?

#10 - 20.12.2018 10:48 - smina would

I just understand my mistake! sorry

#11 - 20.12.2018 10:53 - smina would

I import peercert.der to windows certmgr but the problem remains the same.

#12 - 20.12.2018 11:05 - Tobias Brunner

> I import peercert.der to windows certmgr but the problem remains the same.

No sure what your peercert.der is exactly (the server cert?), but if you use EAP, you only need to install the CA certificate on the client. Make sure that it's placed in the right credential store and subdirectory (WindowsClients has some information on configuring clients).

#13 - 20.12.2018 11:39 - smina would

> No sure what your peercert.der is exactly

it's the End Entity Certificates, including san, serverAuth and ikeIntermediate flag. I imported caCert.der first time, but doesn't work.

Should I include it like this? :

```
ipsec pki --self --in ca.key --dn "C=FR, O=xxxxx, CN=yyyyy" --san svpn.domaine.fr --flag serverAuth --flag ike
Intermediate --ca > caCert.der
```

I don't think or I misunderstood the wiki page Win7CertReq

pki --print --in caCert.der :

```
  subject:  "C=FR, O=xxxxx, CN=yyyyy"
  issuer:   "C=FR, O=xxxxx, CN=yyyyy"
  validity:  not before Dec 20 09:27:58 2018, ok
             not after  Dec 19 09:27:58 2021, ok (expires in 1094 days)
  serial:    23:4c:64:14:b5:70:e1:c9
  flags:     CA CRLSign self-signed
  subjkeyId: 3d:c6:72:85:60:a2:20:2d:14:eb:9c:df:fb:e8:56:15:01:87:c5:fa
  pubkey:    RSA 4096 bits
  keyid:     af:29:98:f0:ce:45:1f:d3:f0:40:c5:5c:15:2f:ef:46:b6:ff:df:aa
  subjkey:   3d:c6:72:85:60:a2:20:2d:14:eb:9c:df:fb:e8:56:15:01:87:c5:fa
```

pki --print --in peerCert.der :

```
  subject:  "C=FR, O=xxxxx, CN=svpn.domain.fr"
  issuer:   "C=FR, O=xxxxx, CN=yyyyy"
  validity:  not before Dec 20 09:47:36 2018, ok
             not after  Dec 19 09:47:36 2021, ok (expires in 1094 days)
  serial:    22:85:71:67:1b:fa:f1:1c
  altNames:  svpn.univ-lemans.fr
  flags:     serverAuth ikeIntermediate
  authkeyId: 3d:c6:72:85:60:a2:20:2d:14:eb:9c:df:fb:e8:56:15:01:87:c5:fa
```

```
subjkeyId: cf:64:e2:76:8d:4b:26:24:c4:32:44:64:90:17:7a:3c:fe:ba:c5:b8
pubkey:    RSA 4096 bits
keyid:     21:f8:b1:9b:fe:a8:5a:92:af:b4:05:81:aa:12:7e:24:0b:55:8a:b6
subjkey:   cf:64:e2:76:8d:4b:26:24:c4:32:44:64:90:17:7a:3c:fe:ba:c5:b8
```

#14 - 20.12.2018 13:50 - Tobias Brunner

> No sure what your peercert.der is exactly

> it's the End Entity Certificates

That doesn't really clarify it (in particular the plural form).

> I imported caCert.der first time, but doesn't work.

Make extra sure that the certificate is located in the correct place (it won't work if it isn't).

> Should I include it like this? :

What do you mean? Also, adding a SAN to the CA certificate, which you also included in the end-entity certificate (at least in the DN, apparently not as SAN, so that might also be some mix-up), might not be such a good idea.

> I don't think or I misunderstood the wiki page Win7CertReq

That page only covers end-entity certificates (server and further down client), not CA certificates, where there are no requirements regarding flags and SANs.

#15 - 20.12.2018 14:23 - smina would

> That doesn't really clarify it (in particular the plural form).

Sorry, end entity certificate as explained here : SimpleCA

> Make extra sure that the certificate is located in the correct place (it won't work if it isn't).

Placed into Trusted root certification authorities.

#16 - 20.12.2018 14:46 - Tobias Brunner

> That doesn't really clarify it (in particular the plural form).

> Sorry, end entity certificate as explained here : SimpleCA

That's a general term and could signify certificates for users or servers, which are usually slightly different (with EAP you don't need any client certificates). End-entity certificates are the opposite of CA certificates (root and intermediate), basically leaf nodes in the PKI tree.

> Make extra sure that the certificate is located in the correct place (it won't work if it isn't).

> Placed into Trusted root certification authorities.

Of the "Local Computer" or the "My user account" certificate store? See Win7EapCert.

You might want to start from scratch again and make sure you don't add unnecessary or conflicting information in these certificates.

#17 - 20.12.2018 15:04 - smina would

> Of the "Local Computer" or the "My user account" certificate store? See Win7EapCert.

Local Computer.

> You might want to start from scratch again and make sure you don't add unnecessary or conflicting information in these certificates.

Yes, I will start from scratch again, I hope to finally understand what I'am doing wrong.

#18 - 03.01.2019 09:23 - smina would

Hi Tobias,

Have a happy, wealthy and successful year 2019 for you and Strongswan :)

Finally, I found the mistake! now all the systems work. The only thing that remains a mystery, why the ubuntu client could connect when it should not be possible (leftcert was not generated from the CA used on the client).
Anyway, thank you very much for your help, I understand a little better the operation of certificates in Strongswan.

#19 - 09.01.2019 15:29 - Noel Kuntze

- Status changed from Feedback to Closed

- Priority changed from Low to Normal

- Resolution set to No change required