strongSwan - Issue #3630

The certificate is loaded but not used.

17.11.2020 09:40 - bo lee

Status:	Feedback	
Priority:	Normal	
Assignee:		
Category:		
Affected version:	5.3.5	**Resolution:**

Description

Nov 16 13:27:51 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Nov 16 13:27:51 00[ASN] file content is not binary ASN.1
Nov 16 13:27:51 00[ASN] -----BEGIN CERTIFICATE-----
Nov 16 13:27:51 00[ASN] -----END CERTIFICATE-----
Nov 16 13:27:51 00[ASN] L0 - x509:

Nov 16 13:27:51 00[CFG] loaded ca certificate "C=JP, O=SBM, CN=SBM ROOT CA" from
'/etc/ipsec.d/cacerts/CNC_CasaSeGW_SBM_ROOT_CA_TEST.pem'
Nov 16 13:27:51 00[IKE] Entering get_ref in fsm_public_key
Nov 16 13:27:51 00[IKE] Entering destroy in fsm_public_key
Nov 16 13:27:51 00[IKE] Exiting destroy in fsm_public_key
Nov 16 13:27:51 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'

It loads normally without any problem. However, it does not use the ca loaded as shown below.
"C=JP, O=SBM, CN=CTC-SeGW" certificate is chaing with "C=JP, O=SBM, CN=SBM ROOT CA"
There is no problem with the chain of certificates.
Why not use a loaded ca?
Should I put the leftca parameter?
Attach log and conf files.
Thank you.

Nov 16 13:27:53 20[CFG] <femto_ap|1> no issuer certificate found for "C=JP, O=SBM, CN=CTC-SeGW"
Nov 16 13:27:53 20[IWS] <femto_ap|1> on_alert(29)
Nov 16 13:27:53 20[IKE] <femto_ap|1> no trusted RSA public key found for 'C=JP, O=SBM, CN=CTC-SeGW'
Nov 16 13:27:53 20[IWS] <femto_ap|1> on_alert(4)
Nov 16 13:27:53 20[ENC] <femto_ap|1> added payload of type NOTIFY to message
Nov 16 13:27:53 20[ENC] <femto_ap|1> order payloads in message
Nov 16 13:27:53 20[ENC] <femto_ap|1> added payload of type NOTIFY to message
Nov 16 13:27:53 20[ENC] <femto_ap|1> generating INFORMATIONAL request 2 [N(AUTH_FAILED)]
Nov 16 13:27:53 20[ENC] <femto_ap|1> insert payload NOTIFY into encrypted payload
Nov 16 13:27:53 20[ENC] <femto_ap|1> generating payload of type HEADER
Nov 16 13:27:53 20[ENC] <femto_ap|1> generating rule 0 IKE_SPI

History

#1 - 17.11.2020 10:59 - Tobias Brunner

- Status changed from New to Feedback

> "C=JP, O=SBM, CN=CTC-SeGW" certificate is chaing with "C=JP, O=SBM, CN=SBM ROOT CA"
> There is no problem with the chain of certificates.

I guess either that's not true or some of your numerous code modifications causes this.

> Why not use a loaded ca?

See above.

> Should I put the leftca parameter?

No, that makes no difference. But there is this in the log:

```
Nov 17 17:30:41 11[CFG] CA certificate "C=JP, O=SBM, CN=CTC-SeGW" not found, discarding CA constraint
```

However, I don't see any *rightca* setting in the config you posted (and that DN also seems to be the subject DN of the peer's end-entity certificate, not of a CA certificate).

> Attach log and conf files.

Please also attach the certificates, or at least some metadata e.g. from pki --print.

#2 - 18.11.2020 08:02 - bo lee

- File charon.log added

- File CNC_CasaSeGW_myCert_Qucell_TEST.key added

- File CNC_CasaSeGW_myCert_Qucell_TEST.pem added

- File CNC_CasaSeGW_SBM_ROOT_CA_TEST.pem added

- File ipsec.conf added

- File ipsec.secrets added

- File strongswan.conf added

I put the subjectname of the ca certificate in rightca.
But it fails.
Attach new log and certificate files.

#3 - 18.11.2020 10:29 - Tobias Brunner

> I put the subjectname of the ca certificate in rightca.
> But it fails.

Such constraints only apply after verifying the certificate in the first place.

> Attach new log and certificate files.

Your local key and certificate (C=KR, O=Innowireless Co. Ltd., CN=Qucell-HeNB) are completely irrelevant here. Important is the certificate of the peer (C=JP, O=SBM, CN=CTC-SeGW).

Files

ipsec.conf	1.25 KB	17.11.2020	bo lee
ipsec.secrets	44 Bytes	17.11.2020	bo lee
charon.log	125 KB	17.11.2020	bo lee
strongswan.conf	1.14 KB	17.11.2020	bo lee
CNC_CasaSeGW_myCert_Qucell_TEST.key	1.64 KB	18.11.2020	bo lee
charon.log	125 KB	18.11.2020	bo lee
CNC_CasaSeGW_myCert_Qucell_TEST.pem	1.12 KB	18.11.2020	bo lee
CNC_CasaSeGW_SBM_ROOT_CA_TEST.pem	1.18 KB	18.11.2020	bo lee
ipsec.conf	1.29 KB	18.11.2020	bo lee
ipsec.secrets	44 Bytes	18.11.2020	bo lee
strongswan.conf	1.14 KB	18.11.2020	bo lee