strongSwan - Feature #2326

Add eap-aka-3gpp plugin providing 3GPP MILENAGE software implementation

16.05.2017 11:55 - Thomas Strangert

Status:	Closed	**Start date:**	16.05.2017
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.6.0		
Resolution:	Fixed		

Description

I have written a eap_aka_3gpp plugin with proper 3GPP MILENAGE quintuple handling, tested and compliant with 3GPP telecom systems. MILENAGE is the algorithm used worldwide in "all" UMTS/3G and LTE/4G mobile networks, and is defined in the standard 3GPP TS 35.206 (http://www.3gpp.org/DynaReport/35206.htm)

I used the eap_aka_3gpp2 plugin as a base. (Also corrected a file name "bug" in the conf/Makefile.am for the 3gpp2 plugin.)

The plugin supports multi-thread/parallell authentications (as opposed to 3GPP's reference code I've seen been used in some rather notable places, none mentioned..).

I want to give something back to the community, dunno how to do this other than by opening a feature ticket.

Related issues:

Related to Issue #2316: Regarding testing with Stongswan client 5.5.2	**Closed**

Associated revisions

Revision 1aba82bf - 05.07.2017 10:03 - Tobias Brunner

eap-aka-3gpp: Add plugin that implements 3GPP MILENAGE algorithm in software

This is similar to the eap-aka-3gpp2 plugin. K (optionally concatenated
with OPc) may be configured as binary EAP secret in ipsec.secrets or
swanctl.conf.

Based on a patch by Thomas Strangert.

Fixes #2326.

History

#1 - 16.05.2017 12:10 - Tobias Brunner

- Status changed from New to Feedback

Thanks! Please have a look at Contributions regarding licensing options (we'd obviously prefer a submission under the MIT X11 license, but you are free to submit under the GPL if you want). And please post a proper patch (i.e. commit to a branch in your local repository and then use git format-patch).

I have not yet looked that closely over the code but why is there a Rijndael implementation in *_function.c? Can't you use any of the AES implementations provided by the other plugins?

#2 - 16.05.2017 15:03 - Thomas Strangert

Hi,

I've basically never used git before so I have no idea how to do a patch. I googled and tried a little but it doesn't come out any good and I can't be bothered to spend more time on it, sorry.

The plugin files are previously non-existent and are just to drop in without any conflict. The other 4 files only differ one or a few conflict-free lines each compared with the ones in release 5.5.2 so that's easy enough to check with a manual diff before you drop in those files as well.

As regards to X11 or GPL I don't care which one, but since I based my work on the eap_aka_3gpp2 plugin and that used GPL, so did I. Perhaps the license could be changed but I didn't dare to do that.

I could probably have used an existing AES implementation but I didn't investigate those, what they do exactly/how to invoke those.

Anyhoo:
My plugin works just fine and is tested against 3rd party HW/SW (USIM cards, HLRs, ...) and I wanted to contribute something back. Take it as is and merge it in max 15 minutes or ignore it all together, I don't really care. My source files are in the attached zip so maybe someone else find use for it.

Thanks for a great project :)

#3 - 16.05.2017 19:07 - Tobias Brunner

- Subject changed from Make my eap_aka_3gpp plugin official? to Add eap-aka-3gpp plugin providing 3GPP MILENAGE software implementation

- Assignee set to Tobias Brunner

> The plugin files are previously non-existent and are just to drop in without any conflict. The other 4 files only differ one or a few conflict-free lines each compared with the ones in release 5.5.2 so that's easy enough to check with a manual diff before you drop in those files as well.

Well, you also changed the line endings to CRLF (and you renamed a file), so not exactly drop-in. But OK. And there were lots of code-style issues.

> As regards to X11 or GPL I don't care which one, but since I based my work on the eap_aka_3gpp2 plugin and that used GPL, so did I. Perhaps the license could be changed but I didn't dare to do that.

OK, I've added the MIT X11 header to the files.

> I could probably have used an existing AES implementation but I didn't investigate those, what they do exactly/how to invoke those.

I've refactored that (I actually changed quite a lot in that particular file).

> My plugin works just fine and is tested against 3rd party HW/SW (USIM cards, HLRs, ...) and I wanted to contribute something back.

That's definitely appreciated. I've pushed an updated version of the plugin to the *2326-eap-aka-3gpp* branch of our repository. Would be great if you could test if it still works as expected.

I changed how the secrets are configured. Since ipsec.secrets and swanctl.conf already support configuring binary EAP secrets (0x or 0s prefix) there is no need to convert the secret manually (for which you could have used the chunk_from_hex() helper, by the way).

#4 - 16.05.2017 19:11 - Tobias Brunner

- Related to Issue #2316: Regarding testing with Stongswan client 5.5.2 added

#5 - 17.05.2017 17:54 - Thomas Strangert

Thank you for importing the code and creating a branch!

Also thank you for tweaking the code to use the existing AES library and improved ipsec.secrets handling (both things I realised too late that I could/should have used).

I will definitely compile and test your branch to verify it (I've browsed/compared the new code, looks fine). It will take a couple of weeks, I need to set up my test environment first. Been a while since I wrote my plugin (2015/Strongswan v5.2.2), but now I have a project that caused me to re-open it and also to submit it to you.

#6 - 17.05.2017 18:22 - Tobias Brunner

> I will definitely compile and test your branch to verify it (I've browsed/compared the new code, looks fine). It will take a couple of weeks, I need to set up my test environment first.

Thanks. Not to rush you, but our next release is already scheduled in two weeks (5.5.3), the one after that about three months later. Therefore, it would be great if you could get the tests done as soon as possible, so we could include the plugin in the upcoming release.

By the way, is there a particular reason you made OPc configurable and not OP? OPc could easily be derived from K and OP, so I wondered if it's more common to set OPc than OP (I saw the 3GPP documents mention that operators might want to keep OP private, even though it doesn't increase the security).

#7 - 18.05.2017 07:59 - jos george

Hi Tobias / Thomas,

I could also test this add on with real epdg and AAA and HSS . But i am not sure how to compile it and use it . If you can guide on that part , I will test

and update you in another 2 days time .

Regards
Jos

#8 - 18.05.2017 09:25 - Tobias Brunner

> But i am not sure how to compile it and use it . If you can guide on that part , I will test and update you in another 2 days time .

That'd be great. With what do you need help exactly?

#9 - 18.05.2017 09:29 - Thomas Strangert

Two weeks will be tight they way my project dependencies lie, but I'll try!

Regarding choice of OP or OPc:

> **OPc = XOR (OP, AES (OP, K))**
> where K is the secret Key, normally individual/unique to each subscriber (i.e. USIM card)
> and OP is a semistatic constant chosen by the operator, common to all/many subs/USIMs.

So while the cryptographic strength on an individual level isn't increased by using the OPc rather than the OP, the aggregated secrecy of millions USIM cards out in the "public" will potentially be better if they'll not all share a common value (OP) but will only contain the unique values K and OPc. Well, that is the official argument anyway...

#10 - 18.05.2017 09:45 - jos george

Hi Tobias,

I have only a little knowledge on how to compil . I have installed 5.5.2 and tested using eap_aka_3gpp2 plugin , can you please guide on what all modifications i have to make the eap aka using milenage work . Also I am planning to keep Ki and OPc values in ipsec.secrets file instead of using actual usim card

Regards
jos

#11 - 18.05.2017 10:02 - Tobias Brunner

> I have only a little knowledge on how to compil . I have installed 5.5.2 and tested using eap_aka_3gpp2 plugin , can you please guide on what all modifications i have to make the eap aka using milenage work .

You'd want to uninstall all the binary packages related to strongSwan you installed before starting to build from sources. Otherwise, you'll get conflicts with incompatible libraries or plugins. Then clone the Git repository and checkout the branch I mentioned above e.g. with:

```
git clone -b 2326-eap-aka-3gpp https://git.strongswan.org/strongswan.git
```

Then refer to InstallationDocumentation, in particular regarding the tools required when building from the Git repository and the plugin dependencies, and make sure to add *--enable-eap-aka-3gpp* and *--enable-eap-aka* to the configure options.

> Also I am planning to keep Ki and OPc values in ipsec.secrets file instead of using actual usim card

That's the whole point of the plugin. Just configure an EAP secret associated with the client's identity with a binary value of 32 bytes length (K followed by OPc), this can either be encoded as hex or Base64 string (0x or 0s prefix, respectively).

#12 - 18.05.2017 11:21 - Thomas Strangert

> I could also test this add on with real epdg and AAA and HSS .

You would then set up your Strongswan to be a client, i.e. acting like a phone trying to connect to the ePDG using credentials in its USIM.

In Strongswan, you should have an entry in ipsec.secrets looking something like:

> **IMSI : EAP KOPc** (a concatenation of K and OPc in hex or Base64) or
> **IMSI : EAP K** (where OPc is set to 0 if not given)

Edit: The KOPc and K values shouldn't be quoted with "

#13 - 18.05.2017 11:49 - jos george

Hi Thomas,

Yes , i am trying to do the same way you have explained.

Regards
Jos

#14 - 18.05.2017 14:47 - jos george

- File strongswan.log added

Hi Tobias,

I have tried and i was failing during the make step

Below are the steps i have performed and failure log attached

1)git clone -b 2326-eap-aka-3gpp https://git.strongswan.org/strongswan.git

2)cd strongswan/
3) ./autogen.sh

4) ./configure --prefix=/usr --sysconfdir=/etc --enable-eap-aka --enable-eap-simaka-sql --enable-sql --enable-eap-aka-3gpp2 --enable-attr-sql --enable-sqlite --enable-eap-sim --enable-eap-sim-file --enable-eap-radius --enable-eap-identity --enable-eap-aka-3gpp

1. last line of output as below

config.status: executing depfiles commands
config.status: executing libtool commands

```
strongSwan will be built with the following plugins
---------------------------------------------------
libstrongswan: aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkc
s12 pgp dnskey sshkey pem fips-prf gmp curve25519 xcbc cmac hmac sqlite
libcharon:     attr attr-sql kernel-netlink resolve socket-default stroke vici sql updown eap-identity eap-sim
 eap-sim-file eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-simaka-sql eap-radius xauth-generic
libtnccs:
libtpmtss:
```

5)make

logs attached

#15 - 18.05.2017 14:58 - Tobias Brunner

You are missing gperf, as mentioned before, you need additional tools when building from the Git repository (see the page I linked above). Run make distclean after installing the additional tools, then go through the build steps again beginning with ./autogen.sh.

#16 - 19.05.2017 13:05 - jos george

Hi Tobias,

Thank you for the help , currently i am trying to test the client

Ki and OPc values I have to configure in ipsec.secrets file is 32 bit hex values as shown below

00112233445566778899AABBCCDDEEFF ----> KI
0ED47545168EAFE2C39C075829A7B61F ----> OPC

I have configured as below

include /etc/ipsec.d/*.secrets

0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org : EAP "0x00112233445566778899AABBCCDDEEFF"
0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org : EAP "0x0ED47545168EAFE2C39C075829A7B61F"

While running the test , I am getting below error

"invalid EAP K or K+OPc key found for 0 404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org to authenticate with AKA, should be a 16 or 32 byte long binary value."

What change I can do now

Regards
Jos

#17 - 19.05.2017 13:27 - Thomas Strangert

Think that you shouldn't have double quotes " when giving hex-encoded values starting with 0x. The file parser might interpret that as if you have an actual string value starting with "0x..." and neglect to do the string-to-binary conversion.

And: If you want to give both K and OPc for a particular subscriber then with your values it should have it all in one line like this:
0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org : EAP 0x00112233445566778899AABBCCDDEEFF0ED47545168EAFE2C39C075829A7B61F
(even though this forum seems to show it on two lines)

#18 - 19.05.2017 13:47 - jos george

Hi Thomas,

We have tried without qoute , single qoute for this hex value but results are the same

{{May 19 17:07:21 localhost charon: 11[IKE] server requested EAP_AKA authentication (id 0x01)
May 19 17:07:21 localhost charon: 11[LIB] ignoring skippable EAP-SIM/AKA attribute AT_CHECKCODE
May 19 17:07:21 localhost charon: 11[IKE] invalid EAP K or K+OPc key found for 0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org to authenticate with AKA, should be a 16 or 32 byte long binary value}}

We have tried below syntax also , but it's failing

0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org : EAP 0x00112233445566778899AABBCCDDEEFF0ED47545168EAFE2C39C075829A7B61F

Regards
JOs

#19 - 19.05.2017 14:25 - Tobias Brunner

You definitely have to omit the quotes. Is there perhaps another secret loaded for that same identity? The code just tries the first one it finds, it doesn't check for other secrets with the same identity. Check the log when the daemon starts, it will list all the secrets that are loaded.

#20 - 22.05.2017 13:27 - jos george

Hi Tobias /Thomas,

Thank you for the suggestions

We have deleted the quintuplets db and restarted the client and it started working perfectly . Strongswan client successfully authenticated and MSK is established.IP is also assigned to our strongswan client from our network.
But after that we are getting the following error “constraint requires public key authentication, but EAP was used”.
I have question here ,if pubkey authentication was mandatory, then it should have failed at earlier stages. Why this is failing after IP is assigned ?
The ipsec.conf file is also attached for your reference.

```
EAP method EAP_AKA succeeded, MSK established
authentication of '0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org' (myself) with EAP
generating IKE_AUTH request 3 [ AUTH ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (84 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (196 bytes)
parsed IKE_AUTH response 3 [ AUTH CPRP(ADDR) SA TSi TSr N(MOBIKE_SUP) ]
authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with EAP successful
constraint requires public key authentication, but EAP was used
selected peer config 'net-net' inacceptable: constraint checking failed
no alternative config found
generating INFORMATIONAL request 4 [ N(AUTH_FAILED) ]
```

Ipsec conf file

```
conn net-net
        left=10.43.103.245
        leftid=0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org
        leftsubnet=0.0.0.0/0
        leftsourceip=%config
        leftauth=eap-aka
        right=10.53.83.25
        rightid=srvcc.nsn.com
        rightauth=pubkey
```

```
        rightsubnet=0.0.0.0/0
        rightsendcert=always
        eap_identity=0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org
        auto=start
```

#21 - 22.05.2017 14:39 - Tobias Brunner

Looks like there is a mutual authentication with EAP-AKA, so configure *rightauth=eap-aka*.

#22 - 22.05.2017 15:03 - jos george

I have changed righauth=eap-aka . But getting below error . i can see networking is sharing mobile ip to the ue and after that ipsec client is sending authentication failure

```
EAP method EAP_AKA succeeded, MSK established
authentication of '0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org' (myself) with EAP
generating IKE_AUTH request 3 [ AUTH ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (84 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (196 bytes)
parsed IKE_AUTH response 3 [ AUTH CPRP(ADDR) SA TSi TSr N(MOBIKE_SUP) ]
authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with EAP successful
constraint check failed: EAP identity '404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org' required
selected peer config 'net-net' inacceptable: constraint checking failed
no alternative config found
generating INFORMATIONAL request 4 [ N(AUTH_FAILED) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (68 bytes)
establishing connection 'net-net' failed
```

#23 - 22.05.2017 15:15 - Tobias Brunner

Where does 404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org come from? You seem to have *rightid=srvcc.nsn.com* configured and the client's ID has a 0 prepended. Anyway, you could try setting *aaa_identity=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org*.

#24 - 23.05.2017 12:54 - jos george

We have tried as per your suggestions above still we have the error

Currently our test network only accepts with “0” as prefix.(i.e 0404996699887700@xxx is valid ID).

As in our case authentication with 0404996699887700 is getting successful. MSK was getting established, IP also received .So is it really necessary for strongswan to check the eap_identity at the end ? . Is there any alternate way we can force the strongswan to skip this check .

Please find the log's below

```
generating IKE_AUTH request 1 [ IDi IDr CPRQ(ADDR DNS) SA TSi TSr N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (260 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (188 bytes)
parsed IKE_AUTH response 1 [ IDr EAP/REQ/AKA ]
server requested EAP_AKA authentication (id 0x01)
ignoring skippable EAP-SIM/AKA attribute AT_CHECKCODE
allow mutual EAP-only authentication
generating IKE_AUTH request 2 [ EAP/RES/AKA ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (100 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (68 bytes)
parsed IKE_AUTH response 2 [ EAP/SUCC ]
EAP method EAP_AKA succeeded, MSK established
authentication of '0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org' (myself) with EAP
generating IKE_AUTH request 3 [ AUTH ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (84 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (196 bytes)
parsed IKE_AUTH response 3 [ AUTH CPRP(ADDR) SA TSi TSr N(MOBIKE_SUP) ]
authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with EAP successful
constraint check failed: EAP identity '0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org' required
selected peer config 'net-net' inacceptable: constraint checking failed
no alternative config found
generating INFORMATIONAL request 4 [ N(AUTH_FAILED) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (68 bytes)
establishing connection 'net-net' failed
```

Logs with aaa_identity=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org is as below
---

```
generating IKE_AUTH request 1 [ IDi IDr CPRQ(ADDR DNS) SA TSi TSr N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
```

```
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (260 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (188 bytes)
parsed IKE_AUTH response 1 [ IDr EAP/REQ/AKA ]
server requested EAP_AKA authentication (id 0x01)
ignoring skippable EAP-SIM/AKA attribute AT_CHECKCODE
allow mutual EAP-only authentication
generating IKE_AUTH request 2 [ EAP/RES/AKA ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (100 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (68 bytes)
parsed IKE_AUTH response 2 [ EAP/SUCC ]
EAP method EAP_AKA succeeded, MSK established
authentication of '0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org' (myself) with EAP
generating IKE_AUTH request 3 [ AUTH ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (84 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (196 bytes)
parsed IKE_AUTH response 3 [ AUTH CPRP(ADDR) SA TSi TSr N(MOBIKE_SUP) ]
authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with EAP successful
constraint check failed: EAP identity 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' required
selected peer config 'net-net' inacceptable: constraint checking failed
no alternative config found
generating INFORMATIONAL request 4 [ N(AUTH_FAILED) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (68 bytes)
establishing connection 'net-net' failed
```

Regards
jos

#25 - 23.05.2017 14:21 - Tobias Brunner

I wonder if mutual EAP is the way to go. As it seems difficult to configure this properly via the ipsec.conf backend (it adds *eap_identity* to both the local and remote authentication round, which seems a bit strange to me). You could try configuring via swanctl.conf, where you can at least configure the *eap_id* specifically for each end of the authentication. If you want to use ipsec.conf it might work if you configure *rightauth=pubkey* and let the gateway actually authenticate with a certificate first.

#26 - 25.05.2017 07:41 - jos george

Hi Tobias,

I have tried with leftauth=eap-aka,rightauth=pubkey . But my epdg is not replying with certificate data. When i checked the trace i can see in IKE_AUTH message , one notify message is flowing Notify Message Type: EAP_ONLY_AUTHENTICATION (16417) . So if EAP_ONLY_AUTH is flowing edpg wont send back certifate info

Documetent says like below

IKEv2 EAP AKA method uses two methods of authentication: EAP and PKI.
EAP only authentication is mutual authentication and key agreement completely based on EAP (no PKI) .

Can you please help to suppress the notify from strongswan client

Regards
JOs

#27 - 25.05.2017 07:58 - Tobias Brunner

> Can you please help to suppress the notify from strongswan client

You can disable *charon.multiple_authentication* in strongswan.conf.

#28 - 25.05.2017 14:29 - jos george

As suggested by you ,, we have supressed the “EAP_ONLY” notification message . Now the epdg is sending certificate ,but unfortunately we are getting error “IDr Payload missing”.
Below mentioned steps for root CA and VPN certificate generation.

```
ipsec pki --gen > caKey.der -
ipsec pki --self --in caKey.der --dn "C=CH, O=strongSwan, CN=strongSwan CA" --san srvcc.nsn.com --ca >  caCert
.der  ROOT CA
ipsec pki --gen >  peerKey.der
ipsec pki --pub --in peerKey.der | ipsec pki --issue --cacert caCert.der --cakey caKey.der --dn "C=CH, O=stron
gSwan, CN=10.53.83.25" --san srvcc.nsn.com > peerCert.der  SERVER CERTIFICATE
```

peerKey and peerCert are stored in the epdg.
Here is the Charon logs :

```
ipsec up net-net
initiating IKE_SA net-net[2] to 10.53.83.25
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) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (334 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (284 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
sending cert request for "C=CH, O=strongSwan, CN=strongSwan CA"
establishing CHILD_SA net-net
generating IKE_AUTH request 1 [ IDi CERTREQ CPRQ(ADDR DNS) SA TSi TSr ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (244 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (60 bytes)
parsed IKE_AUTH response 1 [ ]
IDr payload missing
generating INFORMATIONAL request 2 [ N(AUTH_FAILED) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (68 bytes)
establishing connection 'net-net' failed
```

ipsec conf file:

```
conn net-net
        left=10.43.103.245
        leftid=0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org
        leftsubnet=0.0.0.0/0
        leftsourceip=%config
        leftauth=eap-aka
        right=10.53.83.25
        righted=srvcc.nsn.com
        rightauth=pubkey
        rightsubnet=0.0.0.0/0
        rightsendcert=always
        #aaa_identity=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org
        eap_identity=0404996699887700@nai.epc.mnc099.mcc404.3gppnetwork.org
        auto=start
```

Kindly help in this issue ..

#29 - 26.05.2017 08:59 - Tobias Brunner

> parsed IKE_AUTH response 1 [ ]

Your ePDG responds with an invalid empty IKE_AUTH message. I suggest you check the log there to see why it does so.

#30 - 29.05.2017 11:44 - jos george

Hi ,

Currently epdg is accepting the certificate ,
I can see from logs " authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with RSA signature successful "

After that message it's failing with the error

constraint check failed: identity 'srvcc.nsn.com' required

and in ipsec.conf file we have configured rightid=srvcc.nsn.com , if we are keeping rightid=%any we can passing this step , but it is failing at our network end because we are not providing rightid .

Please find the command for epdg certificate generation we have used

ipsec pki --pub --in peerKey.der | ipsec pki --issue --cacert caCert.der --cakey caKey.der --dn "C=CH, O=strongSwan, CN=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org" --san srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org --san srvcc.nsn.com > peerCert.der

Charon logs

```
[root@localhost srnpdg]# ipsec up net-net
initiating IKE_SA net-net[2] to 10.53.83.25
```

```
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) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (334 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (284 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
sending cert request for "C=CH, O=strongSwan, CN=strongSwan CA"
establishing CHILD_SA net-net
generating IKE_AUTH request 1 [ IDi CERTREQ IDr CPRQ(ADDR DNS) SA TSi TSr ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (268 bytes)
received packet: from 10.53.83.25[500] to 10.43.103.245[500] (1372 bytes)
parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/AKA ]
received end entity cert "C=CH, O=strongSwan, CN=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org"
  using certificate "C=CH, O=strongSwan, CN=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org"
  using trusted ca certificate "C=CH, O=strongSwan, CN=strongSwan CA"
checking certificate status of "C=CH, O=strongSwan, CN=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org"
certificate status is not available
  reached self-signed root ca with a path length of 0
authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with RSA signature successful
constraint check failed: identity 'srvcc.nsn.com' required
selected peer config 'net-net' inacceptable: constraint checking failed
no alternative config found
generating INFORMATIONAL request 2 [ N(AUTH_FAILED) ]
sending packet: from 10.43.103.245[500] to 10.53.83.25[500] (68 bytes)
establishing connection 'net-net' failed
```

Regards
Jos

#31 - 29.05.2017 12:14 - Tobias Brunner

> Currently epdg is accepting the certificate ,
> I can see from logs " authentication of 'srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org' with RSA signature successful "

Yep, looks like your ePDG uses that as its IDr. So why don't you configure *rightid=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org* if that's the ID it want to use?

> After that message it's failing with the error
>
> constraint check failed: identity 'srvcc.nsn.com' required
>
> and in ipsec.conf file we have configured rightid=srvcc.nsn.com

Yes, that's because of that setting.

> , if we are keeping rightid=%any we can passing this step , but it is failing at our network end because we are not providing rightid .

Correct. You could also use *rightid=%srvcc.nsn.com* then that identity is checked against all *subjectAlternativeName* extensions of the certificate and it must not match the IDr value used by the server. But this also causes the IDr not to get sent in the request (to avoid that would require a patch).

#32 - 29.05.2017 14:46 - jos george

srvcc.nsn.com is the service name or access point name(APN) set in AAA/HSS .

case 1) When I configure rightid=srvcc.nsn.com , In IKE_AUTH message Strongswan will send it as responder id . epdg will fetch this id and fill in service name as srvcc.nsn.com and forward it to AAA/HSS , So that they will pass on service related info to epdg.

case 2) When we configure rightid=srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org . epdg will fill in service name as " srnepdg.epdg.epc.mnc099.mcc404.pub.3gppnetwork.org" .AAA will give error unkown apn name and call will fail .

case 3) When we configure rightid=%any , Strongswan won't send any responder id and epdg will be forwarding service name as null to AAA and call will fail again .

In case 1 , epdg is accepting the certificate and authentication is successful , but strongswan is looking for one more authentication of our right id srvcc.nsn.com . at this point our call is failing , can we suppress this ?

#33 - 29.05.2017 15:32 - Tobias Brunner

> can we suppress this ?

Not without code changes (or perhaps server-side configuration changes, like e.g. a hard-coded service name).

#34 - 30.05.2017 08:27 - jos george

HI Tobias,

I am able to get IP after changing the service name in hss as per our epdg id .

Thanks a lot for the help .

Do we able to load this in android phone ?

#35 - 30.05.2017 09:25 - Tobias Brunner

> Do we able to load this in android phone ?

You can enable the plugin but to prepare the secret you probably need to apply some code changes (to get that in binary form).

#36 - 30.05.2017 09:25 - Tobias Brunner

- Target version set to 5.6.0

#37 - 30.05.2017 19:46 - jos george

I wish we have one for Android also. Thanks a lot Thomas for your plugin . We will be able to use it for our testings . Thank you Tobias for all the guidence & thanks a lot for such a wonderful project.

#38 - 31.05.2017 10:24 - Tobias Brunner

> I wish we have one for Android also.

As I said there is not really anything preventing you from using this plugin on Android.

#39 - 03.06.2017 09:37 - jos george

Can you please guide us on what all changes we have to make to install strongswan on andriod

#40 - 07.06.2017 11:48 - Tobias Brunner

> Can you please guide us on what all changes we have to make to install strongswan on andriod

I already outlined the required changes above. Please ask specific questions if you need help.

#41 - 05.07.2017 10:04 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

#42 - 16.10.2017 13:29 - Thomas Strangert

Long overdue feedback on this plugin:
I've pulled, compiled and tested the official 5.6.0 version and it works just fine to the extent I previously was using my original, unofficial contribution.
I.e. the merge into the code base is AOK.

#43 - 16.10.2017 14:17 - Tobias Brunner

> Long overdue feedback on this plugin:
> I've pulled, compiled and tested the official 5.6.0 version and it works just fine to the extent I previously was using my original, unofficial contribution.
> I.e. the merge into the code base is AOK.

Great, thanks for the feedback.

Files

eap_aka_3gpp.zip	52.2 KB	16.05.2017	Thomas Strangert
Clipboard01.gif	27.3 KB	16.05.2017	Thomas Strangert
strongswan.log	14.7 KB	18.05.2017	jos george